landing. The size and windings of the reader antenna can be properly designed using the known design principles of RF antennas to generate operational magnetic fields (Hov) at 13.56 MHz for activation with payment card devices operating in the vicinity. The intensities of the Hov are in a specific range at least within the inverted frustroconical operating volume. The specified range is selected taking into account that the payment cards displayed in the field, which can be manufactured by different issuers or sellers of cards for different specifications, can show a range of behaviors. For example, inductive coupling antennas or RFID tags on cards that operate in the vicinity issued by different vendors may have different sizes and shapes. The specified range of the magnetic field strengths in the frustoconical operating volume is selected to obtain adequate energy to activate and communicate with a range of interacting payment cards of different origin and behaviors.

The frustoconical operating volume is defined by the geometric parameters (for example, the diameters of the base DI and D2, and the axial length of the SI cone and the axial cylindrical length S2) shown in Figure 1). Table I lists the nominal values of these selected parameters for an exemplary definition of the frustoconical operating volume for the PayPass reference reader of Figure 2.

TABLE 1 Volume DI 3 cms operative D2 5 cms dimensions SI 1 cm S2 3 cms In the exemplary PayPass reference reader, the reader antenna has a diameter of approximately 7 cm and is placed approximately 15 cm below the landing plane. The antenna has dual activity and dummy or simulated windings that when they are food with electric currents, provide at least a minimum field strength Hmin needed to feed and communicate with a payment card that is placed within the specified frustroconomic operating volume. At the same time, the operational magnetic fields (Hov) generated by the antenna are restricted to remain below a certain maximum intensity Hmax. The value of Hmax is appropriately selected to limit energy dissipation in payment cards to thresholds below those commonly accepted to avoid damage to the device. Likewise, the magnetic field strengths inside and outside the operating volume are limited to comply with all international and national regulations and laws related to safe use and exposure limits for such radiations.

The operating volume of the exemplary PayPass reference reader can be characterized or calibrated using an appropriate reference card, for example, a PayPass reference card (Figure 3), which is also described in the co-pending US patent application No. Operating magnetic fields (Hov) in the frustoconical operating volume can be specified or measured in equivalent terms of the required energy transfer (Vov voltage) from the reader to a payment card.

Table II shows a specification of the minimum and maximum values for the Vov energy transfer voltages in the frusconical operating volume of the PayPass reference reader. Electromagnetic coupling (ie, mutual inductance) between the card and the reader's antennas disturbs the operational magnetic fields when a card is brought to the operating volume. In particular, the magnetic field strength within the operating volume decreases due to the additional load caused by the card. The Vov values for the reader and 1 card can be measured at appropriate definition points in the reference reader and antenna circuits of the reference card, respectively. The charge of a card can be measured by observing a circuit voltage drop? Vov (Vov, air-free) at an appropriate point in the antenna circuit of the PayPass reference reader. Table II also shows a maximum acceptable value of? Vov corresponding to a nominal charge of the card.

TABLE II Topic Parameter PCD Nom. Max. PICC Non. Max. Units min min. Transfer VOT 3-az 8.5 2.8-az 8.7 V power PCD? PICC _a 0.35 0.35 V / cm? Vo ^ pat C 8 V The arrangement of the inventive reader (eg, the PayPass reference reader) having a defined frustoconical operating volume can be used in conjunction with the systems and methods described in the co-pending US patent application N / S for testing the product payment cards, for example, to verify compliance with specifications. An exemplary procedure to verify compliance with the specifications of a product card may include the following steps: (a) measure the transmission of the data by the product card in the reference reader PayPass, with the reader sending "average" value instructions to the product card and with the PayPass reference reader providing an "average" energy level. The energy level and characteristics of the instructions produced by the PayPass reference reader are calibrated with respect to a reference card, and (b) measuring the data reception and energy sensitivity of the product card under test using the PayPass reference reader.

During operation a signal of ± 600 mW can be fed to the input impedance of 50 O of the reader input to generate a magnetic field, which is representative of most PayPass readers deployed in the field. The product cards can be characterized under conditions that simulate the conditions of use of the card in the field. For example, the behavior of a product card can be characterized or measured at different distances from and in different orientations in relation to the reader antenna. In an exemplary test routine, the reader is held in a stationary position and the target product card moves slowly through the operating volume from one test position to the next for the measurements. Figure 5 shows a series of these test positions that are used in the exemplary test routine. The series of test positions is distributed along a three-dimensional space of the frustoconical operating volume. The test positions are shown as quadruplet coordinates (r, f, z,?) In Figure 5, where the polar coordinates r, f and z represent the center of the product card under test. With reference to Figure 1, (r, f, z) = (0,0,0) represents the center of the landing plane. In the exemplary testing routine, all measurements on the object product card are made with the card held perpendicular to the z-axis. the z coordinate represents the height of the payment card from the landing plane. The coordinate? represents the orientation of the card in relation to the axis f = 0. While the present invention has been described particularly with reference to the exemplary embodiments thereof, those skilled in the art will understand that various modifications and alterations can be made without departing from the spirit. and scope of the invention. Accordingly, the described embodiments of the invention are considered only demonstrative, and the invention is limited in scope only as specified in the appended claims.

Patent Citations (58)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US4066873A	1976-01-26	1978-01-03	The First National Bank Of Chicago	Identification and access card with associated optical decoding means
JPS61201390A	1985-03-04	1986-09-06	Casio Comput Co Ltd	Ic card
FR2586428B1 *	1985-08-26	1988-11-25	Pasteur Institut	POLYPEPTIDES AND ANTIBODIES, CHARACTERISTICS OF PAPILLOMAVIRUS AND THEIR APPLICATIONS TO IN VITRO DIAGNOSIS, PREVENTION AND / OR CONTROL OF PAPILLOMAVIRUS INFECTIONS
US5880452A *	1990-11-15	1999-03-09	Geo Labs, Inc.	Laser based PCMCIA data collection system with automatic triggering for portable applications and method of use
US5225977A *	1991-03-18	1993-07-06	Hooper John B	Card payment system for service dispensing devices
GB9105851D0	1991-03-20	1991-05-08	Security Systems Consortium Th	Securing financial transactions
US5466919A *	1993-04-02	1995-11-14	Hovakimian; Henry	Credit/charge card system enabling purchasers to contribute to selected charities

US5511111A *	1993-11-01	1996-04-23	Engineering And Business Systems, Inc.	Caller name and identification communication system with caller screening option
US5623552A	1994-01-21	1997-04-22	Cardguard International, Inc.	Self-authenticating identification card with fingerprint identification
US5511114A *	1994-06-06	1996-04-23	Call Processing, Inc.	Telephone pre-paid calling card system and method
US5602744A *	1994-09-29	1997-02-11	Meek, Jean L.	Universal send/receive utility usage data gathering system
JPH08123919A *	1994-10-28	1996-05-17	Mitsubishi Electric Corp	Noncontact ic card system and communication method thereof
US5748737A *	1994-11-14	1998-05-05	Daggar; Robert N.	Multimedia electronic wallet with generic card
US5625628A *	1995-03-15	1997-04-29	Hughes Electronics	Aloha optimization
US6010074A *	1996-04-01	2000-01-04	Cubic Corporation	Contactless proximity automated data collection system and method with collision resolution
US6486813B1 *	1996-07-30	2002-10-15	Micron Technology, Inc.	Radio frequency data communications device with adjustable receiver sensitivity and method
DE19635311A1 *	1996-09-02	1998-03-12	Angewandte Digital Elektronik	Adaptive identification of contactless chip cards
US6150955A *	1996-10-28	2000-11-21	Tracy Corporation Ii	Apparatus and method for transmitting data via a digital control channel of a digital wireless network
GB2319698B *	1996-11-21	2001-08-08	Motorola Inc	Method for communicating with a plurality of contactless data carriers and contactless data carrier for use therein
US6119940A *	1997-02-18	2000-09-19	Unisys Corporation	Identification methods
US6112981A	1997-02-25	2000-09-05	Dresser Industries, Inc.	Bar code reader for a fuel dispenser
GB9719583D0	1997-09-16	1997-11-19	Ncr Int Inc	A method of authenticating a magnetic card
US6810304B1	1997-09-26	2004-10-26	Gilbarco Inc.	Multistage ordering system for a fueling and retail environment
US6134309A *	1997-09-30	2000-10-17	Creative Games International, Inc.	Pre-paid phone card system with promotional link
US6061344A *	1998-02-19	2000-05-09	Micron Technology, Inc.	Method of addressing messages and communications system
US6072801A *	1998-02-19	2000-06-06	Micron Technology, Inc.	Method of addressing messages, method of establishing wireless communications, and communications system
US6315195B1 *	1998-04-17	2001-11-13	Diebold, Incorporated	Transaction apparatus and method
US6710701B2	1998-04-22	2004-03-23	Gilbarco Inc.	Rfid tag location using tag or host interaction record
DE19830526A1 *	1998-07-08	2000-01-13	Orga Kartensysteme Gmbh	Method and device for controlling communication between a terminal and a number of chip cards
US6297789B2 *	1998-07-09	2001-10-02	Tyco Electronics Corporation	Integrated circuit card with liquid crystal display for viewing at least a portion of the information stored in the card
US6404643B1 *	1998-10-15	2002-06-11	Amerasia International Technology, Inc.	Article having an embedded electronic device, and method of making same
US6657729B1 *	1999-06-10	2003-06-10	Cubic Corporation	Multiple protocol smart card communication device
JP3824451B2 *	1999-07-29	2006-09-20	富士通株式会社	Non-contact IC card presence / absence detection circuit
AU6674000A *	1999-08-11	2001-03-13	Mark Iv Industries Limited	Method and means for rf toll collection
JP2001076117A	1999-08-31	2001-03-23	Toppan Forms Co Ltd	Advantageous card
US6145742A *	1999-09-03	2000-11-14	Drexler Technology Corporation	Method and system for laser writing microscopic data spots on cards and labels readable with a CCD array
US6394346B1 *	1999-10-07	2002-05-28	Cubic Corporation	Contactless smart card high production encoding machine
WO2001031555A1 *	1999-10-28	2001-05-03	Gould David B	Prepaid cash equivalent card and system
DE10055602A1	1999-12-30	2001-07-12	Ibm	Exit control system for supermarket or department store, produces receipt based on contactlessly received information and updates payment status
FR2809251B1 *	2000-05-17	2003-08-15	St Microelectronics Sa	DEVICE FOR PRODUCING AN ELECTROMAGNETIC FIELD FOR A TRANSPONDER
KR100486758B1 *	2000-08-31	2005-05-03	매그나칩 반도체 유한회사	Radio Frequency Identification Tag System for preventing collision and collision preventing method thereof

AU9260001A	2000-09-08	2002-03-22	American Express Travel Relate	A system and method for loyalty program distribution and settlement
FR2815490B1 *	2000-10-16	2006-07-07	Inside Technologies	CONTACTLESS INTEGRATED CIRCUIT READER
US7253717B2 *	2000-11-29	2007-08-07	Mobile Technics Llc	Method and system for communicating with and tracking RFID transponders
JP2002351585A *	2001-05-22	2002-12-06	Sankyo Seiki Mfg Co Ltd	Data updating method and controller for nonvolatile memory
US7889052B2	2001-07-10	2011-02-15	Xatra Fund Mx, Llc	Authorizing payment subsequent to RF transactions
US6666982B2	2001-10-22	2003-12-23	Tokyo Electron Limited	Protection of dielectric window in inductively coupled plasma generation
JP2003162755A	2001-11-27	2003-06-06	Great Information Kk	Prepaid card information issuing system, call tariff settling system, and value settling system
US7011250B2 *	2001-12-20	2006-03-14	Matsushita Electric Industrial Co., Ltd.	IC card reader/writer, identification method and program
US7792759B2 *	2002-07-29	2010-09-07	Emv Co. Llc	Methods for performing transactions in a wireless environment
KR100560770B1 *	2003-09-15	2006-03-13	삼성전자주식회사	Contactless integrated circuit card with real-time protocol switching function and card system including the same
US20050222961A1 *	2004-04-05	2005-10-06	Philippe Staib	System and method of facilitating contactless payment transactions across different payment systems using a common mobile device acting as a stored value device
MX2007000546A *	2004-07-15	2007-03-30	Mastercard International Inc	Contactless payment card reader with a frusto-conical operating volume.
US7692532B2 *	2004-07-30	2010-04-06	Reva Systems Corporation	Interference monitoring in an RFID system
KR101059872B1 *	2005-01-03	2011-08-29	삼성전자주식회사	Communication collision prevention protocol using unique identifier
US7274284B2 *	2005-02-04	2007-09-25	Atmel Corporation	Method for RF card detection in a contactless system
US20060273176A1 *	2005-06-03	2006-12-07	Actividentity, Inc.	Blocking contactless personal security device
JP4584082B2 *	2005-09-05	2010-11-17	ソニー・エリクソン・モバイルコミュニケーションズ株式会社	Reader / writer and communication method

* Cited by examiner, † Cited by third party

Cited By (158)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
MX2007000546A *	2004-07-15	2007-03-30	Mastercard International Inc	Contactless payment card reader with a frusto-conical operating volume
WO2006069330A2	2004-12-20	2006-06-29	Proxense, Llc	Biometric personal data key (pdk) authentication
KR101059872B1 *	2005-01-03	2011-08-29	삼성전자주식회사	Communication collision prevention protocol using unique identifier
US7506813B2 *	2005-01-06	2009-03-24	Quad/Graphics, Inc.	Resonator use in the print field
FR2881007B1 *	2005-01-19	2007-02-23	Gemplus Sa	ESTABLISHING COMMUNICATION BETWEEN NON-CONTACT DEVICES
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
CN102968604B *	2005-09-28	2016-06-15	维萨国际服务协会	Reduce the equipment of the interaction time of contactless transaction, system and method
US8985436B2 *	2006-01-18	2015-03-24	Symbol Technologies, Inc.	Peer-to-peer radio frequency communications for management of RFID readers
US8412949B2	2006-05-05	2013-04-02	Proxense, Llc	Personal digital key initialization and registration for secure transactions
US9401063B2 *	2006-06-08	2016-07-26	Mastercard International Incorporated	All-in-one proximity payment device with local authentication
US7958291B2 *	2006-10-10	2011-06-07	Atmel Rousset S.A.S.	Supplemental communication interface

EP2156367B1 *	2006-10-12	2011-11-23	Nxp B.V.	Device, system and method for compensating signal delays in an rfid communication system
US9269221B2	2006-11-13	2016-02-23	John J. Gobbi	Configuration of interfaces for a location detection system and application
US8281998B2	2006-12-07	2012-10-09	Smart Systems Innovations, Llc	Public transit system fare processor for transfers
US8763900B2	2006-12-07	2014-07-01	Smart Systems Innovations, Llc	Mass transit fare processing system
US7991156B2 *	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
CN101617330A *	2006-12-19	2009-12-30	迅城有限公司	The transaction system of in authorising cashless transactions, using
US8052055B2 *	2007-01-31	2011-11-08	Hewlett-Packard Development Company, L.P.	Method and system for perturbing multi-radio-frequency-identification-tag-reader networks to increase interrogation efficiency
US20080244208A1 *	2007-03-30	2008-10-02	Narendra Siva G	Memory card hidden command protocol
US7844558B2 *	2007-05-09	2010-12-07	Atmel Rousset S.A.S.	Managing power and timing in a smart card device
WO2009006635A1 *	2007-07-05	2009-01-08	Mastercard International Incorporated	Method and system for detecting a signal generated by a proximity-based transaction device
US9038914B2 *	2007-07-05	2015-05-26	Mastercard International Corporation	Method and system for simulating a proximity-based transaction device
JP4977543B2	2007-07-20	2012-07-18	日本電気通信システム株式会社	Control device, control system, control method, and control program
JP5260908B2	2007-07-20	2013-08-14	日本電気通信システム株式会社	Control device, communication device, control system, control method, and control program
US20090070691A1 *	2007-09-12	2009-03-12	Devicefidelity, Inc.	Presenting web pages through mobile host devices
US8659427B2	2007-11-09	2014-02-25	Proxense, Llc	Proximity-sensor supporting multiple application services
JP4420296B2 *	2007-11-19	2010-02-24	フェリカネットワークス株式会社	Information processing apparatus, information processing method, and program
US8171528B1	2007-12-06	2012-05-01	Proxense, Llc	Hybrid device having a personal digital key and receiver-decoder circuit and methods of use
US9741027B2 *	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US9251332B2 *	2007-12-19	2016-02-02	Proxense, Llc	Security system and method for controlling access to computing resources
US8838198B2 *	2008-01-09	2013-02-26	Nxp B.V	Evaluating an electromagnetic field strength of an electromagnetic gate apparatus
WO2009102979A2	2008-02-14	2009-08-20	Proxense, Llc	Proximity-based healthcare management system with automatic access to private information
KR101527368B1 *	2008-03-12	2015-06-09	한국전자통신연구원	RFID reader device for situational command retransmission and control method therefor
KR20090097784A *	2008-03-12	2009-09-16	한국전자통신연구원	Rfid interrogator with a collision diagnostics function and method for controlling of the same
US11120449B2	2008-04-08	2021-09-14	Proxense, Llc	Automated service-based order processing
EP2131313A1	2008-06-02	2009-12-09	Gemplus	Method for selecting an application in a mobile wireless communication device in an NFC system and corresponding mobile wireless communication device
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
KR101039449B1 *	2008-11-25	2011-06-07	엘지엔시스(주)	Method for testing PBPR using a damaged type of financial contract information
CN101739583B *	2008-11-26	2013-04-10	國民技术股份有限公司	Radio frequency SIM card, radio frequency card reader and magnetic induction control method for radio frequency communication
US8630584B2	2008-11-26	2014-01-14	Nationz Technologies Inc.	RF SIM card, card reader, and communication method
DE102009009846A1 *	2009-02-20	2010-09-02	Bundesdruckerei Gmbh	Improved card reader for contactless readable cards and method of operating such a card reader

EP2401708A4 *	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
CN101833378 *	2009-03-11	2014-08-13	中兴通讯股份有限公司	Method and terminal for realizing application selection in non-contact electronic payment
JP5169937B2 *	2009-03-25	2013-03-27	株式会社デンソー	Portable machine
US8485436B2 *	2009-04-06	2013-07-16	Mastercard International Incorporated	Simulated contactless identification card reader
US8135354B2 *	2009-06-02	2012-03-13	Symbol Technologies, Inc	Method and system for chopped antenna impedance measurements with an RFID radio
US20110007843A1 *	2009-07-07	2011-01-13	Broadcom Corporation	Low power fm transmitter
CN102048928 *	2009-08-31	2014-03-26	鸿富锦精密工业（深圳）有限公司	Multi-function card reader testing device and method
SK288555B6 *	2009-11-14	2018-05-02	Smk Corporation	Method and system of data transmission from the transponder to the reader, especially in payment solutions with a mobile communication device
CN101742469B *	2009-11-24	2012-05-30	候万春	System and method for controlling mobile phone RFID non-contact transaction attribution
JP5304615B2 *	2009-11-26	2013-10-02	株式会社デンソーウェーブ	Non-contact communication device
US9418205B2	2010-03-15	2016-08-16	Proxense, Llc	Proximity-based system for automatic application or data access and item tracking
CN102215050B *	2010-04-02	2014-03-19	国民技术股份有限公司	Detection method for radio-frequency SIM (Subscriber Identity Module) card collision with low-frequency magnetic communication
CN102468988A *	2010-11-11	2012-05-23	上海华虹集成电路有限责任公司	Device for automatically detecting signal protocol type in international standardization organization/international electrotechnical commission (ISO/IEC) 14443 protocol
CN102479308B *	2010-11-23	2014-10-08	上海华虹宏力半导体制造有限公司	Radio frequency identification anti-collision circuit and realizing method thereof
FR2968804B1	2010-12-13	2013-01-04	St Microelectronics Rousset	METHOD FOR MANAGING THE DIALOGUE BETWEEN EQUIPMENT AND AT LEAST ONE MULTI-APPLICATION OBJECT SUCH AS A CONTACTLESS CHIP CARD AND CORRESPONDING OBJECT
US9265450B1	2011-02-21	2016-02-23	Proxense, Llc	Proximity-based system for object tracking and automatic application initialization
DE102011103740A1 *	2011-05-31	2012-12-06	Smartrac Ip B.V.	A method and arrangement for providing and managing information associated with RFID media in a network
CN102982294B *	2011-09-05	2015-12-02	国民技术股份有限公司	A kind of collision detection method utilizing magnetic two-way communication
US9022427B2	2012-02-29	2015-04-28	Verifone, Inc.	Point of sale device and method for operating same
CN102622565A *	2012-03-06	2012-08-01	无锡儒安科技有限公司	Processing method and device for detecting and preventing electronic tag collision
US8699412B2 *	2012-03-15	2014-04-08	Apple Inc.	Backlight structures and backlight assemblies for electronic device displays
KR101383566B1 *	2012-09-14	2014-02-17	주식회사 티제텍스	Apparatus and method for generating unique identity of radio frequency
US9852419B2 *	2012-09-17	2017-12-26	Capital One Financial Corporation	Systems and methods for providing near field communications
US9405898B2	2013-05-10	2016-08-02	Proxense, Llc	Secure element as a digital pocket
US9323964B2 *	2013-08-20	2016-04-26	Cubic Corporation	Card detection and selection
US9014323B2 *	2013-08-30	2015-04-21	Nxp B.V.	Clock synchronizer for aligning remote devices
CN104636771A *	2013-11-12	2015-05-20	上海华虹集成电路有限责任公司	Non-contact module testing circuit and method
CA2924701A1 *	2013-11-21	2015-05-28	Jet Medical, Inc.	System for facilitating intranasal guidance
CN103761492A *	2013-12-10	2014-04-30	上海动联信息技术股份有限公司	Method of non-contact device for carrying out operation on multiple cards on the basis of 13.56 MHz working frequency
US10509939B2 *	2014-12-24	2019-12-10	Intel Corporation	Method and apparatus for energy harvest from a proximity coupling device

CN104484636A *	2014-12-31	2015-04-01	深圳市科漫达智能管理科技有限公司	Data reading method and device
EP3082061A1	2015-04-13	2016-10-19	Phitek Systems Limited	Communications system for aircraft
CN105668480B *	2015-08-04	2019-05-07	电子科技大学	Ultrahigh frequency RFID signal scanner
US20170200148A1 *	2016-01-07	2017-07-13	Vantiv, Llc	Point of interaction device emulation for payment transaction simulation
US11188893B2 *	2016-01-15	2021-11-30	Mastercard International Incorporated	Access control bypass on mobile for mass transit
CN106934431B *	2017-02-24	2019-09-13	飞天诚信科技股份有限公司	A kind of method and card reader of testing smart card
CN107403118A *	2017-07-06	2017-11-28	上海动联信息技术股份有限公司	The test suite and method of a kind of card reader
EP3499397B1 *	2017-11-29	2021-03-24	ams AG	Method for supplying energy wirelessly by means of radio frequency identification, rfid, and rfid system
CN108021957B *	2017-12-05	2021-07-23	深圳市艾特智能科技有限公司	Anti-collision method and system, readable storage medium and card reading device
CN108038397B *	2017-12-15	2021-01-01	神思电子技术股份有限公司	Test device and method for read-write timing of RFID reader-writer
CN108288008A *	2018-02-08	2018-07-17	飞天诚信科技股份有限公司	A kind of method and device of card activation
US10546644B2	2018-06-21	2020-01-28	Capital One Services, Llc	Systems and methods for secure read-only authentication
CN109033906A *	2018-07-27	2018-12-18	天津科畅慧通信息技术有限公司	A kind of device and method for testing RFID sensitivity
CA3115142A1	2018-10-02	2020-04-09	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10630653B1	2018-10-02	2020-04-21	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10992477B2	2018-10-02	2021-04-27	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
WO2020072550A1	2018-10-02	2020-04-09	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10489781B1	2018-10-02	2019-11-26	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
CA3108917A1	2018-10-02	2020-04-09	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10733564B2	2018-10-02	2020-08-04	Capital One Services, Llc	Systems and methods for establishing identity for order pick up
US10511443B1	2018-10-02	2019-12-17	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10783519B2	2018-10-02	2020-09-22	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
AU2019355110A1	2018-10-02	2021-04-08	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
AU2019355878A1	2018-10-02	2021-02-25	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
KR20210065961A	2018-10-02	2021-06-04	캐피탈 원 서비시즈, 엘엘씨	System and method for cryptographic authentication of contactless card
WO2020072687A1	2018-10-02	2020-04-09	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10771253B2	2018-10-02	2020-09-08	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10607214B1	2018-10-02	2020-03-31	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10505738B1	2018-10-02	2019-12-10	Capital One	Systems and methods for cryptographic authentication of contactless cards

			Services, Llc	
US10582386B1	2018-10-02	2020-03-03	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10566587B1	2018-10-02	2020-02-18	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10579998B1	2018-10-02	2020-03-03	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
KR20210068028A	2018-10-02	2021-06-08	캐피탈 원 서비시즈, 엘엘씨	System and method for cryptographic authentication of contactless card
US10558411B1	2018-10-02	2020-02-04	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
CA3115064A1	2018-10-02	2020-04-09	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10592710B1	2018-10-02	2020-03-17	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10581611B1	2018-10-02	2020-03-03	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10841091B2	2018-10-02	2020-11-17	Capital One Services, Llc	Systems and methods for cryptographic authentication of contactless cards
US10949520B2	2018-10-02	2021-03-16	Capital One Services, Llc	Systems and methods for cross coupling risk analytics and one-time-passcodes
US10909527B2	2018-10-02	2021-02-02	Capital One Services, Llc	Systems and methods for performing a reissue of a contactless card
US10542036B1	2018-10-02	2020-01-21	Capital One Services, Llc	Systems and methods for signaling an attack on contactless cards
US10771254B2	2018-10-02	2020-09-08	Capital One Services, Llc	Systems and methods for email-based card activation
KR20200060623A	2018-11-22	2020-06-01	삼성전자주식회사	Operating method of electronic device performing near field communication functions
US11037136B2	2019-01-24	2021-06-15	Capital One Services, Llc	Tap to autofill card data
US10510074B1	2019-02-01	2019-12-17	Capital One Services, Llc	One-tap payment using a contactless card
US10467622B1	2019-02-01	2019-11-05	Capital One Services, Llc	Using on-demand applications to generate virtual numbers for a contactless card to securely autofill forms
US11120453B2	2019-02-01	2021-09-14	Capital One Services, Llc	Tap card to securely generate card data to copy to clipboard
US10425129B1	2019-02-27	2019-09-24	Capital One Services, Llc	Techniques to reduce power consumption in near field communication systems
US10523708B1	2019-03-18	2019-12-31	Capital One Services, Llc	System and method for second factor authentication of customer support calls
US10438437B1	2019-03-20	2019-10-08	Capital One Services, Llc	Tap to copy data to clipboard via NFC
US10535062B1	2019-03-20	2020-01-14	Capital One Services, Llc	Using a contactless card to securely share personal data stored in a blockchain
US10643420B1	2019-03-20	2020-05-05	Capital One Services, Llc	Contextual tapping engine
US10984416B2	2019-03-20	2021-04-20	Capital One Services, Llc	NFC mobile currency transfer
US10970712B2	2019-03-21	2021-04-06	Capital One Services, Llc	Delegated administration of permissions using a contactless card
US10467445B1	2019-03-28	2019-11-05	Capital One Services, Llc	Devices and methods for contactless card alignment with a foldable mobile device
US10515447B1	2019-06-17	2019-12-24	Capital One Services, Llc	Dynamic power levels in NFC card communications
US10871958B1	2019-07-03	2020-12-22	Capital One Services, Llc	Techniques to perform applet programming

US10713649B1	2019-07-09	2020-07-14	Capital One Services, Llc	System and method enabling mobile near-field communication to update display on a payment card
US10498401B1	2019-07-15	2019-12-03	Capital One Services, Llc	System and method for guiding card positioning using phone sensors
US10885514B1	2019-07-15	2021-01-05	Capital One Services, Llc	System and method for using image data to trigger contactless card transactions
US10733601B1	2019-07-17	2020-08-04	Capital One Services, Llc	Body area network facilitated authentication or payment authorization
US11182771B2	2019-07-17	2021-11-23	Capital One Services, Llc	System for value loading onto in-vehicle device
US10832271B1	2019-07-17	2020-11-10	Capital One Services, Llc	Verified reviews using a contactless card
US10506426B1	2019-07-19	2019-12-10	Capital One Services, Llc	Techniques for call authentication
US10541995B1	2019-07-23	2020-01-21	Capital One Services, Llc	First factor contactless card authentication system and method
US10701560B1	2019-10-02	2020-06-30	Capital One Services, Llc	Client device authentication using contactless legacy magnetic stripe data
US10825040B1	2019-12-23	2020-12-03	Capital One Services, Llc	Method for mapping NFC field strength and location on mobile devices
US11113685B2	2019-12-23	2021-09-07	Capital One Services, Llc	Card issuing with restricted virtual numbers
US10733283B1	2019-12-23	2020-08-04	Capital One Services, Llc	Secure password generation and management using NFC and contactless smart cards
FR3105662B1 *	2019-12-23	2021-11-26	St Microelectronics Rousset	Setting up a transaction in an electronic contactless device
US10885410B1	2019-12-23	2021-01-05	Capital One Services, Llc	Generating barcodes utilizing cryptographic techniques
US10657754B1	2019-12-23	2020-05-19	Capital One Services, Llc	Contactless card and personal identification system
US10664941B1	2019-12-24	2020-05-26	Capital One Services, Llc	Steganographic image encoding of biometric template information on a card
US10853795B1	2019-12-24	2020-12-01	Capital One Services, Llc	Secure authentication based on identity data stored in a contactless card
US10757574B1	2019-12-26	2020-08-25	Capital One Services, Llc	Multi-factor authentication providing a credential via a contactless card for secure messaging
US10909544B1	2019-12-26	2021-02-02	Capital One Services, Llc	Accessing and utilizing multiple loyalty point accounts
US11038688B1	2019-12-30	2021-06-15	Capital One Services, Llc	Techniques to control applets for contactless cards
US10860914B1	2019-12-31	2020-12-08	Capital One Services, Llc	Contactless card and method of assembly
US10886006B1	2020-04-30	2020-12-08	Capital One Services, Llc	Systems and methods for data access control using a short-range transceiver
US11030339B1	2020-04-30	2021-06-08	Capital One Services, Llc	Systems and methods for data access control of personal user data using a short-range transceiver
US10915888B1	2020-04-30	2021-02-09	Capital One Services, Llc	Contactless card with multiple rotating security keys
US10963865B1	2020-05-12	2021-03-30	Capital One Services, Llc	Augmented reality card activation experience
US11063979B1	2020-05-18	2021-07-13	Capital One Services, Llc	Enabling communications between applications in a mobile operating system
US11100511B1	2020-05-18	2021-08-24	Capital One Services, Llc	Application-based point of sale system in mobile operating systems
US11062098B1	2020-08-11	2021-07-13	Capital One Services, Llc	Augmented reality information display and interaction via NFC based authentication
US11165586B1	2020-10-30	2021-11-02	Capital One Services, Llc	Call center web-based authentication using a contactless card

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
MX2007000546A	2007-03-30	Contactless payment card reader with a frusto-conical operating volume.
EP1896863B1	2010-07-07	Rfid communication systems and methods
US9038914B2	2015-05-26	Method and system for simulating a proximity-based transaction device
US8442796B2	2013-05-14	Method and system for simulating a proximity-based transaction device
Murfett	2004	The challenge of testing RFID integrated circuits
US20190266457A1	2019-08-29	Rfid screw specifically for use on eyeglass frames
Proffitt II	2013	Experimental investigation to inform optimal configurations for dynamic near-field passive uhf rfid systems

Priority And Related Applications

Priority Applications (2)

Application	Priority date	Filing date	Title
US58827004P	2004-07-15	2004-07-15	*US Provisional Application*
PCT/US2005/025110	2004-07-15	2005-07-15	Contactless payment card reader with a frusto-conical operating volume

Legal Events

Date	Code	Title	Description
2013-09-30	FA	Abandonment or withdrawal	

Data provided by IFI CLAIMS Patent Services

Patents ITMI981564

NON-VOLATILE MEMORY ABLE TO RUN A PROGRAM INDEPENDENTLY

Classifications

G11C7/00 Arrangements for writing information into, or reading information out from, a digital store

View 2 more classifications

ITMI981564A1
Italy

Find Prior Art Similar

Other languages: Italian

Inventor: Giovanni Campardo

Worldwide applications

1998 IT 1999 EP US

Application IT98MI001564A events

1998-07-09 Application filed by St Microelectronics Srl

1998-07-09 Priority to IT98MI001564A

2000-01-09 Publication of ITMI981564A1

Info: Patent citations (16), Cited by (15), Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Patent Citations (16)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
JPH0738818782 *	1984-03-23	1995-04-26	株式会社日立製作所	Microcomputer configured in LSI
US5444665A *	1985-06-17	1995-08-22	Hitachi, Ltd.	Semiconductor memory device
US5165023A *	1986-12-17	1992-11-17	Massachusetts Institute Of Technology	Parallel processing system with processor array and network communications system for transmitting messages of variable length
US5546343A *	1990-10-18	1996-08-13	Elliott; Duncan G.	Method and apparatus for a single instruction operating multiple processors on a memory chip
US5325500A *	1990-12-14	1994-06-28	Xerox Corporation	Parallel processing units on a substrate, each including a column of memory
JPH04248642A *	1991-01-18	1992-09-04	Kenneth W Iobst	Pim chip for memory integrated circuit and its controlling method
US5687345A *	1992-03-17	1997-11-11	Hitachi, Ltd.	Microcomputer having CPU and built-in flash memory that is rewritable under control of the CPU analyzing a command supplied from an external device
TW231343B *	1992-03-17	1994-10-01	Hitachi Seisakusyo Kk	
JPH06215160A *	1992-08-25	1994-08-05	Texas Instr Inc <Ti>	Method and apparatus for data processing
TW260788B *	1993-09-01	1995-10-21	Philips Electronics Nv	
JPH0845269A *	1994-07-27	1996-02-16	Hitachi Ltd	Semiconductor memory
EP0757356B1 *	1995-07-31	2001-06-06	STMicroelectronics S.r.l.	Flash EEPROM with controlled discharge time of the word lines and source potentials after erase
US6185704B1 *	1997-04-11	2001-02-06	Texas Instruments Incorporated	System signaling schemes for processor and memory module
US6026478A *	1997-08-01	2000-02-15	Micron Technology, Inc.	Split embedded DRAM processor

US6023761A *	1997-08-13	2000-02-08	Visi Technology, Inc.	Method and system for using decompression on compressed software stored in non-volatile memory of an embedded computer system to yield decompressed software including initialized variables for a runtime environment
US6141705A *	1998-06-12	2000-10-31	Microsoft Corporation	System for querying a peripheral device to determine its processing capabilities and then offloading specific processing tasks from a host to the peripheral device when needed

* Cited by examiner, † Cited by third party

Cited By (15)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
US7350056B2 *	2005-09-27	2008-03-25	International Business Machines Corporation	Method and apparatus for issuing instructions from an issue queue in an information handling system
US20070198812A1 *	2005-09-27	2007-08-23	Ibm Corporation	Method and apparatus for issuing instructions from an issue queue including a main issue queue array and an auxiliary issue queue array in an information handling system
JP4984666B2 *	2006-06-12	2012-07-25	ソニー株式会社	Non-volatile memory
US7991158B2	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
US20080244208A1 *	2007-03-30	2008-10-02	Narendra Siva G	Memory card hidden command protocol
US9741027B2 *	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US8432122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US20100033310A1 *	2008-08-08	2010-02-11	Narendra Siva G	Power negotation for small rfid card
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
EP2401708A4 *	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
US9177646B2	2013-05-06	2015-11-03	International Business Machines Corporation	Implementing computational memory from content-addressable memory
US9785545B2 *	2013-07-15	2017-10-10	Cnex Labs, Inc.	Method and apparatus for providing dual memory access to non-volatile memory
CN107548492B *	2015-04-30	2021-10-01	密克罗奇普技术公司	Central processing unit with enhanced instruction set
EP3115109A1 *	2015-07-06	2017-01-11	Base4 Innovation Limited	Droplet sequencing device

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
ITMI981564A1	2000-01-09	NON-VOLATILE MEMORY ABLE TO RUN A PROGRAM INDEPENDENTLY
DE69810096D1	2003-01-23	Non-volatile memory
DE19880311T1	1999-05-12	Non-volatile memory structure
DE60129025D1	2007-08-02	MEMORY AREA ASSIGNMENT IN A FILE SYSTEM FOR DESCRIPTING ANY AREAS
DE69936028D1	2007-06-21	Non-volatile semiconductor memory
DE69822412T2	2002-05-29	Non-volatile semiconductor memory
FR2770328B1	2001-11-23	REMANENT MEMORY POINT
NO20032188L	2003-07-17	A self-adjusting non-volatile memory cell
DE69814450D1	2003-06-17	Check non-volatile memory
NO20002265L	2000-05-15	Programmable access protection in a temporary memory device
DE10085013T1	2002-10-31	Arranging information stored in non-volatile reprogrammable semiconductor memories

DE19882486T1	2000-06-15	Synchronous, non-volatile page mode memory
AT328375T	2006-06-15	IN A SHAPED CROSS DIPOLANTENNE
DE69431735D1	2002-12-19	Non-volatile memory
AU5314101A	2001-10-15	Page mode erase in a flash memory array
DK101250ZT3	2002-04-15	Grating construction in a fluid bed boiler
DE69700328T2	1999-11-04	Compensate for latency in a memory
FR2771839B1	2000-01-28	PROGRAMMABLE AND ELECTRICALLY ERASABLE NON-VOLATILE MEMORY
DE60043453D1	2010-01-14	DUNG IN A SODAKESSEL
DE60038133D1	2008-04-03	Non-volatile memory
DE59913627D1	2006-08-10	Integrated memory
DE69812038D1	2003-04-17	Non-volatile MOS memory
DE59712601D1	2006-05-11	NON-VOLATILE MEMORY CELL
AT517990T	2011-08-15	EFFECTIVE NUCLEAR PROGRAMMING IN MAMMALS
FR2812753B1	2003-01-03	NON-VOLATILE MEMORY POINT

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
IT98MI001564A	1998-07-09	1998-07-09	NON-VOLATILE MEMORY ABLE TO RUN A PROGRAM INDEPENDENTLY

Applications Claiming Priority (3)

Application	Filing date	Title
IT98MI001564A	1998-07-09	NON-VOLATILE MEMORY ABLE TO RUN A PROGRAM INDEPENDENTLY
EP19990202169	1999-07-02	Non-volatile memory capable of autonomously executing a program
US09/349,702	1999-07-08	Non-volatile memory capable of autonomously executing a program

Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

Patents JP2001167187

Subscription contract mediation method and mobile communication network

Abstract

PROBLEM TO BE SOLVED: To mediate more quickly the subscription contacts of various types of electronic commerce services without forcing the great burden on users. SOLUTION: A credit system comprises a mobile station 100, a mobile telephone network 20, a mobile packet communication network 30, the CAT terminals 40a, 40b..., a CAFIS network 50, the credit servers 60A, 60B..., the Internet 70, etc. A credit contact request given from the station 100 is transmitted to one of credit servers via a gateway server 32. When the credit contact is permitted, the credit contract information is transmitted from one of credit servers to the station 100 via the server 32 and stored in the station 100.

Classifications

- H04W88/02 Terminal devices

View 31 more classifications

JP2001167187A

Japan

Find Prior Art Similar

Other languages: Japanese

Inventor: Takeshi Natsuno, [redacted]

Worldwide applications

1999 JP 2000 IL CA CN AU SN WO KR CN PL US HU EP BR TW 2001 IL NO 2002 HK

Application JP35226599A events

1999-12-10	Application filed by NTT Docomo Inc, [redacted]
1999-12-10	Priority to JP35226599A
2000-12-07	Priority claimed from PCT/JP2000/008858A
2000-12-07	Priority claimed from US09/890,830
2000-12-07	Priority claimed from CA2549387A
2001-06-22	Publication of JP2001167187A
Status	Pending

Info: Patent citations (12), Cited by (23), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (16)

Hide Dependent

[Claims]

1. 1. A mobile communication terminal connected to a network of a contract institution server connected to a network of a user of a mobile communication terminal accommodated in the mobile communication network to mediate a subscription contract for electronic commerce. Receiving a request for the subscription from the user at the mobile communication terminal, and inputting information required for the subscription in response to the request for the subscription at the mobile communication terminal. Prompting the user, and transmitting information required for the subscription entered from the user to the mobile communication terminal to a server of the contracting institution via the mobile communication network. Subscription agreement mediation method.

2. 2. The method according to claim 1, further comprising the step of transmitting information on whether or not to subscribe to the request for the subscription to the mobile communication terminal via the mobile communication network. In this case, the information necessary for e-commerce after the subscription transmitted from the server of the contract organization,
A subscription contract comprising: transmitting to the mobile communication terminal via the mobile communication network; and receiving and storing information required for the electronic commerce after the subscription at the mobile communication terminal. Mediation method.

3. 3. The subscription mediation method according to claim 1, wherein the step of prompting the user at the mobile communication terminal to input information required for the subscription is performed by the user so that the user inputs the required information. Transmitting input screen information to the mobile communication terminal via the mobile communication network; receiving the input screen information at the mobile communication terminal; and displaying the input screen indicated by the received input screen information. Displaying a subscription contract mediation method.

4. 4. The subscription contract mediation method according to claim 3, wherein the input screen information is stored in a server of the contract organization.

5. 5. The subscription mediation method according to claim 3, wherein the input screen information is stored in a relay device that relays data exchange between the mobile communication terminal and a server of the contract organization. Subscription agreement mediation method characterized by the above-mentioned.

6. 6. The subscription mediation method according to claim 1, further comprising the step of performing user authentication of the user.

7. 7. The method of claim 2, wherein the step of transmitting information necessary for the electronic commerce to the mobile communication terminal via the mobile communication network is transmitted from a server of the contract organization. Storing the information necessary for the electronic commerce; requesting the mobile communication terminal to acquire the information necessary for the electronic commerce in accordance with the information on whether the subscription is possible; Transmitting necessary information for the electronic commerce to the mobile communication terminal via the mobile communication network when there is a request for acquisition of important information. Method.

8. 8. The subscription agreement intermediation method according to claim 2, further comprising the step of judging whether the subscription agreement is valid or not based on information necessary for the subscription agreement input by the user. Subscription mediation method.

9. 9. The subscription mediation method according to claim 8, wherein the server of the contract institution determines whether the subscription is acceptable.

10. 10. The subscription contract intermediation method according to claim 8, wherein a relay device that relays data transfer between the mobile communication terminal and a server between the contract machines determines whether the subscription contract is acceptable or not. Characteristic subscription mediation method.

11. 11. The subscription mediation method according to claim 2, wherein all the steps are executed by one communication

12. 12. The subscription contract intermediation method according to claim 2, wherein: a step of receiving the request for the subscription contract from the user; and a step of prompting the user to input information necessary for the subscription contract at the mobile communication terminal. Transmitting the information necessary for the subscription to the server of the contracting organization via the mobile communication network; and transmitting the information on whether or not the subscription is possible via the mobile communication network to the mobile communication terminal. Transmitting the information necessary for the electronic commerce after the subscription to the mobile communication terminal via the mobile communication network; receiving the information necessary for the electronic commerce after the subscription, and storing the information. And a communication performing the steps of performing the above steps is separated from each other.

13. 13. The subscription mediation method according to claim 1, wherein said subscription is a credit contract.

14. 14. The subscription mediation method according to claim 1, wherein said mobile communication terminal is a mobile phone.

15. 15. A mobile communication network for relaying data exchange between a mobile communication terminal and a server of a contract organization that concludes a subscription contract for e-commerce with a user of the mobile communication terminal, According to the request of the subscription from the mobile communication terminal,
Means for transmitting to the mobile communication terminal input screen information for prompting input of information necessary for the subscription contract, and information necessary for the subscription contract input to the mobile communication terminal by the user from the mobile communication terminal. Means for receiving and transmitting to a server of the contracting institution.

16. 16. The mobile communication network according to claim 15, further comprising: means for receiving, from a server of the contract organization, information on whether or not the request for the subscription can be accepted, and transmitting the information to the mobile communication terminal; Means for receiving information required for electronic commerce after the subscription from the server of the contract organization and transmitting the information to the mobile communication terminal.

Description

DETAILED DESCRIPTION OF THE INVENTION

[0001]

BACKGROUND OF THE INVENTION 1. Field of the Invention The present invention relates to a subscription contract mediation method for mediating a contract when subscribing to an electronic commerce service concluded between a user and a contract institution, and to execute the method. It relates to a mobile communication network.

[0002]

2. Description of the Related Art When a credit contract is concluded with a credit company or a deposit account is opened at a financial institution, a user usually first goes to a store of a contract institution such as a credit company (or by mail) to make a necessary payment. Submit the application form with the required items. After receiving the application for the contract, the contracting organization performs a predetermined examination and concludes the contract, creates a credit card or the like for the user to use the e-commerce service, and mails it to the user.

[0003]

As described above, a user who wants to apply for a subscription to various electronic commerce services must go to the store of the contract organization (or mail the application form to the contract organization). Must be done). In addition, a process of creating these cards (for example, a process of imprinting a name or a card number on a credit card and storing predetermined magnetic information in a magnetic stripe on the card) requires a certain time. In addition, these cards are generally delivered to the user by registered mail, which, in addition to a certain number of days for mailing, takes extra time if the user is not home at the time of mail arrival. Therefore, it takes a certain number of days from when the user completes the application for the subscription contract to when he or she obtains a credit card or the like, and it has been difficult to meet the user's need to obtain the card immediately. The present invention has been made in view of the circumstances described above, and has as its object to mediate the subscription contract more quickly without imposing a large burden on the user in various electronic commerce service subscription contracts. .

[0004]

According to an aspect of the present invention, there is provided a mobile communication system in which a contract institution server is accommodated in a mobile communication network via a mobile communication network connected to the network. A method for mediating a subscription contract for electronic commerce between a user of a communication terminal and the contract organization, the method comprising: receiving a request for the subscription contract from the user at the mobile communication terminal; Prompting the user at the mobile communication terminal to input information necessary for the subscription in response to a request for a contract, and transmitting the information required for the subscription entered by the user to the mobile communication terminal, Transmitting to a server of the contract organization via a communication network.

According to a second aspect of the present invention, in the subscription mediation method according to the first aspect, a step of transmitting to the mobile communication terminal via the mobile communication network information on whether or not the subscription to the subscription request has been made, Transmitting, when the subscription contract is approved, information necessary for electronic commerce after subscription transmitted from a server of the contract organization to the mobile communication terminal via the mobile communication network, Receiving and storing information necessary for the electronic commerce after the subscribing at the terminal.

According to a third aspect of the present invention, in the subscription agreement mediation method of the first aspect, the step of prompting the user to input information required for the subscription at the mobile communication terminal includes the step of: Transmitting input screen information for inputting information to the mobile communication terminal via the mobile communication network; and receiving the input screen information at the mobile communication terminal; and receiving the input screen information. And a step of displaying an input screen indicated by the following.

According to a fourth aspect of the present invention, there is provided the subscription mediation method according to the third aspect, wherein the input screen information is stored in a server of the contract organization. Is what you do.

According to a fifth aspect of the present invention, in the method of the third aspect, the input screen information relays data exchange between the mobile communication terminal and a server of the contract organization. Is provided.

According to a sixth aspect of the present invention, there is provided the subscription mediation method according to the first aspect, further comprising a step of performing user authentication of the user.

[0010] According to a seventh aspect of the present invention, in the subscription contract intermediation method according to the second aspect, the step of transmitting information necessary for the electronic commerce to the mobile communication terminal via the mobile communication network includes the contracting institution. Storing information necessary for the electronic commerce transmitted from the server of the mobile communication terminal; requesting the mobile communication terminal to acquire information necessary for the electronic commerce in accordance with the information on whether the subscription is possible; And transmitting a stored information necessary for the electronic commerce to the mobile communication terminal via the mobile communication network when there is a request for obtaining information necessary for the electronic commerce. A feature of the present invention is to provide a subscription mediation method.

[0011] The invention according to claim 8 is the subscription contract mediation method according to claim 2, further comprising a step of judging whether the subscription contract is valid or not based on information necessary for the subscription contract input by the user. The present invention provides a subscription mediation method characterized by performing the following.

[0012] According to a ninth aspect of the present invention, there is provided the subscription mediation method according to the eighth aspect, wherein the server of the contract institution determines whether or not the subscription is permitted. It is.

According to a tenth aspect of the present invention, in the subscription contract intermediation method according to the eighth aspect, a relay device for relaying data exchange between the mobile communication terminal and a server between the contract machines is provided. It is an object of the present invention to provide a subscription mediation method characterized by judging whether or not it is possible.

According to an eleventh aspect of the present invention, there is provided the subscription mediation method according to the second aspect, wherein all the steps are executed by one communication.

According to a twelfth aspect of the present invention, in the subscription contract intermediation method of the second aspect, a step of receiving the request for the subscription from the user, and inputting information required for the subscription in the mobile communication terminal. The step of prompting the user, the step of transmitting the information required for the subscription to the server of the contracting organization via the mobile communication network, and the step of transmitting Transmitting the information necessary for the electronic commerce after the subscription to the mobile communication terminal via the mobile communication network; and transmitting the information necessary for the electronic commerce after the subscription. The method of receiving and storing information is separated from the communication that performs the steps of subscribing.

The invention according to claim 13 is the invention according to claims 1 to 12
The method of claim 1, wherein the subscription is a credit contract.

The invention according to claim 14 is the invention according to claims 1 to 12
The method of claim 1 wherein the mobile communication terminal is a mobile phone.

According to a fifteenth aspect of the present invention, there is provided a mobile communication system for relaying data transfer between a mobile communication terminal and a server of a contract organization which concludes a subscription contract for electronic commerce with a user of the mobile communication terminal. A means for transmitting, to the mobile communication terminal, input screen information for prompting input of information necessary for the subscription contract, in response to a request for the subscription contract from the mobile communication terminal; Means for receiving, from the mobile communication terminal, information required for the subscription contract input to the mobile communication terminal, and transmitting the information to a server of the contract organization. .

According to a sixteenth aspect of the present invention, in the mobile communication network according to the fifteenth aspect, means for receiving, from a server of the contract organization, information on whether or not the subscription to the subscription request is possible, and transmitting the information to the mobile communication terminal Means for receiving information necessary for the electronic commerce after the subscription from the server of the contract organization and transmitting the information to the mobile communication terminal when the subscription contract is approved. It provides a net.

[0020]

DETAILED DESCRIPTION OF THE INVENTION [1. Configuration] [1-1. Configuration of Mobile Station] FIG. 1 is a block diagram showing a configuration of a mobile station 100 used in one embodiment of the present invention. The mobile station 100 includes a transmitting / receiving unit 110, a control unit 12
0, user interface 130, data input / output terminal 1
40, a magnetic writer 150, a magnetic stripe 160, and the like.

The transmitting / receiving unit 110 performs wireless communication with a base station of a mobile communication network that provides mobile telephone communication and mobile packet communication.

The control unit 120 controls each unit of the mobile station 100, and includes a CPU 121, a program R
OM122, ROM123 for credit, RAM124
And so on. Here, the mobile station 100 has a "call mode" for making a call using a mobile communication network,
At least two types of modes can be set, including a "packet communication mode" for performing packet communication using a mobile packet communication network.
The control unit 120 controls each unit of the mobile station 100 according to the setting status of each of these modes.

The RAM 124 is used as a work area for the CPU 121 and a user data area for telephone directory data and the like.

The credit ROM 123 stores information on attributes of a credit contract concluded between the user and the credit company (hereinafter referred to as credit contract information). This credit contract information is given from the credit company to the user, and includes, for example, the name of the credit company with which the user has made a credit contract, the URL of the server of the credit company (described later), the credit number (given for each credit contract). Identification number, usually
16

Digits), credit contract expiration date, user name, and the like. When the user has a plurality of credit contracts with a plurality of credit companies, credit contract information relating to the plurality of contracts is stored in the ROM 123 for credit.

The credit ROM 123 can be accessed only from a dedicated ROM reader / writer or a dedicated server of a credit company. RO for credit from dedicated ROM reader / writer
When accessing M123, the data input / output terminal 14
9, the write information to the credit ROM 123 is sent from the ROM reader / writer connected to the control unit 120 to the control unit 120. The control unit 120 checks the validity of the ROM reader / writer that has accessed the RO
The contents are written to M123. When accessing the credit ROM 123 from a dedicated server, the server writes information to the credit ROM 123 to the control unit 120 via a network such as a mobile packet communication network. Then, after confirming the validity of the accessed server, the control unit 120 writes the contents into the credit ROM 123. In addition,
When the control unit 120 detects a means other than the above that attempts to access the credit ROM 123, the control unit 120 performs processing for disabling the mobile station 100 itself.

A control program is stored in the program ROM 122, and the CPU 121 reads out the control program and executes various control processes. The control programs include various programs described below, in addition to programs related to the call function that the mobile station 100 normally has. This control program includes document data browsing software (so-called browser). CP
U121 loads the browser into the program ROM 122.
By reading and executing the data, it is possible to obtain HTML-format data from various information providing servers connected to the Internet via a gateway server (described later). The mobile station 100 acquires HTML data by transmitting an acquisition request designating a URL of a resource to the information providing server via the gateway server, and correspondingly transmitting the HTML data transmitted from the information providing server. The processing is completed by storing the data in the RAM 124.

In this control program, credit contract information is stored in the ROM 123 for credit,
Alternatively, a program for reading, changing, or deleting credit contract information stored in the credit ROM 123 is included.
The control program further includes a credit ROM by controlling the magnetic writer 150.
A program for writing and erasing the credit contract information read out from the magnetic stripe 160 to the magnetic stripe 160 and a program for giving the credit contract information read out from the credit ROM 123 to the mobile communication network are included.

The control program includes the mobile station 1
When the power of 00 is turned on, a program for transmitting the power on, the identification number of the mobile station 100 (hereinafter referred to as transmission information) using a specific channel is included.

Further, as described above, this control program contains the credit ROM 123 by unauthorized means.
A program for making the mobile station 100 itself unusable when an act of trying to access is detected.

The magnetic writer 150 transmits the credit contract information provided from the control unit 120 to the magnetic stripe 160.
Or the credit contract information on the magnetic stripe 160 is erased.

The magnetic stripe 160 is similar to a magnetic stripe widely used in current credit cards. Therefore, the credit contract information written on the magnetic stripe 160 is a magnetic stripe reading terminal (so-called CAT terminal) which is currently widely used.
Can be read. This magnetic stripe 160
is provided on a plastic card (hereinafter referred to as a magnetic card 161) housed in the mobile station 100. The magnetic card 161 is driven in accordance with a predetermined key operation on a keypad, which will be described later, and is normally stored in the mobile station 100. However, during credit shopping, the magnetic stripe 160 is used. The part is exposed from the mobile station 100 to the outside.

The user interface 130 includes a liquid crystal display 132 for displaying characters and the like, a keypad for the user to perform various input operations, a microphone and a speaker for the user to talk. The keypad may be provided with a "card storage / exposure key" for operating storage / exposure of the magnetic stripe 160,
Alternatively, the magnetic stripe 160 may be stored and exposed by a predetermined key operation using an existing numeric keypad.

FIG. 2 is a perspective view showing the appearance of the mobile station 100 provided with the card storage / exposure key 131. FIG. 4A shows the mobile station 1 in which the magnetic card 161 is stored.
The mobile station 100 is provided with a throttle 101 for storing and exposing the magnetic card 161. FIG. 2B shows the mobile station in a state where the magnetic stripe 160 of the magnetic card 161 is exposed to the outside. By the above-mentioned predetermined operation of the user,
The state shown in FIG. 7A and the state shown in FIG. Note that a signature field for the user is provided on the back surface of the magnetic card 161 in the same manner as a conventional credit card.

[1-2. Configuration of Credit System] FIG.
1 is a block diagram showing a configuration of a credit system using a mobile station 100. This credit system includes a mobile station 100, a mobile telephone network 20, a mobile packet communication network 3
0, CAT terminals 40a, 40b..., CAFIS (Cr
edit and FinanceInformation System) network 50, credit servers 60A, 60B ..., Internet 7
0, user store servers 80C, 80D, etc.

A user who has signed a credit contract
The mobile station 100 is owned. The mobile station 100 is connectable to a mobile telephone network 20 and a mobile packet communication network 30.

The mobile telephone network 20 is a network for providing a general call service using a mobile station.
0 can receive the service through the mobile telephone network 20. The mobile telephone network 20 includes a number of base stations 31 installed at predetermined intervals in a communication area, an exchange (not shown) for performing a circuit switching service, a control station 33 for controlling the network, and a communication line (see FIG. (Not shown). The control station 33 is provided with a subscriber database 331 for storing various information on subscribers who use communication services. The base station 31, the exchange, the control station 33, the communication line and the like are shared with the mobile packet communication network 30.

Here, the subscriber database 331 will be described. FIG. 4A shows the subscriber database 331.
FIG. As shown in the figure, the subscriber database 331 stores, for each "subscriber" of the mobile telephone network 20 (that is, the user of the mobile station 100), the mobile station 10.

5 "phone number", "name", "sex", "date of birth"
In addition, various data such as mobile station 100 and use prohibition information indicating prohibition of credit use are stored. In addition,
A use prohibition flag is registered in the use prohibition information column of the mobile station 100 and a user whose credit use is prohibited.

Referring back to FIG. 3, the configuration of the credit system will be described. In the figure, the mobile packet communication network 30
includes a gateway server 32 in addition to the above-described base station 31, switching center, control station 33, communication line, and the like. The gateway server 32 is a computer system provided in a mobile packet gateway relay exchange for interconnecting the mobile packet communication network 30 with another network such as the Internet 70, and converts different communication protocols among a plurality of networks. I do. In the present embodiment, a mutual conversion between a transmission protocol for the mobile packet communication network 30 and TCP / IP which is a standard communication protocol of the Internet 70 is performed. Also, this gateway server 32
is the mobile station 100, the credit servers 60A, 60B
Controls various data distribution processes performed between the store servers 80C, 80D, and so on.

Here, the gateway server 32 will be described. FIG. 5 is a block diagram showing the configuration of the gateway server 32. This gateway server 32
It comprises a control unit 301, a subscriber information management unit 302, a data distribution management unit 303, and the like. The control unit 301
It controls each unit of the gateway server 32 and functions as an interface between networks, such as performing protocol conversion between the mobile packet communication network 30 and another network such as the Internet 70. Further, the control unit 301 is, for example, an SSL (Secure Sockets L.
ayer), thereby protecting the contents of communication with the credit servers 60A, 60B,... and the user store servers 80C, 80D,. Further, when the user uses a predetermined service of mobile packet communication, the control unit 301 performs user authentication of a user who uses the mobile station 100 that has accessed the gateway server 32. This user authentication is performed by password collation described later.

The subscriber information management unit 302 stores and manages a subscriber registration information file 304 obtained by referring to the subscriber database 331 of the control station 33. The configuration of the subscriber registration information file 304 will be described later.

The data distribution management unit 303 is provided between the users of the plurality of mobile stations 100, between the user of the mobile station 100 and a user of another network such as the Internet 70, or between the user of the mobile station 100 and the credit server 60A. ,
.. And the store servers 80C, 80D,...
For example, the data distribution management unit 303 receives a communication request from the mobile station 100, the credit servers 60A, 60B, and the like, and transmits the communication contents to the destination of the communication request.
Alternatively, the data distribution management unit 303 temporarily stores the received communication content and notifies the terminal of the destination of the communication request (for example, the mobile station 100) that the communication content is stored. When receiving a communication content acquisition request from the terminal, the data distribution management unit 303 transmits the stored communication content to the terminal. For this purpose, the data distribution management unit 303 has a memory (not shown) for temporarily storing communication contents therein. The memory also stores service menu screen information transmitted to the mobile station 100 and used to display a menu of various service items on the liquid crystal display 132 of the mobile station 100. The service menu screen information is HTML format data, and the data of each service item includes the URLs of various servers that execute the respective services. Further, in this memory, store information where credit shopping is possible via the mobile packet communication network 30 is stored. The store information is also HTML format data, and the data of each store includes the URL of the server of each store. The user store information is transmitted to the mobile station 100 and displayed on the liquid crystal display 132 of the mobile station 100. When a user requests a specific service using the mobile station 100, the mobile station 100 transmits a URL included in the data of the service item to the gateway server 32, and the gateway server 32 performs the service based on the received URL. To the server that runs. Further, when the user is in the mobile packet communication network 3
Also, when performing a credit shopping at a certain store via the Internet, the URL of the HTML format data is similarly used.

Here, the subscriber registration information file 304 will be described. FIG. 4B is a diagram showing a data format of the subscriber registration information file 304. As shown in FIG. 2B, the subscriber registration information file 304 contains the "telephone number" of the mobile station 100 for each "subscriber" of the mobile packet communication network 30 (that is, the user of the mobile station 100). "Name", "Gender", "Date of birth", data and e-mail delivered to the user are stored in the data distribution management unit 30.
3 stores various data such as a "storage location" indicating where the information is stored, and a "password" previously registered by the user for application. Control unit 3 of gateway server 32
in step 31, user authentication is performed by comparing a password entered by the user into the mobile station 100 with a password stored in the subscriber registration information file 304.

Referring back to FIG. 3, the configuration of the credit system will be described. In FIG. 3, a number of CAT terminals 40
are installed in a store, a cash dispenser (CD), or the like. The CAT terminals 40a, 40
are provided with a magnetic reader (not shown),
It is possible to read the credit contract information recorded on the magnetic stripe 160 of 00. The CAT terminals 40a, 40b,... Are provided with an input interface (not shown), and a store clerk or the like can input predetermined information (for example, a purchase amount) from the input interface. The CAT terminals 40a, 40b ...
is connected to a dedicated network called the CAFIS network 50 and provides the CAFIS network 50 with the credit contract information read from the magnetic stripe 160 and the information such as the amount of money used, the date of use, and the shop used for credit shopping (Hereinafter, the CAT terminals 40a, 40b,.
The information given to the AFIS network 50 is called credit information).

The CAFIS network 50 has a large number of CAT terminals 4.
0a, 40b ... and credit servers 60A, 60B
.. Are connected. The CAFIS network 50 is a network connecting credit companies, distribution companies, and financial institutions at a nationwide level, and a CAFIS control center (not shown) controls the inside of the network. This CAFI
The S network 50 transfers various credit information generated by the user's credit shopping, cashing, etc. to the credit server 6 which is the credit contractor.
0A, 60B,... Or credit shopping availability information from any of the credit servers 60A, 60B,.
b.

The credit servers 60A, 60B... Are installed in each credit company, and the CAFIS network 50
And the Internet 70. The credit servers 60A, 60B,... Store user attribute information, credit contract information, and the like, and the credit database 62A, which stores contract user credit use history and fund settlement information. 62B ...

Here, the user databases 61A, 61
B and the credit databases 62A, 62B
・ ・ Is explained. 6A is a data format diagram of the user databases 61A, 61B,..., And FIG.
It is a data format figure of 2B ... Figure (A)
The user databases 61A, 61B

, The user databases 61A, 61B,.

・ The "Name", "Age", "Address",
User attribute information such as "phone number", "workplace", "annual income", "credit number" related to each credit contract,
Credit contract information such as "expiration date" and "use limit" is stored. This user attribute information is given by an application from the user at the time of the credit contract,
It is changed at any time by a change application from the user. The credit contract information is information that the credit company grants for each contract at the same time as when the credit contract is concluded, and part of the information is updated each time the expiration date elapses. Also,
As shown in FIG.
A, 628 . Include credit usage history of each user such as "usage date", "usage store", and "usage amount" of credit shopping and cashing, and "settlement amount" for each "settlement month". Is stored. The credit use history ("use date", "use shop" and "usage amount") is obtained from the CAT terminals 40a, 40b... And the use shop servers 80C, 80D.
A, 60B... The credit servers 60A, 60B,... Calculate the "payment amount" for each "payment month" based on the given "use date" and "use amount" information, and store them as fund settlement information. .

The credit servers 60A, 60B,.
・ The main functions of the credit contract (contract conclusion, renewal,
Change, cancellation, etc.), credit use determination, accumulation of various information related to credit contracts and credit use, fund settlement related to credit use, provision of various information to users, etc. Each function will be described in detail.

The credit servers 60A, 60B,...
Has previously stored an input screen given to the mobile station 100 for a credit contract, a change screen given to the mobile station 100 for a contract change, and upon receiving a credit contract request or the like from the mobile station 100, An input screen or the like corresponding to the request is displayed on the Internet 70 and the gateway server 3.
2 and the like to the mobile station 100.

The credit servers 60A, 60B
Create and store contract update candidate user files 601A, 601B,... For contract update processing.
The contract update candidate files 601A, 601B,...
Stores information about a user whose contract is about to be renewed.

Here, the contract update candidate user file 60
1A, 601B,... Will be described. FIG. 6 (C)
The contract update candidate user files 601A, 601B
・ ・ The data format diagram is shown. As shown in FIG. 7C, contract update candidate user files 601A and 601
B... Store data such as "name", "credit number", "telephone number", and "expiration date" of each user. The credit servers 60A, 60B ...
The "expiration date" of the credit contract stored for each user in the user database 61A is set to a fixed period (for example, 2
.. Every four hours) to extract users whose expiration date of the credit contract is approaching (for example, within one week until the expiration date) and to extract information on the extracted users from the user databases 61A, 61B, and so on. Obtain the contract update candidate user files 601A, 601B
・ ・ It is stored in

Again, the credit servers 60A, 60B
・ ・ Return to explanation. Credit server 60A, 60B
.., Have previously stored examination conditions for determining whether or not to accept a credit contract, receive contents input by the user from the mobile station 100 according to the input screen from the mobile station 100, and perform credit based on the input contents and the examination conditions. An examination is conducted to determine whether the contract is valid. And the credit server 60A, 60B
.., If the result of the examination indicates that a credit contract is permitted, generate credit contract information to be stored in the magnetic stripe 160 of the mobile station 100 and give it to the mobile station 100;
Also, user attribute information and credit contract information relating to the contract are stored in the user databases 61A, 61B,.

When the user performs credit shopping or the like, the credit servers 60A and 60B
Are credit information provided from the CAT terminals 40a, 40b (or the user store servers 80C, 80D,...) And the user databases 61A, 61B..
It is determined whether or not the generated credit shopping is valid using various information stored in the CAT terminals 40a, 40b,... (Or as a credit availability information). User store server 80C,
80D ...). And the credit server 6
0A, 60B,... Store the data of the generated credit shopping or the like in the credit databases 62A, 62B.
... is stored.

The credit servers 60A, 60B
. notifies the financial institution with the credit debit account of the fund settlement information via the CAFIS network 50,
Perform credit debit processing.

Further, the credit servers 60A, 60B
. Obtains desired information of the user from information stored in the user databases 61A, 61B... And the credit databases 62A, 62B.
It is provided to the mobile station 100 via the Internet 70 and the mobile packet communication network 30.

The credit servers 60A, 60A
8 ... have an encryption communication algorithm such as SSL (Secure Sockets Layer), so that the gateway server 32 and the store server 80C, 8
0D etc. are protected.

Are servers that provide a so-called virtual shop where the user can perform online shopping. .. Store the shopping screen information displayed on the mobile station 100 as HTML format data. The shopping screen information includes information on a product to be sold to the user (for example, a product name, a product description, a sales price, and the like).
.. Receive the credit shopping request from the user's mobile station 100,
... The mobile station 100 is provided with shopping screen information, and performs processing related to the credit shopping in cooperation with one of the credit servers 60A, 60B,. In addition, the user store servers 80C, 80D,...
For example, it has an encryption communication algorithm such as SSL (Secure Sockets Layer), so that the gateway server 32 and the credit servers 60A, 60B,.

・ The contents of communications with other parties are protected. [2. Operation] Next, the operation of the present embodiment will be described by dividing it into the following operation modes 1. At the time of credit contract 2-. At the time of credit shopping at stores 2- 2. At the time of credit shopping via the mobile packet communication network 30 3. When renewing credit contract When changing the credit contract 5. When canceling credit contract 6. When use of mobile station 100 and credit is prohibited. When referencing credit usage history, etc.

[2-1. Operation at the Time of Credit Contract] FIGS. 7 and 8 are flowcharts showing the operation when a user makes a credit contract using the mobile station 100. FIG. (A) to (J) are diagrams of screens displayed on the liquid crystal display 132 of the mobile station 100 at the time of a credit contract,
FIGS. 7A to 7J are arranged in chronological order corresponding to the operations at the time of the credit contract shown in FIGS. Hereinafter, the operation at the time of a credit contract will be described with reference to FIGS. 7, 8, and 9.

First, in step SP101, the user makes a call to the gateway server 32 with a predetermined telephone number and requests the start of the packet communication mode.

In step SP102, the gateway server 32 starts the packet communication mode for the user by receiving the packet communication mode start request, and displays the service menu screen information stored therein to the mobile station 100. Send.

At step SP103, the mobile station 100
Receives the service menu screen information and displays the service menu screen on the liquid crystal display 132. FIG.
(A) is a diagram of a screen displayed on the mobile station 100 at this time.

In step SP104, the user selects a desired service from the displayed service menu screen by key operation. Here, on the screen shown in FIG. 9A, the user moves the cursor over "credit" and selects it. Then, the mobile station 100 transmits the selected service request (here, "credit") to the gateway server 32.

In step SP105, the gateway server 32 transmits service menu screen information indicating more detailed service contents to the mobile station 100 in response to the received service request.

In step SP106, the mobile station 100
Receives the detailed service menu screen information and displays the service menu screen on the liquid crystal display 132. FIG. 9B is a diagram of a screen displayed on mobile station 100 at this time.

At step SP107, the user selects a desired service from the displayed detailed service menu screen by key operation. Here, FIG. 9 (B)
On the screen shown in FIG. 7, the user moves the cursor on "credit contract" and selects it. Then, the mobile station 100 transmits the selected detailed service request (here,
"Credit contract") to the gateway server 32. The above-described service menu screen is transmitted to the mobile station 100 a plurality of times until the user finally specifies a desired service.

At step SP108, the gateway server 32 receives the detailed service request, and transmits to the mobile station 100 password input screen information for the user to input a password.

In step SP109, the mobile station 100
Receives the password input screen information, and the liquid crystal display 132 displays the password input screen. The user
The password registered in advance in the gateway server 32 is entered in the password entry field 135 on the password entry screen. FIG. 9C is a diagram of a password input screen displayed on mobile station 100 at this time. The user
Enter the password in the password entry field, move the cursor and select "Execute".

At step SP111, the mobile station 100
Transmits the password information input by the user to the gateway server 32.

At step SP113, the gateway server 32 receives the password information.

At step SP115, the gateway server 32 determines whether the password received from the mobile station 100 is
The mobile station 10 stored in the subscriber information management unit 302
User authentication is performed by checking the password of the user 0.

In step SP117, it is determined whether or not the user is authenticated as a result of the user authentication.

If it is determined in step SP117 that the user is a valid user, the process proceeds to step SP119, where the gateway server 32 sends a request to the mobile station 100 in response to a final service request (credit contract request) from the user. The displayed next screen information is transmitted to the mobile station 100.

On the other hand, if it is determined in step SP117 that the user is not a valid user, the process proceeds to step S117.
Proceeding to P121, the gateway server 32 transmits to the mobile station 100 a service refusal notice indicating that a service request (credit contract request) from the user is not accepted.

Then, in step SP123, the mobile station 100 receives the information transmitted from the gateway server 32.

Next, in FIG. 8, step SP125
Then, the next screen received by the mobile station 100 is displayed on the liquid crystal display 132. In this case, the credit company name to which the user can make a contract is displayed on the liquid crystal display 132. FIG. 9D is a diagram of a screen displayed on mobile station 100 at this time. Note that, when the mobile station 100 receives the service unavailable notification, the mobile station 100 displays the notification on the liquid crystal display 132 (not shown), and the process ends.

At step SP126, the user selects a desired credit company from the displayed credit companies by key operation. In other words, the user can see FIG.
A cursor is moved to a desired credit company on the screen shown in (D), and the credit company is selected by a predetermined key operation. Here, for example, it is assumed that the credit company A is selected.

At step SP127, the mobile station 100
Sends the selected credit company name (Company A) and the URL of the credit server 60A of Company A to the gateway server 3
Send to 2.

At step SP129, the gateway server 32 receives the credit company name (company A) and the URL, and transmits a credit contract request to the credit server 60A based on the received URL. At this time, the gateway server 32 protects the content transmitted to the credit server 60A with SSL. In the following description of various operations, the gateway server 3

2. When communication is performed between each of the credit servers 60A, 608,... And the user store servers 80C, 80D,.

At step SP131, the credit server 60A receives a credit contract request from the gateway server 32.

At step SP133, the credit server 60A transmits the information (eg, name, age, date of birth, address, telephone number, work location,
Screen information for input for the user to input annual income, password, etc.) is transmitted to the Internet 70 to the mobile station 100 as a destination.

At step SP135, the gateway server 32 receives the input screen information from the credit server 60A and transmits it to the mobile station 100.

At step SP137, the mobile station 100
Receives the input screen information from the gateway server 32 and displays the input screen on the liquid crystal display 132.
FIG. 9E is a diagram of a screen displayed on mobile station 100 at this time.

At step SP139, the user inputs necessary information while referring to the input screen displayed on the liquid crystal display 132. That is, the user can use FIG.
On the screen shown in (E), necessary information is entered in each input field. Items to be input by the user include various items such as "telephone number" and "workplace" in addition to "name", "date of birth" and "address" shown in FIG. The other items are sequentially displayed on the liquid crystal display 132 when the user scrolls down the screen.

In step SP141, the mobile station 100
Transmits the input content (hereinafter, referred to as input information) to the gateway server 32.

At step SP143, the gateway server 32 receives the input information, and
Send to A.

At the same time, in step SP145, the gateway server 32 sends a transmission completion notification indicating that the input information has been transmitted to the credit server 60A.
Send to 00.

In step SP 147, the mobile station 100 receives the transmission completion notification from the gateway server 32 and displays it on the liquid crystal display 132 to notify the user. FIG. 9F is a diagram of a transmission completion notification screen displayed on the mobile station 100 at this time.

On the other hand, in step SP149, credit server 60A receives input information from gateway server 32.

At step SP151, the credit server 60A examines whether or not a credit contract is possible based on the received input information while referring to the examination conditions stored by itself.

In step SP153, the result of the examination by the credit server 60A is determined. If the result of the determination is that the contract is not possible, the process proceeds to step SP155, where the credit server 60A sends a contract refusal notice to the mobile station 100 as an address to the Internet. 70.

As a result of the determination in step SP153,
If the contract is permitted, the process proceeds to step SP157, in which the credit server 60A generates new credit contract information, and sends the contract permission notification and the generated credit contract information to the Internet 70 to the mobile station 100 as a destination.

Then, in step SP159, the credit server 60A stores the user attribute information and the credit contract information of this contract in the user database 61A.

In step SP161, the gateway server 32 receives the contract refusal notice or the contract permit notification and the credit contract information from the credit server 60A, and temporarily stores the information therein.

At step SP163, gateway server 32 calls mobile station 100 and transmits an information reception notification indicating that information addressed to mobile station 100 has been received from credit server 60A.

At step SP165, the mobile station 100
Receives the information reception notification from the gateway server 32 and displays it on the liquid crystal display 132 to notify the user. FIG. 11G shows the mobile station 1 at this time.
It is a figure of the screen displayed on 00.

Then, in step SP167, the mobile station 100 is operated by a predetermined key operation of the user who saw the display.
Transmits to the gateway server 32 an information acquisition request that requests acquisition of information stored in the gateway server 32. That is, when the user selects "reference" on the screen shown in FIG. 9G, an information acquisition request is transmitted from the mobile station 100 to the gateway server 32.

At step SP169, the gateway server 32 receives the information acquisition request from the mobile station 100,
In response, he / she remembers the contract refusal notice,
Alternatively, the contract acceptability notice and the credit contract information are transmitted to the mobile station 10.
Send to 0.

At step SP171, the mobile station 100
Receives a contract refusal notice or a contract permit notice and credit contract information from the gateway server 32.

At step SP173, the mobile station 100
Displays the received content on the liquid crystal display 132. When the mobile station 100 receives the credit contract availability notification and the credit contract information, the mobile station 100
The received credit contract information is stored in the OM 123.
FIG. 9 (G) is a diagram of a screen showing a notification that a credit contract cannot be made. FIG. 9H is a screen showing a notification that a credit contract is available. When the user selects "next" on this screen, the screen moves to the next screen (FIG. 1I). FIG. 9 (I) is a screen for the user to confirm the contents of the credit contract. As shown in FIG. 1I, a "credit number", an "expiration date", and the like relating to the credit contract are displayed on this screen. Note that the screen information shown in FIG. 1I is stored in the credit ROM 123, and the liquid crystal display 132
And the user can check the credit contract information at any time.

As described above, the mobile station 10 owned by the user
9 and the credit server 60 of the credit company
A, 608,... Perform a process related to a credit contract by an electric communication means, and therefore perform the process (particularly, application of a credit

contract from a user to a credit company, notification of credit availability from a credit company to a user, and credit (Assignment of contract information) can be executed quickly.

Note that the above described step SP in FIG.
The operations shown in 101 to step SP123 are mainly operations from packet communication request to user authentication. In addition to the above-described credit contract, when using a credit using a mobile packet communication network, when changing a credit contract. This is an operation commonly performed at the stage prior to each operation at the time of cancellation or inquiry of credit use history or the like.

[2-2. Operation at Credit Shopping] Next, an operation at the time of credit shopping using the mobile station 100 will be described. There are two forms of credit shopping using the mobile station 100. That is, the credit contract information on the magnetic stripe 160 is provided to the credit server 80 via the CAT terminal 40 at the store, and the credit contract information stored in the ROM 123 for credit is transferred to the credit server 80 via the mobile packet communication network 30. There is a form to give to
Hereinafter, these will be described separately. [2-2. Operation during Credit Shopping at Store] FIG. 10 is a flowchart showing the operation of the mobile station 100 and the credit system in a mode in which the magnetic stripe 160 is used at the store.

First, in accordance with a predetermined operation of the user, in-store credit shopping processing is started in mobile station 100.

At step SP201, the control unit 120 of the mobile station 100 reads out all credit contract information stored in the credit ROM 123 and displays the credit company names on the liquid crystal display 132.

in step SP203, the user selects a desired credit company from the displayed credit companies by key operation. Here, for example, it is assumed that the credit contract of the credit company A is selected. If the number of contracted credit companies is singular, "OK" may be input to the displayed credit company.

At step SP205, the control unit 120 of the mobile station 100 gives the credit contract information of the selected company A to the magnetic writer 150, and the magnetic writer 150 writes the given credit contract information on the magnetic stripe 160.

When the credit contract information is the magnetic stripe 16
When the value is written to 0, the magnetic card 11 is set in an exposing state, and the control unit 120 displays on the liquid crystal display 132 that the exposing is possible. And step SP
in 207, when the user visually confirms that the exposure is possible, the user presses the card storage / exposure key of the mobile station 100, and the magnetic stripe 160 portion of the magnetic card 161 is moved to the mobile station 100.
Exposed from

in step SP209, the magnetic stripe 160 is slid to the magnetic reader of the CAT terminal (here, the CAT terminal 40b), and
0 is read into the CAT terminal 40b.

At step SP211, the clerk or the like
A usage amount or the like related to credit shopping is input to an input interface (not shown) of the CAT terminal 40b.

in step SP213, the CAT terminal 40
b transmits the credit contract information and the CAT terminal 40 to the credit server 60A of the company A via the CAFIS network 50.
b (these information is hereinafter referred to as credit information).

At step SP215, the credit server 60A receives the credit information from the CAT terminal 40b.

In step SP217, the credit server 60A searches the user database 61A based on the received credit information, and determines whether the requested credit shopping is legitimate. This determination may be, for example, whether the credit contract has expired, whether the credit limit has been exceeded, whether the magnetic card has been disabled, or the credit contract itself has become invalid. This is to check whether or not they are not.

If the result of the determination in step SP217 is that the credit is not valid, the process proceeds to step SP219, and the credit server 60A issues a credit rejection notification indicating that the requested credit use is not possible (and if necessary, The reason why credit cannot be used)
0 to the CAT terminal 40b.

On the other hand, as a result of the determination in step SP217,
When it is determined that the credit is valid, the process proceeds to step SP221, and the credit server 60A sends a credit permission notification indicating that the requested credit is available to the CAT terminal 40.
b, and in step SP223, the credit use history and fund settlement information for this credit shopping are stored in the credit database 62A.

In step SP225, the CAT terminal 40
b receives the notification and the like from the credit server 60A.

Then, in step SP227, the CAT
The terminal 40b outputs the received notification or the like to a credit slip or a display device (not shown) of the CAT terminal. The clerk performs a predetermined procedure according to the displayed contents. Thereafter, when the user writes the same signature as the signature on the back of the magnetic card 161 in the signature field of the credit slip displaying the usage amount and the like, the credit shopping is completed.

On the other hand, when the reading of the credit contract information on the magnetic stripe 160 is completed, the user presses the card storage / exposure key of the mobile station 100, and in step SP229, the magnetic card 161 is moved to the throttle 101 of the mobile station 100. Is stored inside.

When the magnetic card is stored, step SP
In 231, the control unit 120 of the mobile station 100 gives a message to the magnetic writer 150 that the credit contract information of the company A stored in the magnetic stripe 160 is erased, and the magnetic writer 150 executes it.

[2-2. Operation during Credit Shopping Using Mobile Packet Communication Network] Next, operation during credit shopping using the mobile packet communication network 30 will be described. FIG. 7 and FIG. 11 are flowcharts showing operations when the user performs credit shopping using the mobile station 100. The operation shown in FIG. 7 is substantially the same as the operation at the time of the credit contract, but in step SP107 in the figure, the user selects "credit shopping" as the desired service. Description of the other operations in FIG. 7 is omitted.

In step SP301 of FIG. 8, the names of all shops where the user can perform credit shopping are displayed on the liquid crystal display 132.

At step SP303, the user selects a desired user shop from the displayed user shops by key operation. Here, it is assumed that, for example, the store C is selected.

At step SP305, the mobile station 100
is the selected store name (store C) and the store server 80
The URL of C is transmitted to the gateway server 32.

In step SP307, the gateway server 32 receives the store name (store C) and the URL, and transmits a credit shopping request to the store server 80C based on the received URL.

In step SP309, the user store server 8
0C receives the credit shopping request from gateway server 32.

At step SP311, the user store server 8
In response to the received credit shopping request, 0C sends the shopping screen information stored by itself to the Internet 70 with the mobile station 100 as the destination.

In step SP313, the gateway server 32 receives the shopping screen information from the credit server 60A and transmits it to the mobile station 100.

In step SP315, the mobile station 100
Receives the shopping screen information from the gateway server 32 and displays the shopping screen on the liquid crystal display 132.

In step SP 317, the user selects a product to purchase while referring to the shopping screen displayed on the liquid crystal display 132.

When the product selection is completed, the mobile station 100
All the credit contract information stored in the credit ROM 123 is read, and the credit company names are displayed on the liquid crystal display 132. Then, in step SP319, the user selects a credit company desired to use in the credit shopping from the displayed credit companies. Here, it is assumed that the credit company B has been selected.

At step SP321, the mobile station 100
Transmits to the gateway server 32, as input information, information on the selected product and the amount of use, credit contract information of the selected company B, the URL of the store server 80C, the URL of the credit server 60B, and the like.

In step SP323, the gateway server 32 receives the input information from the mobile station 100, refers to the contents of the input information, and uses the input information to store the information in the user store server 8.
Send to 0C.

In step SP325, the store server 8
0C receives the input information from the gateway server 32. Then, the store server 80C transmits the credit contract information and the usage amount information among the received input information to the credit server 60B as credit information.

In step SP327, the credit server 60B receives the credit information from the store server 80C.

In step SP329, the credit server 60B searches the user database 61B based on the received credit information, and determines whether or not the requested credit shopping is legitimate. This determination may be, for example, whether the credit contract has expired, whether the credit limit has been exceeded, whether the magnetic card has been disabled, or the credit contract itself has become invalid. This is to check whether or not they are not.

If the result of the determination in step SP329 is that the credit server 60B determines that the credit shopping is not valid, the process proceeds to step SP331, and the credit server 60B sends a credit unavailable notification indicating that the requested credit shopping is unavailable. Send it to server 80C.

On the other hand, as a result of the determination in step SP329,
If it is determined to be valid, the process proceeds to step SP333, in which the credit server 60B transmits a credit available notification indicating that the requested credit shopping is available to the user store server 80C, and further proceeds to step SP335. Store the credit use history and the fund settlement information in the credit database 62B.

In step SP337, the user store server 8
0C receives the notification from credit server 60B.

Then, in step SP339, the store server 80C transmits the received notification to the gateway server 32 with the mobile station 100 as the destination. If the notification is a credit availability notification, the user store server 80C stores the product or the like selected by the user as credit shopping information, and sends the product to the user.
Perform predetermined processing.

[0139] At step SP341, the gateway server 32 receives the notification from the store server 80C and transmits it to the mobile station 100.

In step SP343, the mobile station 100
Receives the notification from the gateway server 32 and displays the received content on the liquid crystal display 132 to notify the user.

[2-3. Behavior when renewing credit contract]
Next, an operation at the time of updating a credit contract will be described. FIG. 12 is a flowchart showing a flow of operation at the time of updating a credit contract.

In step SP401, the credit server (here, credit server 60A) creates a contract update candidate user file 601 with reference to the user database 60A.

In step SP403, the credit server 60A refers to the contract update candidate user file 601, and sends a contract update advance notification for notifying the update of the credit contract in advance to the mobile station of the contract update candidate user (here, the mobile station 100). To the Internet 70 as a destination.

In step SP405, when the gateway server 32 receives the contract update advance notification, the mobile station 1
Call 00 to transfer the above notification.

In step SP407, the mobile station 100
Receives the contract update advance notice from the gateway server 32 and displays the received contract update advance notice on the liquid crystal display 132.

In step SP409, the mobile station 100
Transmits response information to the displayed contract update advance notice by a key operation of the user. This response information indicates that the contract is renewed, or that the contract is not renewed.

At step SP411, the gateway server 32 receives the response information from the mobile station 100 and transmits it to the credit server 60A.

At step SP413, the credit server 60A receives the response information from the gateway server 32.

[0149] In step SP415, the credit server 60A determines the mobile station 1 based on the received response information.
It is determined whether the credit contract of the user 00 is renewable.

If the result of determination in step SP415 is that updating is possible, the flow proceeds to step SP417, where the credit server 60A generates updated new credit contract information, and stores the generated credit contract information in the user database 60A. At the same time, and sends it to the Internet 70 with the mobile station 100 as a destination.

If the result of determination in step SP415 is that renewal is not possible, the process proceeds to step SP421, where the credit server 60A deletes information about users whose contract renewal is not possible, stored in the user database 61A. Then, in step SP423, the credit server 60A sends a contract non-renewal notice indicating the contract non-renewal to the Internet 70 to the mobile station 100 as a destination.

Then, at step SP425, the gateway server 32 receives the updated credit contract information or the contract non-update notice from the credit server 60A, and temporarily stores the information.

In step SP427, gateway server 32 calls mobile station 100 and transmits an information reception notification indicating that information addressed to mobile station 100 has been received from credit server 60A.

In step SP429, the mobile station 100
Receives the information reception notification from the gateway server 32 and displays it on the liquid crystal display 132 to notify the user.

In step SP431, the mobile station 100 transmits to the gateway server 32 an information acquisition request for acquiring information stored in the gateway server 32 by a predetermined key operation of the user who has viewed the display.

In step SP433, the gateway server 32 receives the information acquisition request from the mobile station 100,
In response, the mobile station 100 transmits the updated credit contract information or the contract non-renewal notification stored therein.
Send to

At step SP435, the mobile station 100
Receives updated credit contract information or a contract non-renewal notice from the gateway server 32.

In step SP437, the mobile station 100
Displays the received content on the liquid crystal display 132. Then, when receiving the updated credit contract information, the mobile station 100 updates information such as the expiration date. In addition, when the mobile station 100 receives the notification that the contract has not been renewed, the mobile station 100 sets the credit ROM 123 when the expiration date has passed.
Deletes the credit contract information stored in.

It is also conceivable that the user does not respond to the credit contract advance notification given to mobile station 100 even if the expiration date has expired. In such a case, the credit server 60A transfers the updated credit contract information after the expiration date via the gateway server, assuming that the user has responded to the contract renewal with a "yes" response. This is transmitted to the station 100, and the mobile station 100 updates information such as an expiration date.

[2-4. Operation when Credit Contract is Changed] Even when the user changes the name or address, the mobile station 100
It is possible to carry out such a change procedure using. Hereinafter, the operation when the credit contract is changed will be described.
FIG. 7 and FIG. 13 are flowcharts showing the operation when the user makes a credit contract using the mobile station 100. The operation shown in FIG. 7 is almost the same as the operation at the time of the credit contract, but in step SP107 in the figure, the user selects "change credit contract" as the desired service. Description of other operations is omitted.

At step SP501 in FIG. 13, all credit companies with which the user has contracted are displayed on the liquid crystal display 132.

At step SP503, the user selects a desired credit company from the displayed credit companies by key operation. Note that it is also possible to select all credit companies. Here, it is assumed that the credit company A is selected.

In step SP505, the mobile station 100 stores the name of the selected credit company in the gateway server 32.
Send to

At step SP509, the gateway server 32 receives the credit company name from the mobile station 100 and transmits a credit contract change request to the credit server 60A.

In step SP511, the credit server 60A receives the credit contract change request

At step SP513, the credit server 60A sends screen information for changing the credit contract of the company A to the Internet 70 with the mobile station 100 as a destination.

In step SP515, the gateway server 32 receives the screen information for change from the credit server 60A and transmits the screen information to the mobile station 100 as a destination.

In step SP517, the mobile station 100
Receives the change screen information from the gateway server 32 and displays the change screen on the liquid crystal display 132.

At step SP519, the user inputs the contents to be changed while referring to the change screen displayed on the liquid crystal display 132.

In step SP521, the mobile station 100
Transmits the input contents (hereinafter, referred to as changed contents) to the gateway server 32.

At step SP523, the gateway server 32 receives the content of the change, and

Send the change to A.

At step SP525, credit server 60A receives the content of the change.

In step SP527, the credit server 60A changes the contents of the user attribute information and the credit contract attribute information stored therein based on the received change content.

When the change processing is completed, step SP52
Proceeding to 9, the credit server 60A sends a completion notification indicating that the contract change processing has been completed to the Internet 70 to the mobile station 100 as a destination.

At step SP531, the gateway server 32 receives the completion notification via the Internet 70 and transmits it to the mobile station 100.

In step SP533, the mobile station 100
Receives the completion notification from the gateway server 32.

In step SP535, the mobile station 100
Displays the received completion notification on the liquid crystal display 132. [2-5. Operation when Canceling a Credit Contract] In addition, cancellation processing of a credit contract can be performed using this system. Hereinafter, an operation when a user makes a credit contract using the mobile station 100 will be described. FIG. 7 and FIG. 14 are flowcharts showing the operation when the user makes a credit contract using the mobile station 100. FIG.
is substantially the same as the operation at the time of the credit contract, but at step SP107 in the figure, the user selects "Credit Cancellation" as the desired service. Description of other operations is omitted.

At step SP601 in FIG. 14, all credit companies with which the user has contracted are displayed on the liquid crystal display 132.

In step SP603, the user selects a desired credit company from the displayed credit companies by key operation. Here, it is assumed that the credit company A is selected.

In step SP605, the mobile station 100 stores the name of the selected credit company in the gateway server 32.
Send to

At step SP607, the gateway server 32 receives the credit company name from the mobile station 100 and transmits a credit contract cancellation request to the credit server 60A.

At step SP609, the credit server 60A receives the credit contract cancellation request from the gateway server 32.

In step SP611, the credit server 60A deletes the credit contract, for example, deletes the user attribute information and the credit contract attribute information stored in the user database 61A based on the received credit contract cancellation request.

In step SP613, the credit server 60A sends a completion notification indicating that the contract cancellation processing has been completed to the Internet 70 with the mobile station 100 as a destination.

[0185] In step SP615, the gateway server 32 receives the completion notification via the Internet 70 and transmits it to the mobile station 100.

In step SP617, the mobile station 100
Receives the completion notification from the gateway server 32.

In step SP619, the mobile station 100
Displays the received completion notification on the liquid crystal display 132.

[2-6. Operation When Prohibition of Use of Mobile Station 100 and Credit] A case in which a user loses or stolen the mobile station 100 is considered.
in such a case, if the use of the credit is not prohibited, there is a possibility of unauthorized use by a third party. Hereinafter, the operation when the mobile device 100 and the use of the credit are prohibited will be described. FIG. 15 is a flowchart illustrating a flow of processing for prohibiting use of the mobile device 100 and credit.

When the user loses the mobile station 100, the user contacts the communication company that manages the mobile telephone network 20 and the mobile packet communication network 30 by a predetermined method to use the communication of the mobile station 100 and use the credit. Communicate the prohibition. In step SP701, the communication company that has received the above notification from the user accesses the subscriber database 331 of the control station 33 using a predetermined management terminal, and prohibits the use of communication services and credits for the user. Is registered. Thereafter, the mobile station 10 of the user Use of communication services and credits by 0 is prohibited. Specifically, the operation is as follows.

First, in step SP703, the mobile station 10
The third party illegally acquiring 0 turns on the power of the mobile station 100.

In step SP705, the mobile station 100
indicates that the power is turned on and the mobile station 1 uses a specific channel.
It transmits an identification number 00 (hereinafter referred to as transmission information). The base station including the location of the mobile station 100 in the jurisdiction area (here, the base station 32) receives the transmission information from the mobile station 100 and sends it to the control station 33.

In step SP707, the control station 33
The transmission information is received from the base station 32.

Then, in step SP709, the control station 33 determines the subscriber database 3 based on the received transmission information.
Access is made to the mobile station 100 to check for communication and credit use prohibition information.

In step SP711, the control station 33, which has determined that there is use prohibition information, informs the mobile station 1 via the base station 32 of the prohibition of communication of the mobile station 100 and use of credit.
Send to 00.

In step SP713, the mobile station 100
Receives, via the base station 31, the communication of the mobile station 100 and the prohibition of credit use.

in step SP715, the mobile station 100
Performs communication and credit use prohibition processing. Here, in the communication use prohibition processing, each unit of the mobile station 100 that operates for the communication processing is not operated. In addition, the process of prohibiting the use of credit is performed by the credit ROM 123.
Delete credit contract information stored in.

[2-7. Operation when inquiring credit history etc.] The user can access the credit servers 60A, 60B... Using the mobile station 100 to inquire various information such as credit usage history and the next credit debit amount. It is. The operation at the time of inquiring the credit use history and the like will be described below. 7 and 16
9 is a flowchart showing an operation when a user uses the mobile station 100 to inquire about a credit use history. The operation shown in FIG. 7 is almost the same as the operation at the time of the credit contract,
in step SP107 in the figure, the user selects "credit history" as a desired service. Description of other operations is omitted.

In step SP801 of FIG. 13, all credit companies with which the user has contracted are displayed on the liquid crystal display 132.

In step SP803, the user selects a desired credit company from the displayed credit companies by key operation. Here, it is assumed that the credit company A is selected.

[0200] In step SP805, the mobile station 100 transmits the selected credit company name (company A) to the gateway server 32.

In step SP807, the gateway server 32 sends the credit company name (A
) And transmits a credit use history inquiry request to the credit server 60A.

At step SP809, the credit server 60A receives the credit use history inquiry request.

At step SP811, the credit server 60A searches the credit use history information stored in the credit database 62A.

At step SP813, the credit server 60A sends the credit use history information obtained as a result of the search to the Internet 70 with the mobile station 100 as a destination.

[0205] At step SP815, the gateway server 32 receives the credit use history information via the Internet 70 and transmits it to the mobile station 100.

In step SP817, the mobile station 100
Receives the credit use history information from the gateway server 32.

In step SP819, the mobile station 100
Displays the received credit usage history on the liquid crystal display 1
32.

[B. Modifications] [B-1. Modification Example at the Time of Credit Contract] In the above description, all operations at the time of a credit contract are performed in a continuous session, but this is not always necessary.
That is, a credit contract request operation from the mobile station 100 to the credit server 60 (ie, step SP101 in FIG. 7)
8 to step SP149 in FIG. 8) and the response operation from the credit server 60 to the mobile station 100 (that is, steps SP151 to SP173 in FIG. 8) may be separated. For example, there may be a case where a considerable amount of time is required for the examination process at the time of a credit contract, or a case where a part or all of the examination process is performed on behalf of another information processing device or a person. The communication between the mobile station 100 and the credit server 60 may be terminated once when the operation is completed, and the examination result may be notified to the mobile station 100 later when the credit server 60 acquires the result of the examination processing.

Also, the credit servers 60A, 60B
The process at the time of the credit contract in the... May be only the process related to the credit contract request operation. For example, the process ends in step SP149 of FIG. 7, and thereafter, as a result of the examination by the credit company, if the contract is not possible, the user is notified by telephone or the like, or if the contract is possible, is notified to the user by telephone or other means,
The user may go to a store of a credit company, and credit contract information may be given to the mobile station 100 by a dedicated ROM reader / writer installed there.

[B-2. Modification example when changing credit contract]
The contents of the change in the credit contract include, in addition to the above-mentioned name change and address change, various changes such as, for example, a

credit limit change and a card grade change (for example, a change from a normal credit card to a gold card). Can be considered. In such a case, in addition to the above-described operation steps, a step of examination by a credit company, a step of notifying (impossible) change from the credit server 60 to the mobile station 100 based on the result of the examination, and the like are necessary. Becomes

[B-3. Modification when mobile station 100 and credit use are prohibited] The mobile station 100 transmits transmission information not only when the power is turned on, but also various other timings can be considered. For example, the mobile station 100
May request the call service or the packet communication service from the mobile communication network, or the mobile station 100 may start the process of using the credit at the store. That is,
As long as the mobile station 100 is set to transmit outgoing information in response to a certain operation by the person holding the mobile station 100, any operation may be used as the trigger. Alternatively, the mobile station 100 may constantly or periodically transmit the transmission information while the power is on.

[0212] When the use prohibition information is registered in the control station 33, the control station 33 or the like may call the mobile station 100 related to the use prohibition and give the use prohibition information to the mobile station 100. On the other hand, when the mobile station 100 receives the use prohibition information, it transmits a reception confirmation signal, and the control station 33 confirms that the mobile station 100 has received the use prohibition information by receiving the reception confirmation signal. Further, the control station 33 may always transmit the above-mentioned use prohibition information to each jurisdiction area via many base stations 32. And
The mobile station 100 that has received the transmitted use prohibition information
May perform a credit function use prohibition process.

[0213] The control station 33 may have only the communication use prohibition information of the mobile station 100 and only give the mobile station 100 the communication use prohibition information. Then, the mobile station 100 that has received the communication use prohibition information may perform the credit use prohibition process by determining that not only the use of communication but also the use of credit is prohibited.

[B-4. Modification of Configuration of Gateway Server 32, Credit Server 60, and Store Server 80] In the above description, the credit server 60A,
60B ... and the store server 80 are connected to the Internet 7
In addition to those connected to 0, it may be connected to the gateway server 32 via a dedicated line, or provided inside a mobile communication network.

[B-5. Modification of Role Allocation of Gateway Server 32, Credit Server 60, and Store Server 80] Gateway Server 32, Credit Server 60
The functions of each of the user server 80 and the store server 80 are not limited to the above-described embodiments. For example, various functions such as the gateway server 32 acting as a part of the functions of the store server 80 and the credit server 60 may be used. Is possible. An example will be described below.

Are not stored by the credit servers 60A, 60B,... As in the above-described embodiment at the time of a credit contract or change, but by the gateway server 32.
Information may be stored. Thereby, when a contract request or a change request is transmitted from the mobile station 100 to the gateway server 32, the gateway server 32 does not need to access the credit servers 60A, 60B,.
Input screen information and the like can be provided to the mobile station 100.

The credit servers 60A, 60B
Does not perform the examination for judging whether or not the credit contract is acceptable, but the gateway server 32 may perform the examination. For this purpose, the gateway server 32 stores contract availability determination conditions given in advance from each of the credit servers 60A, 60B,... For each credit company, and conducts an examination in accordance with those conditions.

The gateway server 32 may have a contract update candidate user file 601. In this case, the gateway server 32
From 0A, 60B, etc., the contract update candidate user file 6
01, and the subsequent processing with the mobile station 100 is performed based on the given contract update candidate user file 60.

In the above-described embodiment, the gateway server 32 has the credit servers 60A and 60B.
(For example, credit contract information and various notifications) are temporarily stored, and an information reception notification is transmitted to the mobile station 100. Then, in response to the notification, the mobile station 100
When there is a credit contract information acquisition request from, the gateway server 32 gives the mobile station 100 the credit contract information and the like.
However, this need not be the case. For example, gateway server 3
2 receives any information destined for the mobile station 100 from the credit servers 60A, 60B,... Without transmitting any information to the mobile station 100 in advance (or at the same time as notifying the mobile station 100). 100 may be given. In this case, the mobile station 100 is
When the gateway server 32 receives the information from the mobile station 100, the gateway server 32 confirms that the mobile station 100 has received the information by receiving the reception confirmation signal.

In the embodiment of the credit shopping using the mobile packet communication network 30, the input information transmitted by the mobile station 100 is received by the store server 80 via the gateway server 32, and the store Although the server 80 transmits the credit contract information and the usage amount information to the credit server 60 from the input information, this is not always necessary. For example,
The gateway server 32 classifies the content of the input information into a destination for the store server 80 and a destination for the credit server 60,
Each may be transmitted separately. That is, the gateway server 32 transmits the merchandise information from the input information to the store server 80, and transmits the credit contract information and the usage amount information to the credit server 60. Then, the credit availability information from the credit server 60 may be provided to the mobile station 100 via the store server 80, or may be directly provided from the credit server 60 to the mobile station 100 and the store server 80, respectively. . Further, the gateway server 32 may store a shopping screen, and when a request is received from the mobile station 100, the stored shopping screen may be given to the mobile station 100.

[B-6. Kind of Subscription Contract] In the above embodiments, the credit contract was described as a subscription contract, but the present invention is not limited to the credit contract, and other subscription contracts may be used. For example, it may be a deposit or loan contract with a financial institution, an insurance contract with an insurance company, or a membership contract for becoming a member of various organizations.

[B-7, Mobile Station 100 and CAT Terminal 4
Modification 0] [B-7-1, First Modification] The mobile station 100 transmits the credit contract information to the CAT terminals 40a and 40 using a barcode.
b ... may be given. FIG. 17 is a block diagram illustrating a configuration of the mobile station 100 that displays a barcode indicating credit contract information on the liquid crystal display 132. The mobile station 100 includes a user interface 13 having a transmitting / receiving unit 110, a control unit 120, and a liquid crystal display 132.
0, a data input / output terminal 140 and the like. The control programs stored in the program ROM 122 include:
A barcode creation program for creating barcode data indicating credit contract information is included. CPU 12
1, when it is necessary to display the credit contract information, it reads the credit contract information from the credit ROM 123 and creates barcode data indicating the credit contract information according to a barcode creation program.
The information is displayed on the liquid crystal display 132.

On the other hand, the CAT terminals 40a, 40b,.
is equipped with a bar code reader, and can read a bar code displayed on the liquid crystal display 132 of the mobile station 100. FIG. 18 is a block diagram illustrating a configuration of the CAT terminal 40 including the barcode reader. The CAT terminal 40 includes a user input interface 41,
A transmitting / receiving unit 42, an output interface 43, a control unit 44,
it comprises a barcode reader 45 and the like. Control unit 44
Controls each unit of the CAT terminal 40. The user interface 41 is for a clerk or the like to input a usage amount or the like. The barcode reader 45 reads a barcode displayed on the liquid crystal display 132 of the mobile station 100. The transmission / reception unit 42 exchanges various data with the CAFIS network 50. The output interface 43 is a credit slip printing device or the like. Other configurations and operations are the same as those of the first embodiment. What is displayed on the liquid crystal display 132 only needs to be optically readable, and may be, for example, a color code, a peri code, or the like.

[B-7-2. Second Modification] Mobile Station 100
May give credit contract information to the CAT terminals 40a, 40b,. FIG.
is a block diagram showing a configuration of the mobile station 100 that gives credit contract information to the CAT terminals 40a, 40b,... By infrared communication.
The mobile station 100 includes a transmitting / receiving unit 1
10, control unit 120, user interface 130, data input / output terminal 140, modulation unit 170, infrared radiation unit 1
80 and the like. When it is necessary to provide the credit contract information to the CAT terminals 40a, 40b,..., The CPU 121 reads the credit contract information from the credit ROM 123 and supplies the read credit contract information to the modulation unit 170. The modulation unit 170 modulates the infrared carrier with a signal wave corresponding to the given credit contract information, and
Give to 80. Infrared radiating section 180 radiates a given infrared ray.

Are provided with an infrared receiving unit and a demodulating unit. The CAT terminals 40a, 40b,... Receive the infrared rays radiated from the infrared radiating unit 180 of the mobile station 100, demodulate them, and transmit Can be obtained.
FIG. 20 is a block diagram illustrating a configuration of the CAT terminal 40 including the infrared receiving unit and the demodulating unit. This CAT terminal 4

5 is a user input interface 41, a transmitting / receiving unit 42,
Output interface 43, control unit 44, infrared receiving unit 4
6, a demodulation unit 47 and the like. Other configurations and operations are the same as those of the first embodiment.

[B-7-3. Third Modification] Also, mobile station 1
00 may give credit contract information to the CAT terminals 40a, 40b,... Via existing data input / output terminals. FIG. 21 shows that the CAT terminals 40a, 40b,.
FIG. 3 is a block diagram showing a configuration of a mobile station 100 given to the mobile station 100. The mobile station 100 includes a transmitting / receiving unit 110, a control unit 12
0, user interface 130, data input / output terminal 1
40 and the like. When it is necessary to provide the credit contract information to the CAT terminals 40 a, 40 b,..., The CPU 121 reads the credit contract information from the credit ROM 123 and supplies the credit contract information to the data input / output terminal 140. The data input / output terminal 140 transmits the given credit contract information to the CAT terminals 40a, 40b,.
Is provided to the data input / output terminal.

FIG. 22 shows a CA having data input / output terminals.
FIG. 2 is a block diagram illustrating a configuration of a T terminal 40. This CAT
The terminal 40 includes a user input interface 41, a transmission / reception unit 42, an output interface 43, a control unit 44, a data input / output terminal 48, and the like. Other configurations and operations are the same as those of the first embodiment.

[B-7-4. Other Modifications of Mobile Station 100 and CAT Terminal 40] In the above description of mobile station 100 having a magnetic stripe, mobile station 100 has only one magnetic stripe 160, and magnetic stripe 160 Writer 150 writes credit contract information every time a credit is used,
It does not have to be. For example, magnetic card 1
A plurality of magnetic stripes 160 are provided on 61, and one magnetic stripe may correspond to one credit contract. That is, the magnetic stripes 160 are provided by the number of credit contracts. In this case, the CAT terminals 40a, 40b,.
Reads the magnetic stripe 160 in which the card information of the designated credit company is stored among the plurality of magnetic stripes 160.

[0229] When the user performs credit shopping only using the above-mentioned mobile packet communication network,
The mobile station 100 does not need to include the magnetic stripe 160 or the like. This is because in credit shopping using the mobile packet communication network, data can be exchanged with the credit servers 60A, 60B,... Only by the wireless communication function.

In the above description, the mobile station (so-called cellular, PHS, etc.) has card information of a credit card.
The mobile communication terminal is not limited to the mobile station 100 alone, and may be a mobile communication terminal without a telephone function (for example, a PDA).

In the above description, the CAT terminals 40A, 40B,...
00 may be given. For example, at the time of credit shopping, the CAT terminals 40A, 40B,.
Has information such as the date of use, the store used, the amount of use, etc. relating to credit shopping, and the information is stored in the mobile station 1.
00 may be given. Then, the mobile station 100 can accumulate the credit use history or calculate the credit debit amount based on the credit use history without having to access the credit servers 60A, 60B,... . For that purpose, in each of the above embodiments, the CAT terminals 40a, 40b,.
May have a data input / output terminal connected to the data input / output terminal of the mobile station 100 and capable of providing the information.

[B-8. Modification of User Authentication] In the above-described embodiment, the password stored in advance in the gateway server 32 is compared with the password input by the user to the mobile station 100 in response to the packet communication start request. Is a form in which user authentication is performed, but this is not always necessary. For example, a password for user authentication may be stored in the mobile station 100 in advance. By doing so, the mobile station 100 can perform user authentication without communicating with the gateway server 32.

The credit server 60 may store a password (second password) separately from the password (first password) stored by the gateway server 32. In this case, when starting packet communication,
The first password verification is performed between the mobile station 100 and the gateway server 32, and the mobile station 100 is used for credit shopping and credit use history inquiry.

A second password check is performed between the password server and the credit server 60. As a result, higher privacy protection and higher security when using credit can be expected.

As described above, according to the present invention, it is possible to perform the contract processing more quickly without imposing a large burden on the user in the contract of various electronic commerce services

[Brief description of the drawings]

FIG. 1 shows a mobile station 10 used in an embodiment of the present invention.
FIG. 3 is a block diagram showing a configuration of a 0.

FIG. 2A is a perspective view showing an appearance of a mobile station 100 in a state in which a magnetic card 161 is stored, and FIG.
FIG. 9 is a perspective view showing an appearance in a state where a magnetic stripe 160 portion of the magnetic card 161 is exposed from the mobile station 100.

FIG. 3 is a block diagram showing a configuration of a credit system using the mobile station 100.

FIG. 4 is a block diagram showing a functional configuration of the gateway server 32.

5A is a diagram showing a configuration of a subscriber database 331, and FIG. 5B is a diagram showing a subscriber registration information file 3;
04 is a data format diagram of FIG.

6A is a diagram illustrating a configuration of a user database 61, and FIG. 6B is a diagram illustrating a credit database 62;
(C) is a diagram showing a configuration of a contract update candidate user file 601.

FIG. 7 is a flowchart showing an operation performed before a credit contract, a credit shopping using a mobile packet communication network, a credit contract change, a credit contract cancellation, and a credit use history inquiry operation.

FIG. 8 is a flowchart showing operations of the mobile station 100 and the credit system at the time of a credit contract.

FIG. 9 is a diagram showing a screen displayed on the liquid crystal display 132 of the mobile station 100 at the time of a credit contract.

FIG. 10 is a flowchart showing the operation of the mobile station 100 and the credit system at the time of credit shopping at a store.

FIG. 11 is a flowchart showing operations of the mobile station 100 and the credit system during credit shopping using a mobile packet communication network.

FIG. 12 shows a mobile station 1 when renewing a credit contract.
It is a flowchart which shows operation | movement of 00 and a credit system.

FIG. 13 shows a mobile station 10 in changing a credit contract.
0 is a flowchart showing the operation of the credit system.

FIG. 14 shows a mobile station 10 when a credit contract is canceled.
0 is a flowchart showing the operation of the credit system.

FIG. 15 is a flowchart showing a flow of an operation of prohibiting use of the mobile station 100 and credits.

FIG. 16 is a flowchart showing a flow of an operation when inquiring a credit use history.

FIG. 17 is a block diagram showing a configuration of a mobile station 100 that displays a barcode indicating credit contract information on a liquid crystal display 132.

FIG. 18 is a CAT terminal 40 having a barcode reader.
FIG. 3 is a block diagram showing the configuration of FIG.

FIG. 19: Credit contract information is transmitted by infrared communication to C
FIG. 2 is a block diagram showing a configuration of a mobile station 100 provided to AT terminals 40a, 40b,...

FIG. 20 is a block diagram showing a configuration of a CAT terminal 40 having an infrared receiving unit and a demodulating unit.

FIG. 21 is a block diagram showing a configuration of a mobile station 100 that provides credit contract information to CAT terminals 40a, 40b,... Through existing data input / output terminals.

FIG. 22 shows a CAT terminal 40 having a data input / output terminal.
FIG. 3 is a block diagram showing the configuration of FIG.

[Explanation of symbols]

20 mobile telephone network, 30 mobile packet communication network, 31 base station, 32 gateway server, 33 control station, 40 CAT terminal, 50
..CAFIS network, 60 ... credit server, 61
... user database, 62 ... credit database, 70 ... internet, 80 ... store server, 100 ... mobile station, 101 ... throttle, 110 ... transceiver, 120 .. .Control unit, 12
1 ... CPU, 122 ... ROM for program, 1
23: ROM for credit, 124: RAM,
130: user interface, 131: card storage / exposure key, 132: liquid crystal display, 1
40: data input / output terminal, 150: magnetic writer, 160: magnetic stripe, 170: modulation unit, 180: infrared radiation unit, 301: control unit,
302 ... subscriber information management unit, 303 ... data distribution management unit, 304 ... subscriber registration information file, 33
1 ... subscriber database, 601 ... contract update candidate user file

----------続き Continued on front page F-term (reference) HH11 SK101 KK12 KK17 LL00 LL02
LL12 MM07 NN18 NN21 PP04 RR05 SS07 TT06

Patent Citations (12)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
WO1994007205A1 *	1992-09-18	1994-03-31	Kim, Soon, ik	Method for providing service on credit utilizing telephone lines
US5966699A *	1996-10-11	1999-10-12	Zandi, Richard	System and method for conducting loan auction over computer network
US5898783A *	1996-11-14	1999-04-27	Lucent Technologies, Inc.	System and method for employing a telecommunications network to remotely disable a SIM or smartcard
JPH10143570A *	1996-11-15	1998-05-29	Susumu Miyake	Electronic transfer method for individual information of credit card, and miniature ic card, adapter card, terminal adapter, slip issuing machine and portable terminal therefor
JPH10198729A *	1996-11-18	1998-07-31	Fujitsu Ltd	Contract application processing system, contract mediating device, and recording medium storing contract application processing system program
EP0956673A4 *	1996-12-20	2005-04-06	Financial Services Technology	Method and system for processing electronic documents
JPH10232897A *	1997-02-18	1998-09-02	Nippon Shinpan Kk	Credit card system
JPH10312437A *	1997-05-14	1998-11-24	Hitachi Ltd	Internet banking system

JPH10327147A *	1997-05-21	1998-12-08	Hitachi Ltd	Electronic authenticating and notarizing method and its system
CN1246941A *	1997-08-13	2000-03-08	松下电器产业株式会社	Mobile electronic commerce system
US5940812A *	1997-08-19	1999-08-17	Loanmarket Resources, L.L.C	Apparatus and method for automatically matching a best available loan to a potential borrower via global telecommunications network
US6065120A *	1997-12-09	2000-05-16	Phone.Com, Inc.	Method and system for self-provisioning a rendezvous to ensure secure access to information in a database from multiple devices

* Cited by examiner, † Cited by third party

Cited By (23)

Publication number	Priority date	Publication date	Assignee	Title
JP2003122928A *	2001-10-10	2003-04-25	Inkurimento P Kk	System and terminal of insurance contract, and information recording medium
JP2004021311A *	2002-06-12	2004-01-22	Japan Telecom Co Ltd	Information processor and information processing method
JP2004213382A *	2002-12-27	2004-07-29	Japan Research Institute Ltd	Electronic image display device and method, and program for making computer implement this method
Family To Family Citations				
US7113299B2 *	2001-07-12	2006-09-26	Canon Development Americas, Inc.	Printing with credit card as identification
WO2003079250A1 *	2002-03-18	2003-09-25	Fujitsu Limited	Card issuing system
US20040128239A1 *	2002-09-10	2004-07-01	Thami Smires	Method and apparatus for conducting transactions generated at point-of-sale locations
WO2005119607A2 *	2004-06-03	2005-12-15	Tyfone, Inc.	System and method for securing financial transactions
US20050269401A1 *	2004-06-03	2005-12-08	Tyfone, Inc.	System and method for securing financial transactions
GB2410113A *	2004-11-29	2005-07-20	Morse Group Ltd	A system and method of accessing banking services via a mobile telephone
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
US20060226217A1 *	2005-04-07	2006-10-12	Tyfone, Inc.	Sleeve for electronic transaction card
KR100772859B1 *	2005-08-18	2007-11-02	삼성전자주식회사	Multi-user computer system and remote control method for the same
KR101379861B1 *	2006-10-20	2014-04-17	삼성전자주식회사	Apparatus, system and method for providing DRM
US7991156B2	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
US7930249B2	2007-07-11	2011-04-19	Qualcomm Incorporated	Mobile wireless financial instrument for automatically selecting a payment instrument
US8938793B2 *	2007-10-03	2015-01-20	Gmx Sas	System and method for secure management of transactions
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
CN101939947B *	2008-02-29	2013-01-09	三菱电机株式会社	Key management server, terminal, key sharing system, key distribution program, key reception program, key distribution method, and key reception method
US8485112B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
US8224375B2	2009-05-01	2012-07-17	Qualcomm Incorporated	Proximity purchase ringtones
JP5705899B2	2013-03-22	2015-04-22	株式会社アイキューブドシステムズ	Mobile terminal, information management system, information management method and program

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title

KR100554695B1	2006-02-22	Mobile communication terminal
KR100446480B1	2004-08-30	Method for inhibiting use of mobile communication terminal having memory where card information is stored, mobile communication network, and mobile communication terminal
JP2001167187A	2001-06-22	Subscription contract mediation method and mobile communication network
US8583499B2	2013-11-12	System for secured transactions over a wireless network
KR20010100380A	2001-11-14	Method and apparatus for paying a charge of goods or service using a mobile phone
KR20000037471A	2000-07-05	bill-payment service method, and system for the same
EP1760649B1	2011-12-21	Method and system for electronic commerce
JP2001168980A	2001-06-22	Method for inhibiting use of mobile communication terminal, mobile communication network and mobile communication terminal
JP4071445B2	2008-04-02	Transaction mediation system, transaction mediation apparatus and program
JP2001237989A	2001-08-31	Charging acting system to owner of information display type portable telephone
CA2549387C	2012-01-24	Method for disabling mobile communication terminal equipped with memory for storing card information, mobile communication network and mobile communication terminal
JP2003069753A	2003-03-07	Communication rate processing method and managing server
JP2001169357A	2001-06-22	Mobile communication terminal and card information reader

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
JP35226599A	1999-12-10	1999-12-10	Subscription contract mediation method and mobile communication network

Applications Claiming Priority (53)

Application	Filing date	Title
JP35226599A	1999-12-10	Subscription contract mediation method and mobile communication network
CN200710128230.6A	2000-12-07	Mobile communication network for disabling mobile communication terminal equipped with memory for storing card information
HU0105484A	2000-12-07	Electronic commerce contract mediation method and mobil communication network
PCT/JP2000/008654	2000-12-07	Mobile communication terminal and card information reader
KR1020017010147A	2000-12-07	Mobile communication terminal and card information reader
US09/890,830	2000-12-07	Method for inhibiting use of mobile communication terminal having memory where card information is stored, mobile communication network, and mobile communication terminal
KR1020017010145A	2000-12-07	Electronic commerce contract mediation method and mobile communication network
AU17329/01A	2000-12-07	Mobile communication terminal and card information reader
CNB008083690XA	2000-12-07	Mobile communication terminal and card information read device
IL144746/00A	2000-12-07	Method for disabling mobile communication terminal equipped with memory for storing card information, mobile communication network and mobile communication terminal
BR0009958-9A	2000-12-07	Improvement in mobile terminal and credit card information reader
BR0008082-9A	2000-12-07	Improvement in method to disable a mobile communication terminal equipped with memory for the storage of credit card information, mobile communication network and mobile communication terminal
US09/868,477	2000-12-07	Electronic commerce contracts mediating method and mobile communication network
CN200410099863.7A	2000-12-07	Mobile communication terminal
AU17330/01A	2000-12-07	Method for inhibiting use of mobile communication terminal having memory where card information is stored, mobile communication network, and mobile communication terminal
AU17327/01A	2000-12-07	Electronic commerce contract mediation method and mobile communication network
US09/890,910	2000-12-07	Mobile communication terminal and card information reading device

CA002356357A	2000-12-07	Method for disabling mobile communication terminal equipped with memory for storing card information, mobile communication network and mobile communication terminal
HU0105368A	2000-12-07	Method for inhibiting use of mobile communication terminal having memory where card information is stored, mobile communication network, and mobile communication terminal
EP0979968A	2000-12-07	Method for inhibiting use of mobile communication terminal having memory where card information is stored, mobile communication network, and mobile communication terminal
IL144747A	2000-12-07	Mobile communication terminal and card information reading device
CA 2356361	2000-12-07	Electronic commerce contract mediation method and mobile communication network
BR0007805A	2000-12-07	Improvement in the method of intermediation of electronic commerce contracts and mobile communication network
KR1020047019020A	2000-12-07	Mobile communication terminal
PL34926000A	2000-12-07	Electronic commerce contract mediation method and mobile communication network
PL34926400A	2000-12-07	Method of immobilising a mobile communication terminal provided with a card information storing memory, mobile communication network and mobile communication terminal
KR10-2001-7010146A	2000-12-07	Method for inhibiting use of mobile communication terminal having memory where card information is stored, mobile communication network, and mobile communication terminal
BR0008000A	2000-12-07	Improvement in portable telephone and terminal equipment
EP20000979965	2000-12-07	Electronic commerce contract mediation method and mobile communication network
EP0979967A	2000-12-07	Mobile communication terminal and card information reader
PCT/JP2000/008655	2000-12-07	Method for inhibiting use of mobile communication terminal having memory where card information is stored, mobile communication network, and mobile communication terminal
IL144584A	2000-12-07	Electronic-commerce contracts mediating method and mobile communication network
CA002356371A	2000-12-07	Mobile communication terminal and card information reading device
PL34925700A	2000-12-07	Mobile communication terminal and card information reader
HU0200051A	2000-12-07	Mobile communication terminal and card information reader
CA2549387A	2000-12-07	Method for disabling mobile communication terminal equipped with memory for storing card information, mobile communication network and mobile communication terminal
CN00803692A	2000-12-07	Method for inhibiting use of mobile communication terminal having memory where card information is stored, mobile communication network, and mobile communication terminal
PCT/JP2000/008652	2000-12-07	Electronic commerce contract mediation method and mobile communication network
CNB008036950A	2000-12-07	Electronic business contract adjusting method and mobile communication network
TW089126278A	2000-12-08	Mobile communication terminal and card information reader
TW089126273A	2000-12-08	Operation denial method, mobile communication network and mobile communication terminal for mobile terminal equipped with memory card of data memory
TW89126275A	2000-12-08	Brokerage method for electronic commerce contract and mobile communication network
IL144584A	2001-07-26	Electronic-commerce contracts mediating method and mobile communication network
NO20013734A	2001-07-30	Mobile communication terminal and card information reader device
NO20013732A	2001-07-30	Procedure for electronic communication of trade contracts and mobile communication networks
NO20013733A	2001-07-30	Communication network to block a mobile communication terminal said like a mobile phone
IL144746A	2001-08-06	Method for disabling mobile communication terminal equipped with memory for storing card information, mobile communication network and mobile communication terminal
IL144747A	2001-08-06	Mobile communication terminal and card information reading device
HK02103108.1A	2002-04-24	Method for inhibiting use of mobile communication terminal having memory where card information is stored, mobile communication network, and mobile communication terminal
HK02103103.6A	2002-04-24	Mobile communication terminal and card information reader
HK02105886.4A	2002-08-12	Electronic commerce contract mediation method and mobile communication network
US10/689,810	2003-10-21	Mobile communication terminal and card information reading device
US11/026,735	2004-12-30	Mobile communication terminal and card information reading device

Legal Events

Date	Code	Title	Description
2004-01-05	A521	Written amendment	**Free format text:** JAPANESE INTERMEDIATE CODE: A523 **Effective date:** 20031226
2004-03-30	A02	Decision of refusal	**Free format text:** JAPANESE INTERMEDIATE CODE: A02 **Effective date:** 20040330

Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

Patents CN1218276C

IC card

Abstract

The present invention relates to a multifunctional IC card (MFC) which has compatibility with a multimedia card, an SD card, etc. The compatibility comprises that connecting terminals (from #1 to #13) are configured into two rows on a base plate (1) in a tortuous mode; moreover, multifunctional installation is realized and is represented by that a memory card unit (3) and an SIM card unit (4) are respectively connected and installed on the presetting terminals of the connecting terminals (from #1 to #13); the memory card unit (3) and the SIM card unit (4) respectively and independently have areas used for saving safe secret codes. In this way, one IC card can realize multifunctional devices with different safety levels. Because a multi-line layout which corresponds to the distribution of the tortuous mode is adopted, a card inserting port can adopt a correspondingly simple structure, wherein the number of the convex points of the terminals of the card inserting port can be combined with a tortuous part to alternately change. The terminals of the card inserting port are integrally configured in parallel in a line.

Classifications

G06K19/0719 Record carriers with conductive marks, printed circuits or semiconductor circuit elements, e.g. credit or identity cards also with resonating or responding marks without active components with integrated circuit chips at least one of the integrated circuit chips comprising an arrangement for application selection, e.g. an acceleration sensor or a set of radio buttons

View 8 more classifications

CN1218276C

China

Download PDF Find Prior Art Similar

Other languages: Chinese

Inventor: 西泽修幸, 石原雅次, 浅川洋介, 白石敦

Current Assignee : Hitachi Ltd , Hitachi Solutions Technology Ltd

Worldwide applications

2000 CN WO JP CN EP US TW 2003 US 2006 US 2009 US

Application CN008194769A events

2000-04-28	Application filed by Hitachi Ltd, Hitachi ULSI Systems Co Ltd
2000-04-28	Priority to PCT/JP2000/002823
2003-10-29	Publication of CN1452763A
2005-09-07	Application granted
2005-09-07	Publication of CN1218276C
2020-04-28	Anticipated expiration
Status	Expired - Fee Related

Info: Patent citations (52), Cited by (135), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (5)

Hide Dependent

1. IC-card is characterized in that it being the IC-card with splicing ear of first functional block that is made of SiC (semiconductor integrated circuit) and second functional block and a plurality of exposures,

Described a plurality of splicing ear has arrangements of observing two row that are front and back formation from the IC-card direction of insertion, and arrangement between the terminal of the splicing ear in first row and the row that are arranged between the terminal of the splicing ear in secondary series upwards are shifted mutually

Described splicing ear comprises first splicing ear that is connected to and is exclusively used in first functional block, is connected to and is exclusively used in second splicing ear of second functional block, and the 3rd splicing ear of sharing the shared operation power supply of first functional block and second functional block,

Splicing ear on the end that extends on the column direction of the splicing ear in being disposed at described secondary series extends to described splicing ear to be pressed close to be disposed in described first row and is positioned at the position of splicing ear of an end that extends at column direction of its splicing ear at column direction, and

Splicing ear on the other end that extends on the column direction of the splicing ear in being disposed at described secondary series extends to described splicing ear and presses close to be disposed in described first row and be positioned at the position of splicing ear of the other end that extends at column direction of its splicing ear at column direction.

2. as the IC-card in the claim 1, wherein said first functional block is the first storage card unit, comprise electrically rewritable first nonvolatile memory, with one first controller, described first controller is according to carrying out the access control of described first nonvolatile memory from the instruction of described first splicing ear and carrying out by the control of described first splicing ear with the interface in the external world

Wherein said second functional block is the second storage card unit, comprise electrically rewritable second nonvolatile memory, with one second controller, described second controller is according to carrying out the access control of described second nonvolatile memory from the instruction of described second splicing ear and carrying out by the control of described second splicing ear with the interface in the external world.

3. as the IC-card in the claim 2, wherein said first controller has function of keeping secret, to writing the data encryption in described first nonvolatile memory and carry out other encryptions to the data decryption read from described first nonvolatile memory or to data,

And described second controller has function of keeping secret, to writing the data encryption in described second nonvolatile memory and carrying out other encryptions to the data decryption read from described second nonvolatile memory or to data.

4. as the IC-card in the claim 2, wherein said first splicing ear comprises clock terminal and data terminal, described second splicing ear comprises clock terminal and data terminal, and described the 3rd splicing ear comprises supply voltage power supply terminal and ground voltage power supply terminal, and

Wherein said first storage card unit and the described second storage card configuration of cells become a parallel work-flow multiple bank storage unit.

5. IC-card is characterized in that it being to have first functional block that is made of SIC (semiconductor integrated circuit) and a splicing ear of second functional block and a plurality of exposures,

Described a plurality of splicing ear has arrangements of observing two row that are front and back formation from the IC-card direction of insertion, and arrange and be arranged in upwards displacement mutually of row at the column direction of the terminal of the splicing ear that is arranged in secondary series at the column direction of the splicing ear that is arranged in first row

Described splicing ear comprises first splicing ear that is connected to and is exclusively used in described first functional block, be connected to and be exclusively used in second splicing ear of described second functional block, and the 3rd splicing ear of sharing the shared operation power supply of described first functional block and second functional block

Described the 3rd splicing ear comprises the splicing ear that is positioned at first row and is used for supply voltage power supply, and provide and the corresponding splicing ear in secondary series so as and power supply power supply splicing ear adjoining position have terminal to the zone between terminal

Description

integrated circuit card

Technical field

The present invention relates to the expansion of the maintenance of the compatibility in the IC-card and function thereof, and relate to a kind of, such as, can under the condition that keeps with the multimedia card compatibility, effectively be applied to IC-card and be used for carrying out multiple bank (multibank) or multi-functional technology.

Background technology

Consider between cell phone and digital network equipment or similar devices and carry out information transmission, proposed a kind of storage card that dimensional weight reduces and interface is simplified of similar multimedia card.As, described in " interface " (in Dec, 1999 distribution) of publishing such as, CQ publishing company. multimedia card has 7 splicing ears as the external interface terminal and adopt serial ports.Compare with the ata interface that PC card or hard disk adopt, this can reduce the load of main system, and even also can obtain for fairly simple system.In addition, same list of references is also mentioned, and has proposed the storage card of a kind of SD card as the top compatibility of multimedia card.

The inventor once discussed the storage system IC-card, as multimedia card or similar card, the function expansion.Like this, the inventor has declared this invention before this: can keep the compatibility to the standardized terminal arrangement of multimedia card or the like when extended terminal is provided, thereby can make function be expanded into possibility, enroll the number (Japanese Laid-Open Patent Application No.2000-18030) that increases data bit In addition, the inventor once discussed the multiple bank that is intended to realize to use this kind extended terminal or multi-functional.Among GSM (the special seminar of the mobile communication) mobile communication system of SIM (subscriber identification module) card that uses IC-card etc., such as, SIM card has a single-chip microcomputer or analog, but storing subscriber information and account information or the like, these informational needs are used for carrying out user's affirmation and security management and realization communication protocol, and set up Nonvolatile memory card, as flash memory.When attempting storage card, as multimedia card, when being applied to the cell phone of this kind gsm mobile communication system, except the SIM card inserting mouth, storage card also needs one to insert mouth Like this, the inventor finds, exists with the space factor room for improvement.In addition, the inventor finds, the difference of safe level come across in the canned data between storage card and the SIM card inevitably and therefore safe level be allowed to be inevitable as multifunctional different.

Summary of the invention

An object of the present invention is to provide a kind of IC-card, can carry out the compatibility that keeps preassigned that terminal is arranged as multiple bank or multi-functional and so on expanded function simultaneously.

Another object of the present invention provides a kind ofly can expand the different multi-functional IC-card of safe level.

Above-mentioned purpose of the present invention, other purposes and new feature can obtain understanding from description of the invention and accompanying drawing.

(1) a kind of IC-card according to the present invention is considered compatibility and function expansion thereof.About the compatibility of IC-card, upward compatibility and downward compatibility can keep.Upward compatibility, such as, be that downward IC-card can the insertion mouth of IC-card uses by inserting upwards.Downward compatibility, such as, be that IC-card can use by the insertion mouth that inserts downward IC-card.IC-card has first functional block and second functional block, and the formation of each all comprises SIC (semiconductor integrated circuit) and has wherein a plurality of splicing ears is the configurations that expose.

With regard to the compatibility of IC-card, a plurality of splicing ears are the tortuous multirows in front and back between the row that are configured as in adjacency observing from the IC-card direction of insertion.If take to be different from the expression of its tortuous configuration, then can be described as a plurality of splicing ears and have one and observe the arrangements of two row that form before and after being from the IC-card direction of insertion, and the terminal in the middle of splicing ear that is arranged in first row arrangement and of terminal area is arranged in secondary series splicing ear in the middle of terminal to displacement mutually on the direction that is arranged in row of terminal area.If tortuous layout is adopted another different expression, then can be described as a plurality of splicing ears and have one and observe the arrangements of two row that form before and after being from the IC-card direction of insertion, and the row of splicing ear that are arranged in first row to layout and the row of splicing ear that are arranged in secondary series to layout in upwards displacement mutually of row.

Because the corresponding multiple row layout of canonical form that the tortuous mode in the arrangement of employing and splicing ear forms can adopt simple relatively structure in card inserting mouth, wherein its a large amount of mouth terminals that insert replace configured in parallel, and the while, its teat quantity changed.The splicing ear of IC-card is arranged and is adopted the splicing ear that is exclusively used in IC-card to arrange as it is downwards On the other hand, arrange if the IC-card special function that will make progress is given another tortuous splicing ear, then this kind can use also by the feasible upwards IC-card of the insertion mouth that is installed on downward IC-card and can realize downward compatibility.

With regard to the expanded function of IC-card, the splicing ear of IC-card comprises first splicing ear that is connected to and is exclusively used in first functional block, be connected to and be exclusively used in second splicing ear of second functional block, and the 3rd splicing ear of sharing the shared operation power supply of first functional block and second functional block.By the data terminal beyond the power supply or other are exclusively used in first functional block and second functional block respectively, can promote the realization of upward compatibility and downward compatibility.

When attempt realizes three generations's IC-card or the above IC-card of three classes compatible, be to have supposed following situation, the splicing ear of first IC-card is arranged by adopting as it is with the corresponding splicing ear row of first row, the special function of adding second IC-card simultaneously to is given and the corresponding splicing ear row of another tortuous secondary series, and the special function of adding the 3rd IC-card to give with the corresponding dedicated terminals row of first row and with the corresponding splicing ear row of secondary series.At this moment, consider the upward compatibility between second IC-card and the 3rd IC-card and the realization of downward compatibility.For this purpose, the structure of adopting is that the splicing ear on the end that extends on the column direction of the wherein splicing ear in being disposed at secondary series extends to splicing ear and presses close to be disposed in first row and be positioned at the position of splicing ear of an end that extends at column direction of its splicing ear at column direction, and the splicing ear on the other end that extends on the column direction of the splicing ear in being disposed at secondary series extends to splicing ear and presses close to be disposed in first row and be positioned at the position of splicing ear of an end that extends at column direction of its splicing ear at column direction.In view of the above, this first to the 3rd IC-card even the insertion mouth and the operable compatibility that can be inserted into other IC-cards mutually can realize at an easy rate.

(2) expansion of the function of this IC-card is intended to, such as, the multiple bank storer.At this moment, first functional block is the first storage card unit, comprise electricity and rewrite first nonvolatile memory, with one first controller, first controller is according to carrying out the access control of first nonvolatile memory from the instruction of first splicing ear and carrying out by the control of first splicing ear with extraneous interface.Second functional block is the second storage card unit, comprise electricity and rewrite second nonvolatile memory, with one second controller, second controller is according to carrying out the access control of second nonvolatile memory from the instruction of second splicing ear and carrying out by the control of second splicing ear with extraneous interface.

If place multimedia card under this kind environment or other to obtain considering, although the special function of each splicing ear is random, then first splicing ear comprises a clock terminal and data terminal, second splicing ear comprises a clock terminal and data terminal, and the 3rd splicing ear comprises supply voltage power supply terminal and ground voltage terminal.

The first storage card unit and the second storage card unit are configured to a parallel work-flow multiple bank storage unit.

In order to increase the safety of data that is stored in each nonvolatile memory, first controller can have function of keeping secret, can be to writing the data encryption in first nonvolatile memory and carrying out other encryptions to the data decryption read from first nonvolatile memory or to data, and second controller can have function of keeping secret, can be to writing the data encryption in second nonvolatile memory and carrying out other encryptions to the data decryption read from second nonvolatile memory or to data.

(3) expansion of the function of this IC-card is intended to multi-functional.At this moment, first functional block is first data processing unit, comprise first nonvolatile memory and one first controller, first controller is carried out the access control of first nonvolatile memory and is carried out by the control of first splicing ear with extraneous interface.Second functional block is second data processing unit, comprises second nonvolatile memory and one second controller, and second controller is carried out the access control of second nonvolatile memory and carried out by the control of second splicing ear with extraneous interface.First data processing unit and second data processing unit have respectively and are used for the zone of storing secret security code separately.

Like this, an IC-card just can be realized the multifunctional equipment that safe level is different.

First data processing unit even can secret identification code be write the secret identification code memory block in the nonvolatile memory production phase.Second data processing unit even can secret identification code be write the secret identification code memory block in the IC-card production phase.Like this, just can set secret identification code by keeping secret necessary method or step according to the difference of safe level.Such as, set the storage card unit that becomes a conventional data storage application when first data processing unit, and second data processing unit is set when becoming microcomputer SIM card unit, then the security of the second data processing unit processing/account executive information is compared with first data processing unit and will be kept strict inevitably, thereby can fully satisfy this kind requirement.

Even ought set the storage card unit that becomes a conventional data storage application by first data processing unit, first controller also preferably adopt can to write in first nonvolatile memory data encryption and to data decryption of reading from first nonvolatile memory or the function of keeping secret that data are carried out other encryptions, purpose is the validity that strengthens copyright protection of being stored in the data in the storage card unit or the like.

When storage card unit and SIM card unit or the like are used as multifunctional equipment, such as, first splicing ear comprises clock terminal, long numeric data terminal and 1 order of the bit terminal, second splicing ear comprises clock terminal, data terminal and reseting terminal, and the 3rd splicing ear comprises supply voltage power supply terminal and ground voltage power supply terminal.

(4) when the splicing ear of supply voltage power supply be disposed at the corresponding splicing ear row of first row of observing from the IC-card direction of insertion the time, be listed in the corresponding splicing ear of secondary series and form in abutting connection with the position of supply voltage power supply splicing ear and have terminal to terminal area.If with other splicing ears of supply voltage power supply terminal adjacency be disposed at the corresponding splicing ear row of the secondary series of winding form in, just might be to insert mouthful in IC-card inserts the process of card inserting mouth, to insert with the terminal of the corresponding card inserting mouth of other splicing ear will both contact the power supply splicing ear of powering before mouthful contacting other splicing ears and also contact other splicing ears that are positioned at other splicing ear fronts.If power supply or power supply insert a mouthful terminal and contact with the supply voltage power supply terminal under this state, with regard to worrying power supply to power supply short circuit.If adopt to guarantee the structure of terminal to terminal area, then can adopt increase with the corresponding splicing ear row of first and second row between distance and the device of the width of each splicing ear of shortening

According to above-mentioned requirements, the invention provides following four kinds of IC-cards.

A kind of IC-card, it is characterized in that it being IC-card with splicing ear of first functional block that constitutes by SIC (semiconductor integrated circuit) and second functional block and a plurality of exposures, described a plurality of splicing ear has arrangements of observing two row that are front and back formation from the IC-card direction of insertion, and arrangement between the terminal of the splicing ear in first row and the row that are arranged between the terminal of the splicing ear in secondary series upwards are shifted mutually, described splicing ear comprises first splicing ear that is connected to and is exclusively used in first functional block, be connected to and be exclusively used in second splicing ear of second functional block, and the 3rd splicing ear of sharing the shared operation power supply of first functional block and second functional block, splicing ear on the end that extends on the column direction of the splicing ear in being disposed at described secondary series extends to described splicing ear to be pressed close to be disposed in described first row and is positioned at the position of splicing ear of an end that extends at column direction of its splicing ear at column direction, and the splicing ear on the other end that extends on the column direction of the splicing ear in being disposed at described secondary series extends to described splicing ear and presses close to be disposed in described first row and be positioned at the position of splicing ear of the other end that extends at column direction of its splicing ear at column direction.

A kind of IC-card, it is characterized in that it being splicing ear with first processing unit and second processing unit and a plurality of exposures, wherein said a plurality of splicing ear comprises first splicing ear that is connected to and is exclusively used in described first processing unit, be connected to and be exclusively used in second splicing ear of described second processing unit, and the 3rd splicing ear of sharing the shared operation power supply of described first processing unit and described second processing unit, wherein said first processing unit is carried out the access control of first nonvolatile memory and is carried out by the control of described first splicing ear with the interface in the external world, wherein said second processing unit is carried out the access control of second nonvolatile memory and is carried out by the control of described second splicing ear with the interface in the external world, wherein said first processing unit uses first secret identification code of storing in a zone of described first nonvolatile memory, and wherein said second processing unit uses second secret identification code of storing in a zone of described second nonvolatile memory.

A kind of IC-card, it is characterized in that it being to have first functional block that constitutes by SIC (semiconductor integrated circuit) and the splicing ear of second functional block and a plurality of exposures, described a plurality of splicing ear has arrangements of observing two row that are front and back formation from the IC-card direction of insertion, and arrange and be arranged in upwards displacement mutually of row at the column direction of the terminal of the splicing ear that is arranged in secondary series at the column direction of the splicing ear that is arranged in first row, described splicing ear comprises first splicing ear that is connected to and is exclusively used in described first functional block, be connected to and be exclusively used in second splicing ear of described second functional block, and the 3rd splicing ear of sharing the shared operation power supply of described first functional block and second functional block, described the 3rd splicing ear comprises the splicing ear that is positioned at first row and is used for supply voltage power supply, and provide and the corresponding splicing ear of secondary series so as and power supply power supply splicing ear adjoining position have terminal to the zone between terminal.

A kind of IC-card, it is characterized in that it being to have first functional block that constitutes by SIC (semiconductor integrated circuit) and the splicing ear of second functional block and a plurality of exposures, wherein said first functional block is carried out the access control to nonvolatile memory, wherein said second functional block is carried out the security control to enciphered data, and described splicing ear comprises first splicing ear that is connected to and is exclusively used in described first functional block, be connected to and be exclusively used in second splicing ear of described second functional block, and the 3rd splicing ear that described first functional block is provided the operation power supply.

Description of drawings

Fig. 1 illustrates one to have with the illustrated example figure of the type of attachment in the middle of splicing ear and the circuit unit as the configuration of main basic multi-functional IC-card according to of the present invention.

Fig. 2 is the illustrated example figure of tabulation that the splicing ear function of multi-functional IC-card is shown.

Fig. 3 is the planimetric map of virtual condition that the circuit installation surface of multi-functional IC-card is shown.

Fig. 4 is the rear view of virtual condition that the circuit installation surface of multi-functional IC-card is shown.

Fig. 5 illustrates the skeleton view of mobile phone appearance.

Fig. 6 illustrates the planimetric map that multi-functional IC-card is installed on the state in the card inserting mouth.

Fig. 7 illustrates the planimetric map that multi-functional IC-card is installed on the state in the card inserting mouth that multimedia card uses.

Fig. 8 is the functional block diagram of storage card unit.

Fig. 9 is the functional block diagram of SIM card unit.

Figure 10 is the functional block diagram that can use the mobile phone of multi-functional IC-card.

Figure 11 illustrates second to have with the illustrated example figure of the type of attachment in the middle of splicing ear and the circuit unit as the configuration of main basic multiple bank storage card according to of the present invention.

Figure 12 is the illustrated example figure of tabulation that the splicing ear function of the multi-functional IC-card among Figure 11 is shown.

Figure 13 illustrates the explanation diagrammatic sketch of power supply to the comparative example of the splicing ear arrangement of power supply short circuit takes place.

Embodiment

< multi-functional IC-card >

Fig. 1 illustrates one to have with the illustrated example figure of the type of attachment in the middle of splicing ear and the circuit unit as the configuration of main basic multi-functional IC-card according to of the present invention.

Be shown in the multi-functional IC-card MFC of Fig. 1 and multimedia card, SD card or the like compatible part and be that the splicing ear 2 (#1 to #13) of card substrate 1 is configured as two row of winding form and the multifunctional equipments that are achieved as follows, promptly storage card unit 3 is respectively only to be mounted for to be connected with the predetermined terminal of splicing ear 2 (#1 to #13) with SIM card unit 4.Label 5 expression connects leads, illustrates to be used for storage card unit 3 and SIM card unit 4 are connected to the general symbol(s) of the line figure, welding lead or the like of splicing ear 2.

Suppose that multi-functional IC-card MFC can be used for being installed on the mobile phone herein.Storage card unit 3 is configured as data-storage applications, and it has a nonvolatile memory, as electric erasing flash memory (its details is stated as follows) and a controller, and telephone book data, melody data of entering or the like is stored in wherein.The formation of SIM card unit 4 comprises a microcomputer that has onboard flash memory, is used for storing subscriber information and account information, and these information confirm for the user of the mobile phone of GSM etc. and user management is essential.

Seemingly be directly connected to storage card unit 3 and SIM card unit 4 though be shown in the splicing ear 2 of the #1 to #13 of Fig. 1, in fact the splicing ear 2 of #1 to #13 is positioned at the back side (terminal surface) of card substrate 1, the connection pads that is connected to its existing splicing ear by through hole or line pattern is the surface (installation surface) that is disposed at card substrate, and storage card unit 3 is connected with these connection pads with SIM card unit 4.

Multi-functional IC-card MFC is based on the size of multimedia card and meet following standard: its thickness is 1.4mm, and planar dimension is 24mm * 32mm.The splicing ear 2 that the card substrate 1 of multi-functional IC-card is configured as #1 to #13 is by resin substrate, as glass epoxy resin etc., on the terminal surfaces of the substrate of making on the plug-in card direction (on its longitudinal direction) observe configuration before and after two row adjacent to each other.

The splicing ear 2 of #1, #2, #5 to #8 and #13 is connected to storage card unit 3, and #9, #11 and #12 are connected to SIM card unit 4, and the splicing ear 2 of power supply #3 that is used for powering and #4 be connected to storage card unit 3 and SIM card unit 4 both.

The splicing ear 2 of #1 to #7 has layout and the function based on the multimedia card standard respectively.General application of multimedia mode card of multimedia card and SPI (serial peripheral interface).The selection of operational mode is according to the state decision of predetermined terminal of when energising.The terminal function of multimedia card is shown in the row of 7 pins (1) among Fig. 2.Multimedia card pattern and SPI mode difference point are shown in the bracket.In the multimedia card pattern, #1 is as keeping terminal NC (open a way or be fixed in logical value " 1 "), #2 is as command terminals CMD (fill order input and and answer signal output), #3 and #6 are used separately as circuit ground voltage (ground connection) terminal Vss1 and Vss2, #4 is as supply voltage power supply terminal Vdd, #5 is as clock input terminal CLK, and #7 is as data input/output terminal Data.In SPI (serial peripheral interface) pattern, #1 selects terminal CS as chip, #2 is as the sub-Din of data input pin (being used for from main equipment to card input data and order), #3 and #6 are used separately as circuit ground voltage (ground connection) terminal Vss1 and Vss2, #4 is as supply voltage power supply terminal Vdd, #5 is as clock input terminal CLK, and #7 is as the sub-Dout of data output end (carry out and snap into the data of main equipment and the output of state from storage).The multimedia card pattern is the operational mode that is suitable for using simultaneously the system of a plurality of multimedia cards.In order to discern corresponding multimedia card, adopt with the multimedia card initial order and multimedia card is set card identification id (relative address) by not shown main equipment.The SPI pattern is suitable in the system of simple cheap most.The selection of multimedia card is carried out according to the chip select signal that offers the #1 splicing ear from main equipment.In any operational mode, the command execution that the controller of storage card unit 3 response main equipment provides to the access control of storage chip and to the control of the interface of main equipment.

The splicing ear 2 of #8 to #13 is as the extended terminal to multimedia card.The splicing ear 2 of #1 to #7 constitutes arranging with the corresponding splicing ear of first row of relative card substrate 1, and the additional splicing ear 2 of #8 to #13 constitutes and the corresponding splicing ear arrangement of second row, and this journey is positioned at the corresponding splicing ear of first row arranges the position of leaving.The size of the splicing ear 2 of #9 to #12 is identical with other splicing ears 2.The splicing ear 2 of #13 places first row and observes the position that an end of arranging at splicing ear extends to thoroughly close #7 from its orientation.Be positioned at first row with the corresponding splicing ear 2 of terminal #8 and observe to extend to partly and overlap and adjoining position with the #1 splicing ear that splicing ear is arranged from its orientation.Arrange with the corresponding splicing ear of first row and arrange, observe displacement mutually the capable layout of splicing ear from line direction with the corresponding splicing ear of second row.In other words, arranging and arrange with the corresponding splicing ear of second row with the corresponding splicing ear of first row is to be configured as meander-shaped.

4 bit patterns shown in the row of 9 pins (4) of the extended terminal of #8 to #13 in Fig. 2 are selected when being used for multi-functional IC-card MFC is effective terminal.In other words, when selecting 4 bit patterns, the terminal of #2 to #7 is endowed and the corresponding identical pattern of multimedia card pattern.In corresponding multimedia card pattern, be used as the terminal #1 that keeps terminal, as and the 4th corresponding data terminal Data3, additional terminal #8 and #9 be used separately as with second corresponding data terminal Data1 and with the 3rd corresponding data terminal Data2.With first corresponding data terminal Data0 corresponding to the terminal #7 identical with the multimedia card pattern.Like this, when multi-functional IC-card MFC was selected 4 bit patterns, the I/O of data was enabled with 4 bit parallels At this moment, consider #8 to #13 splicing ear 2 shape will with the splicing ear compatibility of SD card.The data terminal function of #8 to #13 can transposition in 4 bit patterns.4 bit patterns also can have the compatibility with the SD card.

The storage card unit 3 of multi-functional IC-card MFC disposes the backward compatible pattern to multimedia card.In other words, the controller in the storage card unit 3 has the SPI pattern of multimedia card or is similar to 1 bit pattern of multimedia card pattern, and uses 4 bit data terminal #1, #7, #8 and #13 to carry out 4 bit patterns of data I/O with 4 bit parallels.1 bit pattern is to allow the operational mode of multi-functional IC-card MFC as multimedia card.

Operational mode can respond the state of predetermined splicing ear or set from the state of predetermined splicing ear order input.When multi-functional IC-card MFC was installed on the card inserting mouth of multimedia card, terminal #8 and #13 became unsteady.Therefore, controller can detect terminal #8 and #13 or any one quick condition wherein (floating state) and multi-functional IC-card is set at 1 bit pattern when energising.When it is installed on have respectively with the special-purpose card inserting mouths of 9 splicing ears, 2 corresponding card inserting mouth terminals in the time, make the card inserting mouth terminal corresponding of terminal #8 and #9 importing card inserting mouth with it.Therefore, when energising controller detect from main equipment to both or any one special signal or order that provides terminal #8 and the #9 at least, thereby can set 4 bit patterns to multi-functional IC-card MFC.

Extended terminal #9 to #12 is respectively the dedicated terminals that is connected with SIM card unit 4.The formation of SIM card unit 4 comprises that has a built-in nonvolatile memory, as flash memory, single-chip microcomputer.#9 represents data input/output terminal I/O, and #10 represents not splicing ear, and #11 represents clock terminal CLK, and #12 represents reseting terminal.The operate power of SIM card unit 4 is through #3 ground terminal Vss and #4 power supply terminal Vdd supply.If mobile phone etc. provide the corresponding card inserting mouth of describing in the row with 13 pins in Fig. 2 of terminal arrangement, and multi-functional IC-card MFC is installed in the card inserting mouth, then storage card unit 3 and SIM card unit 4 independent operating mutually.If multi-functional IC-card MFC is connected with personal computer etc. through card adapter etc., then corrects on the storage card of telephone book data or the like in multi-functional IC-card MFC and can implement expeditiously.

The planimetric map of the virtual condition of the circuit installation surface among the multi-functional IC-card MFC shown in Figure 3, and in Fig. 4 the virtual condition of terminal surfaces.The splicing ear 2 that the card substrate 1 of multi-functional IC-card is configured as #1 to #13 is by resin substrate, as glass epoxy resin etc., arrange with 2 row on the terminal surfaces of the substrate of making, in (on its longitudinal direction) observation configuration before and after row adjacent to each other on the plug-in card direction.Connection pads 7 is formed on installation or the package surface correspondingly with splicing ear 2.Connection pads 7 is formed by the conductive pattern of aluminium, copper or copper or ferroalloy or the like respectively.Gold-plated or nickel plating or the like forms splicing ear 2 by the conductive pattern that makes aluminium, copper or copper or ferroalloy or the like.The electrical connection of connection pads 7 and splicing ear 2 makes the front and rear surfaces conducting of card substrate 1 by enforcements such as wire pattern on the not shown card substrate 1 and through holes.

Storage card unit 3 has, and such as, electrically rewritable flash memory 8 be used for controlling the controller 9 of flash memory 8, all is disposed on the installation surface of card substrate 1.Although be not particularly limited, flash memory 8 and controller 9 have independently semi-conductor chip formation respectively.Certainly, both can be made by a chip or together by forming different chips is bonded to each other.

Controller 9 is according to the read-write operation of the instruction control flash memory 8 that provides from the corresponding splicing ear 2 of outside warp.When considering data security, controller 9 can also further be configured as to have the enciphered data of making and writes flash memory 8 and the data of reading from flash memory 8 are implemented deciphering or to applying close function of keeping secret in fact.

Controller 9 has shape long on vertical or the vertical direction, extends along the orientation of splicing ear 2.In splicing ear 2 sides, controller 9 comprises a plurality of connecting interface terminal 9Pi, is connected with splicing ear 2 through connection pads 7 respectively, and in flash memory 8 sides, comprises that a plurality of memory interface terminal 9Pj are connected with flash memory 8.Flash memory 8 has a plurality of control unit interface terminal 8Pk and is connected with controller 9 in controller 9 sides.Connection pads 7 is connected to the connecting interface terminal 9Pi corresponding with it of controller 9 by welding lead 10.The memory interface terminal 9Pj of controller 9 is connected to the control unit interface terminal 8Pk corresponding with it of flash memory 8 by welding lead 11.Connecting interface terminal 9Pi has respectively and #1 to #8 and the corresponding terminal function of #13.Memory interface terminal 9Pj is respectively, such as, be used for controlling the terminal of flash memory 8, and corresponding with a plurality of terminals with following function, export, write enable signal as chip enable signal and

export, order enable signal output, data I/O, the output of output enable signal, the output of ready/busy signal, reset signal to export or the like.Control unit interface terminal 8Pk is a plurality of terminals with following function, as chip enable signal input, write enable signal input, the input of order enable signal, data I/O, the input of output enable signal, the input of ready/busy signal, reset signal and import or the like.In addition, card substrate 1 comprises calibrating terminal 13, is connected with controller 9 and flash memory 8 by welding lead (wire pattern) 12.

SIM card unit 4 is connected with connection pads 7 corresponding to #9, #11 and #12 through welding lead 17A.The operation power supply supply of SIM card unit 4 is such as providing through welding lead 17B.A pair of welding lead with label 16 marks is the interface lead that is used for connecting controller 9 and SIM card unit 4.Welding lead is to allowing in storage card unit 3 and SIM card unit 4 intermediate conveyor information.

Card substrate 1 is installed on and is fixed in housing 14, and its installation surface is towards its inside.Installation surface has housing 14 to cover and protection, and its terminal surfaces exposes from housing 14.

Outer Fig. 5 that is shown in of mobile phone.Multi-functional IC-card MFC is installed in the card inserting mouth of determining in the side of mobile phone 20.

Fig. 6 illustrates multi-functional IC-card MFC to be installed on state diagram in the card inserting mouth 21.Card inserting mouth 21 has card inserting mouth terminal 22 at its back side, and card inserting mouth terminal 22 outstanding and corresponding splicing ears 2 combine.Because splicing ear 2 is arranged as two row of meander-shaped, the card inserting mouth terminal (22 (L)) that the card inserting mouth terminal 22 of the card inserting mouth 21 that its overhang is little (22 (S)) and its length are long can alternately change in meanders Can adopt a kind of fairly simple configuration, wherein card inserting mouth terminal 22 is whole parallel, and the overhang of card inserting mouth terminal 22 is changed.The contact of contact splicing ear 2 is corresponding to the tip portion (with the ● mark) of card inserting mouth terminal 22.

Fig. 7 illustrates multi-functional IC-card MFC and is installed on situation in the card inserting mouth 23 that multimedia card uses.Because the arrangement of the splicing ear 2 of the #1 to #7 of multi-functional IC-card MFC is based on multimedia card, multi-functional IC-card MFC can be installed in the card inserting mouth 23 that multimedia card uses so that even be complementary with the application of independent use storage card unit 3.Label 24 is represented the card inserting mouth terminal of card inserting mouth 23 respectively, and this card inserting mouth terminal can be connected with the splicing ear 2 of #1 to #7.

Fig. 8 is depicted as the functional block diagram of storage card unit 3.Controller 9 has an interface controller 30, flash controller 32, encrypting and decrypting circuit 33 and secure circuit 34.Interface controller 30 is connected to mobile phone 20 through splicing ear 2, thereby and the command decode that mobile phone 20 is provided so as to carry out to the general control of the inside of storage card unit 3 and to the control of the interface of mobile phone 20.Although be not specifically limited, this kind control program or state exchange steering logic provide in interface controller 30 inside.Control program can place in the flash memory 8.

Interface control is with equivalent through the interface control of splicing ear 2 based on multimedia card pattern or SPI pattern.The general control of the inside of storage card unit is comprised the authentication control that utilizes secure circuit 34 as the first step, as the encrypt/decrypt control to the I/O data of flash memory 8 in second step, and the access control of carrying out through the file memory to flash memory 8 of flash controller 32.

Access control is a kind of consideration, such as, with the sector be the control of compatibility of the basic file system of data management.In order to manage data or the file in 512 byte sector units, such as, the storage that utilizes electricity to rewrite flash memory 8 is arranged, the directorial area that its data field that to be divided into a sector be 512 bytes and each data field are provided with.Each directorial area comprises the information of indication sector user mode, such as, data of whether remaining valid with to the directional information of next sector in corresponding data field, or the like.Sector management table 35 of the whole composition of these directorial areas.When access control, the sector of the file of ready access combines with the corresponding physical address that its electricity is rewritten flash memory 8, and the result makes can carry out each storage operation, as reads, wipes, writes and verification or the like

Encrypting and decrypting control is carried out, such as, make encrypting and decrypting circuit 33 at first to the data encryption that writes flash memory 8 and allow enciphered data to write the process of flash memory 8, and make 33 pairs in encrypting and decrypting circuit utilize flash controller 32 to rewrite data decryption or the logarithm that flash memory 8 reads to execute another time encryption factually, and allow treated data to output to the outside from interface controller 30 from electricity.The encrypting and decrypting method can adopt the suitable algorithm of utilizing private key or private key and PKI.

The following describes authentication control.Supposing to use storage card unit 3 to wait by mobile phone 20 provides music information, literature information or the like, then preferably considers the copyright protection to these information When telephone number or the like is stored in the storage card unit 3 and uses, will require the secret protection of this kind information and executing.

Although copyright protection is not specifically limited, in the fabrication phase of electricity rewriting flash memory 8, the predetermined authentication codes of relevant right of duplicating is write electricity and rewrite in flash memory 8 specific regions.When information provided, the relevant authentication codes that duplicates right sent to mobile phone 20 or the like from main equipment.This is arranged in the authorization code admin table 36 of secure circuit 34.The information that combines with authorization code that provides, such as, flash memory 8 is downloaded and write to music information or the like.It is write memory address and combines with authorization code and be arranged in the authorization code admin table 36 of secure circuit 34.Afterwards, multi-functional IC-card MFC takes off and this time appends to one from mobile phone 20 and duplicates end device etc.Respond the request of access that this end device sends, the interface controller 30 of multi-functional IC-card MFC makes secure circuit 34 utilize authorization code admin table 36 to judge whether the file storage address that is intended to visit is the memory block that combines with authorization code in the authorization code admin table 36.When the memory block is when combining with authorization code, secure circuit 34 does not allow file access, rewrites predetermined pass between the authorization code of flash memory 8 and ties up to its fabrication phase and set up unless remain in the authorization code in the secure circuit 34 and write electricity.Authorization code admin table 36 can be rewritten nonvolatile memory by electricity and constitute.Authorization code admin table 36 can place interface controller 30 or flash memory 8.

In case secret cognizance code is from an equipment; such as; mobile phone; be set in the secret cognizance code admin table 37 of secure circuit 34, as relevant secret protection described; finish at each multi-functional IC-card MFC initialization procedure, when request was for the first time carried out read access to electricity rewriting flash memory 8, secure circuit 34 required the corresponding secret cognizance code of interface controller 30 inputs.Before outside input and secret cognizance code that secret cognizance code being arranged at secret cognizance code admin table 37 is consistent, the memory access that secure circuit 34 makes interface controller 30 stop to respond read request is controlled.Secret cognizance code admin table 37 can be rewritten nonvolatile memory by electricity and constitute Authorization code admin table 36 can place interface controller 30 or electricity to rewrite flash memory 8.

Fig. 9 illustrates the functional block diagram of SIM card unit 4.SIM card unit 4 can be by chip microcontroller, it comprises CPU (CPU (central processing unit)) 40, be used as the RAM (random access memory) 41 of the workspace of CPU 40, be kept for the ROM (ROM (read-only memory)) 42 of the running program or the like of CPU 40, be used for carrying out serial interface circuit (SIO) 43 and flash memory 44 the data I/O of outside.In gsm mobile communication system, SIM card unit 4 keeps the telephonist of GSM to support and the necessary user profile of authentication/management GSM user, as the user profile of store/manage about security, and generation/leading subscriber PIN (personal identity number) or the like.In addition, SIM card unit 4 keeps account information, and GSM serves information necessary, as cripetura dialing/target Fixed Dialing or the like.CPU 40 carries out these information is retained in the flash memory 44 also by using RAM 41 these information of management.The program that in RAM 42, keeps its execution.In addition, the SIM card unit 4 implements communication agreement implementation, file management and safety managements.Safety management is by using authentication codes, as user PIN, confirms the validity of user's use authority and the validity of using

system.Though concrete authentication formality is not described in detail the authentication codes that GSM service provider serves with the man-to-man corresponding relation storage GSM to each user in advance in the flash memory 44 of SIM card unit 4 Use the authentication codes that is registered in advance in the SIM card unit 4 to come to consistent with the code in being input to SIM card unit 4 such as all calling judgements.Validity is to confirm according to this judged result.Also have the relation with accounting, and therefore the safe level of SIM card unit 4 is set usually than the safe level height of storage card unit 3.In multi-functional IC-card MFC, SIM card unit 4 and storage card unit 3 are endowed intrinsic splicing ear respectively as the data input/output terminal.So, to its secret identification code, as security information, read-write just can carry out independently.This makes can carry out different transaction mutually aspect safe level.In other words, allow the difference on the safe level as multi-functional difference.

Can use the functional block diagram of the mobile phone of multi-functional IC-card MFC shown in Figure 10.

Microphone 51 is caught and is grabbed sound and be transformed to digital audio signal as the analog audio signal and by A/D transducer 52, is input to data processor 53 then.Data processor 53 is carried out acoustic coding processes and channel encode-decode process or the like and is handled and export treated signal as sending signal as the layer to the digital audio signal that receives.Although do not specifically illustrate, can utilize DSP to carry out acoustic coding processing and channel coding/decoding processing.Although do not specifically illustrate, data processor 53 can be set up accelerator for channel coding and decoding device and sound coder-decoder therein.

By the transmission signal of data processor 53 generations, by, such as, GMSK modulation circuit 54 is modulated, and further is transformed to simulating signal by D/A transducer 55, sends from high frequency transmitting element (RF transmitting element) by antenna 57 again.

The signal that antenna 57 receives is received by high frequency receiving element (RF receiving element) 58 and is transformed to digital signal by A/D transducer 59, sends into data processor 53 afterwards.Data processor 53 is carried out Viterbi (Viterbi) decode procedures, and voice codec process or the like is to take out sound or audio signal and with its output.The Veterbi decoding process, voice codec process or the like is carried out by DSP or not shown accelerator.

The audio signal of these data processor 53 outputs is transformed to the analog audio signal by D/A transducer 60, is re-used as sound through loudspeaker 61 outputs.

Data processor 53 in the mobile phone 20 shown in Figure 10 comprises CPU (central processing unit) (CPU) 62, direct memory access controller (DMAC) 63, the ROM (read-only memory) (ROM) 64 of working procedure of maintenance CPU 62 usefulness or the like, be used as the random access storage device (RAM) 65 of the workspace of CPU 62, and input/output circuitry (I/O) 66, as input/output end port, serial ports etc.In the example of this mobile phone 20, although be not particularly limited, running program, as be used for the acoustic coding decode procedure of acoustic coding/decoding, system's control procedure of carrying out as the channel encode-decode process of layer process and by data processor 53 or the like remains among the ROM 64.The process that is used to DMAC 63 to set transmission controlled condition is implemented by being stored in ROM 64 corresponding running programs by CPU 62 execution.

Although be not particularly limited, input switch unit 70, display controller 71 and card interface controller 72 are connected to the I/O 66 of data processor 53.But input switch unit 70 comprises a large amount of input switches that function is specified input digit and character that passes through.Multi-functional IC-card MFC and data processor 53 middle interfaces that card interface controller 72 is implemented to be installed in the card inserting mouth 21 are controlled.Data processor 53 has carries out following control function: show suitably on LCD 75 that through display controller 71 state of mobile phone 20 is as sending telephone number, caller ID, communications status, cell voltage or the like

< multiple bank storage card >

Figure 11 illustrates second to have with the illustrated example figure of the type of attachment in the middle of splicing ear and the circuit unit as the configuration of main basic multiple bank storage card according to of the present invention.

Multiple bank storage card MBC shown in Figure 11 has with multi-functional IC-card MFC shown in Figure 1 and similarly arranges.The splicing ear 2 of #1 to #13 on the card substrate 1 is configured as 2 row of winding form.Storage card unit 3 is connected with the splicing ear 2 of #1 to #13 with 3A and forms the multiple bank storer of parallel running.Label 5 expression connects leads, illustrates to be used for storage card unit 3 and 3A are connected to the general symbol(s) of the line figure, welding lead or the like of splicing ear 2.

Storage card unit 3 is connected to the splicing ear 2 of #1 to #8 and #13 and has the configuration same with the storage card unit 3 of multi-functional IC-card MFC shown in Figure 1.Like this, storage card unit 3 can use as the multimedia card shown in 7 pins among Figure 12 (1 's) the row in mode described above.In addition, the similar mode of SD card that illustrates during storage card unit 3 can be listed as with 9 pins (4) with Figure 12 is carried out the I/O operation of 4 bit parallel data.When being connected to card inserting mouth as mentioned above, its operational mode is determined according to the state of splicing ear 2.As mentioned above, the multimedia card pattern and with the SPI pattern of the operational mode of multimedia card compatibility according to to by main equipment the appointment during to 3 initialization of storage card unit determine.

Storage card unit 3A only has as the function that can carry out based on the storage card of 1 bit serial I/O of multimedia card.The power supply of storage card unit 3A has ground voltage Vss1, supply voltage Vdd and ground voltage Vss2, and from #3, #4 and #6 share with storage card unit 3.In the multimedia card pattern, #9 is as keeping terminal NC-2 (open a way or be fixed in logical value " 1 "), #10 is as command terminals CMD-2 (being used for fill order input and answer signal output), and #11 is as clock input terminal CLK-2, and #12 is as data input/output terminal Data-2.In the SPI pattern, #9 selects terminal CS-2 (negative logic) as chip, #10 is as the sub-Din-2 of data input pin (being used for from main equipment to card input data and order), #11 is as clock input terminal CLK-2, and #12 is as the sub-Dout-2 of data output end (carry out and snap into the data of main equipment and the output of state from storage).As mentioned above, multimedia card pattern and SPI pattern according to to by main equipment the appointment during to the 3A initialization of storage card unit determine.

When multiple bank storage card MBC shown in Figure 11 is installed on as shown in Figure 6 the card inserting mouth with 13 card inserting mouth terminals 22 21 so that during with host device interface, can introduce the operational mode of storage card unit 3 and 3A when two storage card unit 3 and 3A concurrent working respectively, at first be to be used for the both is set at the multimedia card pattern in the multimedia card compatibility mode in 13 pins (A) row that are shown in Figure 12 or the form of SPI pattern.Secondly, as shown in 13 pins (B) row of Figure 12, operational mode is to be used for that storage card unit 3 is set at the form of the pattern that can carry out 4 bit parallel I/O and to be used for the form of the multimedia card pattern in the multimedia card compatibility mode that storage card unit 3A is set at.In all case, main equipment can controlling packet be contained in the IC-card mutually independently two storage card unit 3 and 3A, and even can make its parallel running fully.

< prevent that power supply is to power supply short circuit >

In multi-functional IC-card MFC shown in Figure 1 and multiple bank storage card MBC shown in Figure 11, the power supply of the arrangement of two row splicing ears 2 is to power supply short circuit before and after having considered to prevent.In above-mentioned example, there is not terminal at rear portion with the corresponding #4 terminal of power connector end.When splicing ear 2 was configured as winding form shown in Figure 6, short terminal 22 (S) in the card inserting mouth terminal 22 of card inserting mouth 21 and long terminal 22 (L) were alternately configurations thick and fast, each spacing equal each splicing ear 2 spacing 1/2.On the other hand,

if the rear portion does not have splicing ear 2 to exist, as occasion, then at the not long card inserting mouth terminals 22 in both sides (L) of the card inserting mouth terminal 22 (Vdd) of the splicing ear 2 of the #4 that is equivalent to be used to provide supply voltage (Vdd), as shown in Figure 6 at #4.

Suppose IC-card 25, contrast illustrates as Figure 13 (A), and the rear portion that the data terminal of #10 and #11 is disposed at #4 is used to provide supply voltage (Vdd).With IC-card 25 corresponding card inserting mouths 26 in, long card inserting mouth terminal 26Ab is disposed at the adjoiner with the corresponding card inserting mouth terminal of the splicing ear of #4 26Aa

When the IC-card 25 of Figure 13 inserts card inserting mouth 26, the superficial sliding contact of the splicing ear of the splicing ear of the #4 of the contact point of card inserting mouth terminal 26Ab (with the position of ◙ mark) and input supply voltage Vdd and the #3 of input circuit ground voltage Vss is shown in Figure 13 (B).At this moment, when the splicing ear conducting of card inserting mouth terminal 26Aa that has supply voltage Vdd and #4 and have the card inserting mouth terminal 26Ac of circuit ground voltage Vss and during the splicing ear conducting of #3, supply voltage Vdd and ground voltage Vss are through the contact point short circuit of contact point and #3 and the 26Ac of contact point, #4 and the 26Ab of 26Aa, shown in Figure 13 (C).

Because, as shown in Figure 6, there is not splicing ear at rear portion with the terminal of the corresponding #4 of power connector end, the possibility of this kind power supply short circuit can prevent from can not take place.

Though the inventor is the specific embodiment shown in the basis to the description of the invention described above, the invention is not restricted to this.In the scope that does not break away from spirit of the present invention, can carry out various changes to it.

Such as, the present invention even can be applicable to get rid of the storage card of the outside standard of multimedia card, such as, based on the IC-card of other standards, as pocket flash memory or the like.Therefore, the function of the number of the size of card substrate, splicing ear and splicing ear all is not limited to above-mentioned and can suitably changes The storer that is installed to IC-card of the present invention is not limited to nonvolatile memory.Storer can be volatile memory (SRAM, DRAM or the like).Nonvolatile memory is not limited to flash memory and can makes ferroelectric memory.

The present invention can be used as IC-card and is applied to as GSM mobile handset, and other personal digital assistants.The present invention also can be used as the multiple bank IC-card and is widely used in the auxilary unit in digital camera, digital static camera and other electronic installations.In addition, the function of bank book, credit card, IC-card or the like also can combine as the function of multi-functional IC-card with memory function.

Patent Citations (52)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US3934122A *	1974-08-15	1976-01-20	Ricciteili James A	Electronic security card and system for authenticating card ownership
US4447716A *	1982-03-01	1984-05-08	Seiichiro Aigo	Information card
JPH041683082 *	1984-01-31	1992-03-25	Tokyo Shibaura Electric Co	
US4650975A *	1984-08-30	1987-03-17	Casio Computer Co., Ltd.	IC card and an identification system thereof
US4641193A *	1984-12-07	1987-02-03	New York Institute Of Technology	Video display apparatus and method
JPS6389586A *	1986-06-30	1988-01-16	Toshiba Corp	Memory card
JPS63176193A *	1987-01-14	1988-07-20	Nec Corp	Information card
JPH0261680A	1988-08-26	1990-03-01	Seiko Instr Inc	Contact type heat fixing device
JPH0261680U	1988-10-27	1990-05-08		
JP2712497B2 *	1989-03-02	1998-02-10	キヤノン株式会社	Solid camera
US5237609A *	1989-03-31	1993-08-17	Mitsubishi Denki Kabushiki Kaisha	Portable secure semiconductor memory device
US5236372A *	1991-02-20	1993-08-17	Nec Corporation	No-insertion force connector assembly
JPH0557635A	1991-08-27	1993-03-09	Matsushita Electric Works Ltd	Driving tool
EP0532166B1 *	1991-09-11	1995-06-14	ITT INDUSTRIES, INC. (a Delaware corporation)	Memory card grounding apparatus
JP3231882B2	1991-11-26	2001-11-26	株式会社日立製作所	Semiconductor disk using flash memory as storage medium
TW261678	1991-11-26	1995-11-01	Hitachi Seisakusyo Kk	
FR2686171B1 *	1992-01-14	1996-09-06	Gemplus Card Int	MASS MEMORY CARD FOR MICROCOMPUTER WITH FACILITIES FOR EXECUTING INTERNAL PROGRAMS.
FR2698195B1 *	1992-11-19	1994-12-16	Gemplus Card Int	Encryption and authentication method and circuit for synchronous memory card.
ATS183888T *	1993-06-15	2011-08-15	Celltrace Llc	TELECOMMUNICATIONS SYSTEM
DE69318839T2 *	1993-10-22	1998-11-12	Molex Inc	System for discharging electrical charges in connection with memory card connectors

JPH07302318A *	1994-03-09	1995-11-14	Seiko Epson Corp	Card type electronic device
IT1272863B *	1995-01-04	1997-07-01	Ausimont Spa	THERMOPROCESSABLE COPOLYMERS OF TETRAFLUOROETHYLENE
DE19536169A1 *	1995-09-29	1997-04-03	Ibm	Multifunctional chip card
US5999811A *	1996-02-16	1999-12-07	Ericsson, Inc.	Mobile telephone for roaming using dual mode/band equipment including SIM cards
JP3774260B2 *	1996-03-25	2006-05-10	株式会社ルネサステクノロジ	Memory card security system device and memory card thereof
US5772448A *	1996-04-02	1998-06-30	Compaq Computer Corporation	Edgecard circuit board
DE19617943C2 *	1996-04-29	1998-12-17	Mannesmann Ag	Process for making microprocessor cards accessible
US5828753A *	1996-10-25	1998-10-27	Intel Corporation	Circuit and method for ensuring interconnect security within a multi-chip integrated circuit package
US5839058A *	1996-11-01	1998-11-17	Ericsson Inc.	Recyclable cellular telephone and method and apparatus for supporting the use of a recyclable cellular telephone within a cellular telephone network
JPH10334205A *	1997-05-30	1998-12-18	Toshiba Corp	Ic card and memory package
US6094724A *	1997-11-26	2000-07-25	Atmel Corporation	Secure memory having anti-wire tapping
FR2773900B1 *	1998-01-22	2000-02-18	Gemplus Card Int	CARD WITH INTEGRATED CONTACT CIRCUIT (S), COMPRISING A DETACHABLE MINICARD
JPH11273400A	1998-03-24	1999-10-08	Hitachi Ltd	Storage
JPH11282989A *	1998-03-26	1999-10-15	Toshiba Corp	Portable electronic device
US6315195B1	1998-04-17	2001-11-13	Diebold, Incorporated	Transaction apparatus and method
FR2779849B1 *	1998-06-15	2000-07-28	Schlumberger Ind Sa	SECURE INTEGRATED CIRCUIT DEVICE USING COMPLEMENTARY BUS LINES
JP4029234B2 *	1998-07-16	2008-01-09	ソニー株式会社	Information processing apparatus and information processing method
US6401208B2 *	1998-07-17	2002-06-04	Intel Corporation	Method for BIOS authentication prior to BIOS execution
US5933328A *	1998-07-28	1999-08-03	Sandisk Corporation	Compact mechanism for removable insertion of multiple integrated circuit cards into portable and other electronic devices
GB9822697D0 *	1998-10-19	1998-12-09	Nokia Mobile Phones Ltd	Data card holder
FI107973B	1999-03-11	2001-10-31	Nokia Mobile Phones Ltd	Method and means for using option cards in a mobile station
JP3389186B2 *	1999-04-27	2003-03-24	松下電器産業株式会社	Semiconductor memory card and reading device
US6634561B1 *	1999-06-24	2003-10-21	Sandisk Corporation	Memory card electrical contact structure
JP3815936B2	2000-01-25	2006-08-30	株式会社ルネサステクノロジ	IC card
CN1218276C *	2000-04-28	2005-09-07	株式会社日立制作所	IC card
US20030112613A1 *	2002-10-22	2003-06-19	Hitachi, Ltd.	IC card
TW516296B *	2000-07-20	2003-01-01	High Tech Comp Corp	Plug-and-play SIM card holder
JP4671484B2	2000-10-11	2011-04-20	ケル株式会社	Card connector
TW495110U	2000-11-27	2002-07-11	Kinpo Elect Inc	Common seat for memory card
GB2377825A	2001-07-19	2003-01-22	Inventec Appliances Corp	Device with expansion adaprot slotted into battery
US6612492B1	2002-06-06	2003-09-02	Chant Sincere Co., Ltd.	Four-in-one memory card insertion port
DE10303740B4 *	2003-01-30	2006-09-14	Infineon Technologies Flash Gmbh & Co. Kg	Security memory card and manufacturing process

* Cited by examiner, † Cited by third party

Cited By (135)

Publication number	Priority date	Publication date	Assignee	Title
CN101765242A *	2008-12-25	2010-06-30	深圳富泰宏精密工业有限公司	User identification card and connector thereof as well as portable communication device provided with connector
Family To Family Citations				
TW460846B *	1998-12-10	2001-10-21	Toshiba Corp	Data recording media having certification information
JP3822768B2 *	1999-12-03	2006-09-20	株式会社ルネサステクノロジ	IC card manufacturing method
JP3815936B2 *	2000-01-25	2006-08-30	株式会社ルネサステクノロジ	IC card
CN1218276C *	2000-04-28	2005-09-07	株式会社日立制作所	IC card
US20030112613A1 *	2002-10-22	2003-06-19	Hitachi, Ltd.	IC card
US7295443B2	2000-07-06	2007-11-13	Onspec Electronic, Inc.	Smartconnect universal flash media card adapters
US6438638B1	2000-07-06	2002-08-20	Onspec Electronic, Inc.	Flashtoaster for reading several types of flash-memory cards with or without a PC
US6824063B1	2000-08-04	2004-11-30	Sandisk Corporation	Use of small electronic circuit cards with different interfaces in an electronic system
KR20020016430A *	2000-08-25	2002-03-04	윤종용	Multimedia modular card, modular card operating device and incorporated multimedia system
US7107378B1	2000-09-01	2006-09-12	Sandisk Corporation	Cooperative interconnection and operation of a non-volatile memory card and an input-output card
US7137003B2 *	2001-02-27	2006-11-14	Qualcomm Incorporated	Subscriber identity module verification during power management
JP2002259869A *	2001-03-01	2002-09-13	Fujitsu Ltd	Method of controlling portable equipment, method of preventing illicit use of ic card, program for changing setting of portable equipment, and program for preventing illicit use of ic card
US7066819B2	2001-03-29	2006-06-20	Interactive Telegames, Llc	Method and apparatus for identifying game players and game moves
US20020183118A1 *	2001-05-30	2002-12-05	Scott Wolinsky	Method and apparatus for simulating game accessories
AU2003220678A1	2002-04-08	2003-10-27	Socket Communications, Inc	Wireless enabled memory module
US7090256B1	2002-04-26	2006-08-15	Sandisk Corporation	Retractable card adapter
US20030211888A1	2002-05-13	2003-11-13	Interactive Telegames, Llc	Method and apparatus using insertably-removable auxiliary devices to play games over a communications link
JP2004126889A *	2002-10-01	2004-04-22	Sharp Corp	Electronic seal, removable memory medium, advance authentication system, portable device, cellular telephone system, and vihicular starting controller
US7137051B2 *	2002-10-23	2006-11-14	Micron Technology, Inc.	Testing a multibank memory module
US7366803B2	2002-11-13	2008-05-06	Sandisk Corporation	Universal non-volatile memory card used with various different standard cards containing a memory controller
US8037229B2	2002-11-21	2011-10-11	Sandisk Technologies Inc.	Combination non-volatile memory and input-output card with direct memory access
US20050055479A1 *	2002-11-21	2005-03-10	Aviad Zer	Multi-module circuit card with inter-module direct memory access
JP4152178B2 *	2002-12-03	2008-09-17	株式会社ルネサステクノロジ	Memory card and electronic device
JP2004240795A *	2003-02-07	2004-08-26	Renesas Technology Corp	Nonvolatile storage device
US20040164170A1 *	2003-02-25	2004-08-26	Marcelo Krygier	Multi-protocol memory card
JP4308551B2 *	2003-03-06	2009-08-05	株式会社ルネサステクノロジ	Memory card and host device
JP3958243B2 *	2003-04-14	2007-08-15	松下電器産業株式会社	IC card and its OS startup method

US7305535B2 *	2003-04-17	2007-12-04	Sandisk Corporation	Memory cards including a standard security function
US20040245620A1 *	2003-06-03	2004-12-09	Jackson Hsieh	Memory card capable of indicating an inserting direction
EP1647136A4	2003-06-09	2009-07-08	Wavien Inc	A light pipe based projection engine
KR20100107057A *	2003-07-03	2010-10-04	로데사스 일렉트로닉스 가부시키가이샤	Semiconductor card device
US6902412B2 *	2003-08-26	2005-06-07	Motorola, Inc	Apparatus for intrinsically safe power interface
US7237719B2 *	2003-09-03	2007-07-03	Stmicroelectronics, Inc.	Method and apparatus for a USB and contactless smart card device
JP4412947B2	2003-09-08	2010-02-10	株式会社ルネサステクノロジ	Memory card
JP2005085089A *	2003-09-10	2005-03-31	Renesas Technology Corp	Ic card and manufacturing method thereof
JP2007041629A *	2003-11-04	2007-02-15	Renesas Technology Corp	Memory card and semiconductor device
US7209995B2 *	2003-12-09	2007-04-24	Sandisk Corporation	Efficient connection between modules of removable electronic circuit cards
KR101083366B1 *	2003-12-11	2011-11-15	삼성전자주식회사	Memory system and method for setting data transfer speed between host and memory card
JP4072503B2 *	2004-02-04	2008-04-09	シャープ株式会社	IC card with built-in coprocessor for auxiliary operation and control method thereof
US7112082B2 *	2004-03-17	2006-09-26	Wieson Technologies Co., Ltd.	Miniature memory card/SIM card dual-function connector
US8267780B2	2004-03-31	2012-09-18	Nintendo Co., Ltd.	Game console and memory card
US7771280B2 *	2004-03-31	2010-08-10	Nintendo Co., Ltd.	Game console connector and emulator for the game console
US7837558B2 *	2004-03-31	2010-11-23	Nintendo Co., Ltd.	Game console and emulator for the game console
US8016681B2	2004-03-31	2011-09-13	Nintendo Co., Ltd.	Memory card for a game console
KR101114987B1 *	2004-04-01	2012-06-11	삼성전자주식회사	Multi-channel memory card and control method thereof
US7710736B2	2005-08-02	2010-05-04	Sandisk Corporation	Memory card with latching mechanism for hinged cover
US8748726B2 *	2004-04-16	2009-02-03	Sandisk Corporation	Memory card with two standard sets of contacts and a hinged contact covering mechanism
US7152801B2	2004-04-16	2006-12-26	Sandisk Corporation	Memory cards having two standard sets of contacts
JP4651332B2	2004-04-26	2011-03-16	ルネサスエレクトロニクス株式会社	Memory card
JP2005322109A *	2004-05-11	2005-11-17	Renesas Technology Corp	Ic card module
JP4591754B2 *	2004-07-30	2010-12-01	ソニー株式会社	COMMUNICATION DEVICE, ELECTRONIC DEVICE, AND COMMUNICATION SYSTEM
KR100579053B1 *	2004-08-26	2006-05-12	삼성전자주식회사	Method of multi-interfacing between smart card and memory card and multi-interface card
CN100465933C *	2004-09-07	2009-03-04	瑞昱科技股份有限公司	Removable electronic device and its method
US7226383B2 *	2004-09-15	2007-06-05	Inventec Appliances Corp.	Apparatus and a method for extending phone book records of a subscriber identification module (SIM) card
TWI282517B *	2004-10-15	2007-06-11	C One Technology Corp Ltd	Multi-functional integrated circuit card module having mixed interface
JP4515218B2 *	2004-10-22	2010-07-28	ソニー株式会社	Memory card
WO2006045344A1 *	2004-10-29	2006-05-04	Telecom Italia S.P.A.	Method for establishing a secure logical connection between an integrated circuit card and a memory card through a terminal equipment
JP4566966B2 *	2004-10-29	2010-10-20	三洋電機株式会社	Memory element
CN100375102C *	2004-11-30	2008-03-12	國际商业机器公司	Non-contact card reader and information processing system
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card

JP2006253430A	2005-03-11	2006-09-21	Renesas Technology Corp	Semiconductor device and its manufacturing method
JP2006268459A	2005-03-24	2006-10-05	Ricoh Co Ltd	Nonvolatile memory card and shape conversion adapter
US7729660B2 *	2005-04-15	2010-06-01	Sony Corporation	Communication device, non-contact type IC card mounting same, and information apparatus
JP4864346B2 *	2005-05-18	2012-02-01	ソニー株式会社	Memory card and card adapter
EP1727080A1 *	2005-05-27	2006-11-29	Axalto S.A.	SIM with double sets of contacts protected against short-circuit
JP2007011708A	2005-06-30	2007-01-18	Ricoh Co Ltd	Integrated-type memory card and shape transformation adaptor
JP2007065956A *	2005-08-31	2007-03-15	Renesas Technology Corp	Memory card
TWM284108U *	2005-09-02	2005-12-21	Tai Sol Electronics Co Ltd	Connector for a card with a function for avoiding a short cut
KR101155220B1 *	2005-09-13	2012-06-13	엘지전자 주식회사	Uim card including external memory in mobile phone
US7529491B2 *	2005-09-15	2009-05-05	Xerox Corporation	Apparatus and method for adapting a machine to communicate with customer replaceable unit monitors having different interface formats
JP4944442B2 *	2005-12-28	2012-05-30	株式会社エヌ・テ ィ・テ ィ・ドコモ	Mobile communication terminal system
EP1804196A1 *	2005-12-29	2007-07-04	Motorola, Inc.	Method and devices for data access in combined SIM and mass storage cards
US7193161B1 *	2006-02-15	2007-03-20	Sandisk Corporation	SiP module with a single sided lid
WO2007094624A1 *	2006-02-17	2007-08-23	Kfreetel Co., Ltd.	Ic card, terminal with ic card and initializing method thereof
JP2007280347A *	2006-03-14	2007-10-25	Ricoh Co Ltd	Memory card and memory card control changeover method
US20090100238A1 *	2006-03-14	2009-04-16	Masaharu Adachi	Memory card and memory card control changeover method
JP2007317170A *	2006-04-28	2007-12-06	Renesas Technology Corp	Ic module and cellular phone
US9198025B2 *	2006-05-04	2015-11-24	Sandisk Il Ltd.	High-capacity SIM storage control
US8060142B2 *	2006-05-24	2011-11-15	Lg Electronics Inc.	Method for reducing power consumption for detachable card and mobile communication terminal thereof
US8843768B2 *	2006-09-05	2014-09-23	Netapp, Inc.	Security-enabled storage controller
WO2008029206A2 *	2006-09-05	2008-03-13	Nokia Corporation	Device interface
TW200816056A *	2006-09-27	2008-04-01	Renesas Tech Corp	IC card and IC card socket
DE102006045906A1 *	2006-09-28	2008-04-17	Infineon Technologies Ag	Module with a controller for a chip card
KR100770220B1	2006-10-16	2007-10-26	삼성전자주식회사	Memory card and method of manufacturing the same
US7827323B2 *	2006-12-08	2010-11-02	Marvell Israel (M.I.S.L.) Ltd.	System and method for peripheral device communications
US7991158B2 *	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
US8079528B2 *	2007-01-10	2011-12-20	Taiwan Semiconductor Manufacturing Co., Ltd.	Input/output pads placement for a smart card chip
JP2008257506A *	2007-04-05	2008-10-23	Renesas Technology Corp	Semiconductor device
US7572152B2 *	2007-06-27	2009-08-11	Sandisk Il Ltd.	Memory interface card with SIM functions
JP2009032214A *	2007-07-24	2009-02-12	Renesas Technology Corp	Semiconductor integrated circuit, display device, and electronic circuit
JP2009054061A *	2007-08-29	2009-03-12	Renesas Technology Corp	Semiconductor device
KR20090025530A *	2007-09-06	2009-03-11	삼성전자주식회사	Subscriber identify module card and terminal connectable of the same
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US7983099B2	2007-12-20	2011-07-19	Mosaid Technologies	Dual function compatible non-volatile memory device

			Incorporated	
CN101578607B *	2008-05-08	2012-05-30	鸿富锦精密工业（深圳）有限公司	Pad and circuit board used thereby
US8473974B2 *	2008-05-13	2013-06-25	Nbcuniversal Media, Llc	Activation system and method for activating an optical article
US8387876B2 *	2008-05-13	2013-03-05	Nbcuniversal Media, Llc	Activation system and method for activating an optical article
JP5202172B2 *	2008-08-06	2013-06-05	富士通コンポーネント株式会社	Memory card connector
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US8782433B2 *	2008-09-10	2014-07-15	Inside Secure	Data security
US9653004B2	2008-10-16	2017-05-16	Cypress Semiconductor Corporation	Systems and methods for downloading code and data into a secure non-volatile memory
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
KR101555637B1 *	2009-03-27	2015-09-24	삼성전자주식회사	Smart card
CN101587557B *	2009-06-29	2015-12-09	北京握奇数据系统有限公司	A kind of Subscriber Identity Module and manufacture method thereof and system
EP2465040A1	2009-08-14	2012-06-20	SanDisk IL Ltd.	Dual interface card with backward and forward compatibility
JP4906135B2 *	2009-10-21	2012-03-28	ルネサスエレクトロニクス株式会社	Memory card
US8275188B2 *	2009-12-03	2012-09-25	Condel International Technologies Inc.	Systems and methods for managing storage devices
CN1047945238 *	2009-12-07	2018-10-12	三星电子株式会社	Storage card and electronic device
US8666386B2 *	2010-05-03	2014-03-04	Apple Inc.	Wireless network authentication apparatus and methods
CN102289710A *	2010-06-18	2011-12-21	黄金富	Secure digital (SD) memory card having function of subscriber identity model (SIM) card
CN102289711A *	2010-06-18	2011-12-21	黄金富	SD (Secure Digital) memory card for mobile phone payment and with function of contactless smart card
JP5396415B2 *	2011-02-23	2014-01-22	株式会社東芝	Semiconductor device
WO2013013189A2	2011-07-20	2013-01-24	Visa International Service Association	Security gateway communication
US9635549B2	2011-09-01	2017-04-25	Nokia Technologies Oy	Providing subscriber identity module function
US8649820B2 *	2011-11-07	2014-02-11	Blackberry Limited	Universal integrated circuit card apparatus and related methods
USD667830S1 *	2011-11-29	2012-09-25	Samsung Electronics Co., Ltd.	SD memory card
EP2645307B1 *	2012-03-29	2020-11-04	Uros Technology S.à r.l	Apparatus having a plurality of SIMs
US8936199B2	2012-04-13	2015-01-20	Blackberry Limited	UICC apparatus and related methods
USD703208S1	2012-04-13	2014-04-22	Blackberry Limited	UICC apparatus
USD701864S1	2012-04-23	2014-04-01	Blackberry Limited	UICC apparatus
WO2013166278A1	2012-05-02	2013-11-07	Visa International Service Association	Small form-factor cryptographic expansion device
US8904078B2 *	2012-10-22	2014-12-02	Lenovo Enterprise Solutions (Singapore) Pte. Ltd.	High speed serial peripheral interface system
USD707682S1 *	2012-12-05	2014-06-24	Logomotion, S.R.O.	Memory card
CN103164737A *	2013-01-29	2013-06-19	三星半导体(中国)研究开发有限公司	High-density memory smart card module and manufacture method thereof

CN104795651B *	2014-01-22	2017-10-13	富士康(昆山)电脑接插件有限公司	Electronic card coupler
EP2908593B1 *	2014-02-12	2018-08-01	Alcatel Lucent	Apparatuses, methods and computer programs for a base station transceiver and a mobile transceiver
KR10216817081	2014-06-30	2020-10-20	삼성전자주식회사	Memory card
USD783622S1 *	2015-08-25	2017-04-11	Samsung Electronics Co., Ltd.	Memory card
USD783621S1 *	2015-08-25	2017-04-11	Samsung Electronics Co., Ltd.	Memory card
DE102016110780A1 *	2016-06-13	2017-12-14	Infineon Technologies Austria Ag	Smart card module and method for manufacturing a smart card module
CN1063041968 *	2016-08-03	2020-06-09	惠州Tcl移动通信有限公司	FDN-based data flow control method and system
US10027079B2 *	2016-10-27	2018-07-17	Amphenol Shouh Min Industry (Shen Zhen) Co., Ltd.	Connector applied to USF card and micro SD card
KR20190083242A	2018-01-03	2019-07-11	삼성전자주식회사	Memory card and electronic system

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
CN1218276C	2005-09-07	IC card
US7201581B2	2007-04-10	IC card
US7296754B2	2007-11-20	IC card module
JP4937736B2	2012-05-23	Memory card with standard security functions
JP2007183776A	2007-07-19	Semiconductor device
JP2004133843A	2004-04-30	Ic module provided with three types of interfaces, 3-way sim and sim holder, and 3-way ic card and ic card holder
WO2005008453A1	2005-01-27	Universal serial bus driving device having a function of smart card reader
KR100745514B1	2007-08-02	Ic card
JP4761479B2	2011-08-31	IC card
CN1932857A	2007-03-21	Integrated circuit card
CN1916944A	2007-02-21	Integratel circuit cards
KR100743084B1	2007-07-27	Ic card
JP2006202336A	2006-08-03	Non-volatile memory device
CN1434379A	2003-08-06	Method for executing operation to intelligent card from computer

Priority And Related Applications

Child Applications (3)

Application	Priority date	Filing date	Relation	Title
CN200610099656A	2000-04-28	2000-04-28	Division	Cellphone
CN200510078595A	2000-04-28	2000-04-28	Division	IC card
CN200610101765A	2000-04-28	2000-04-28	Division	Non-volatile storage device

Priority Applications (1)

Application	Priority date	Filing date	Title

PCT/JP2000/002823	2000-04-28	2000-04-28	ic card

Legal Events

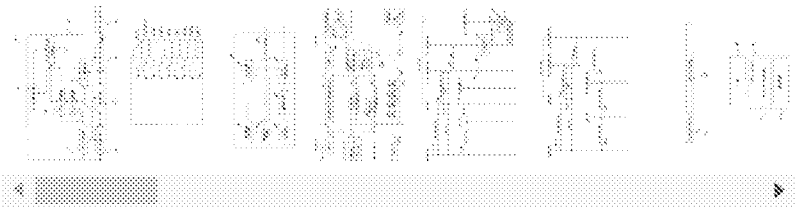
Date	Code	Title	Description
2003-10-29	PB01	Publication	
2003-10-29	C06	Publication	
2004-01-07	C10	Entry into substantive examination	
2004-01-07	SE01	Entry into force of request for substantive examination	
2005-09-07	GR01	Patent grant	
2005-09-07	C14	Grant of patent or utility model	
2017-06-16	CF01	Termination of patent right due to non-payment of annual fee	**Granted publication date**: 20050907 **Termination date**: 20160428

About Send Feedback Public Datasets Terms Privacy Policy

Patents JP4624732

how to access

Images (47)



Classifications

G07F7/1008 Active credit-cards provided with means to personalise their use, e.g. with PIN-introduction/comparison system

View 7 more classifications

JP4624732B2
Japan

Download PDF Find Prior Art Family

Other languages: Japanese

Inventor: 佳彦 高木, 睦文 菊地

Worldwide applications

2004 JP WO TW US TW KR EP KR 2005 IL

Application JP2004197453A events

2003-07-16 Priority to JP2003275672
2004-07-02 Application filed by パナソニック株式会社
2004-07-02 Priority to JP2004197453A
2005-02-24 Publication of JP2005050320A
2011-02-02 Application granted
2011-02-02 Publication of JP4624732B2
Status Active
2024-07-02 Anticipated expiration

Info: Patent citations (70), Cited by (30), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (16) Hide Dependent

1. An access method from a device to a memory device,
The device is
Transmitting designation information for designating an access area to the memory device;
Transmitting the processing instruction to the access area and the verification information on the designation information together;
The memory device is
Receiving the specified information;
Receiving the processing instruction and the verification information, and verifying the designation information using the verification information;
If the verification is successful, executing the processing instruction;
Having an access method.

2. An access method from a device to a memory device,
The device is
Sharing with the memory device possible area information regarding an accessible area to the memory device; and
Referring to the possible area information and transmitting designation information for designating an access area to the memory device;
Transmitting the processing instruction to the access area and the verification information on the designation information together;
The memory device is
Receiving the specified information;
Receiving the processing instruction and the verification information, and verifying the designation information using the verification information;
If the verification is successful, executing the processing instruction;
Having an access method

3. An access method from a device to a memory device,
The device is
Sharing a verification key with the memory device;
Transmitting designation information for designating an access area to the memory device;
Transmitting the processing instruction to the access area together with verification data obtained by encrypting verification information related to the specified information with the verification key;
The memory device is
Receiving the specified information;

Receiving the processing instruction and the verification data, and verifying the designation information using the verification data and the verification key;
If the verification is successful, executing the processing instruction;
Having an access method.

4. An access method from a device to a memory device,
The device is
Sharing with the memory device possible area information regarding an accessible area to the memory device, and
Sharing a verification key corresponding to the accessible area with the memory device;
Referring to the possible area information and transmitting designation information for designating an access area to the memory device;
Transmitting the processing instruction to the access area together with verification data obtained by encrypting verification information related to the specified information with the verification key;
The memory device is
Receiving the specified information;
Receiving the processing instruction and the verification data, and verifying the designation information using the verification data and the verification key;
If the verification is successful, executing the processing instruction;
Having an access method.

5. An access method from a device to a memory device,
The device is
Using the first processing command with the memory device, sharing the possible area information regarding the accessible area to the memory device;
Referring to the possible area information and using a second processing command to transmit designation information for designating an access area to the memory device;
Using the second processing command, a process command to the access area and verification information related to the designation information are transmitted together,
The memory device is
Receiving the specified information;
Receiving the processing instruction and the verification information, and verifying the designation information using the verification information;
If the verification is successful, executing the processing instruction;
Having an access method

6. An access method from a device to a memory device,
The device is
Sharing a verification key with the memory device using a first processing command;
Using a second processing command to send designation information for designating an access area to the memory device;
Using the second processing command, and sending together the processing instruction to the access area and verification data obtained by encrypting the verification information related to the designation information with the verification key;
The memory device is
Receiving the specified information;
Receiving the processing instruction and the verification data, and verifying the designation information using the verification data and the verification key;
If the verification is successful, executing the processing instruction;
Having an access method.

7. A memory device that is read and written from a device,
Processing instruction receiving means for receiving specification information specifying an area to be accessed and receiving verification information based on the specification information together with a read or write command;
A designation information verification means for performing a verification process on the designation information using the verification information;
A storage area for storing data;
A storage area access means for reading from or writing to the designated area of the storage area in response to the processing instruction when the verification process is successful,
Data transmission means for transmitting data read by the storage area access means to the device;
Data receiving means for receiving write data from the device;
A memory device comprising:

8. 8. The memory device according to claim 7, wherein the verification process of the specified information verification unit is performed using the verification information and a verification key.

9. 9. The memory device according to claim 8, further comprising verification key sharing means for sharing the verification key with the device.

10. 8. The memory device according to claim 7, further comprising possible area information sharing means for sharing possible area information indicating an accessible area to the memory device with the device.

11. An information device that reads and writes memory devices,
A designation information determining means for deciding an area to be read or written and determining designation information for designating the area;
Verification information generating means for generating the verification information from the designation information;
A processing command transmission means for transmitting the designation information, and sending the verification information and a processing command for reading or writing together;
If the processing instruction is a write, data transmission means for transmitting data to the memory device,
If the processing instruction is read, data receiving means for receiving data from the memory device;
Data storage means for storing data to be transmitted to the memory device or storing data received from the memory device;
An information device comprising:

12. 12. The information apparatus according to claim 11, wherein the verification information generation process of the verification information generation unit is performed using the designation information and a verification key.

13. 13. The information apparatus according to claim 12, further comprising verification key sharing means for sharing the verification key with the memory device.

14. 12. The information apparatus according to claim 11 , further comprising possible area information sharing means for sharing possible area information indicating an accessible area to the memory device with the memory device.

15. An access method from a device to a memory device,
The device is
Transmitting designation information for designating an access area to the memory device;
Transmitting the processing instruction to the access area and verification data obtained by encrypting verification information related to the specified information with a verification key;
The memory device is
Receiving the specified information;
Receiving the processing instruction and the verification data, and verifying the designation information using the verification data and a verification key;
If the verification is successful, executing the processing instruction;
Having an access method.

16. An access method from a device to a memory device,
The equipment is
Sharing possible area information related to an accessible area to the memory device using a first processing command;
Sharing a verification key corresponding to the accessible area using a first processing command;
Using a second processing command to send designation information for designating an access area to the memory device;
Transmitting a processing command to the access area using a second processing command and verification data obtained by encrypting verification information related to the designation information with the verification key;
The memory device is
Receiving the specified information;
Receiving the processing instruction and the verification data, and verifying the designation information using the verification data and the verification key;
If the verification is successful, executing the processing instruction;
Having an access method.

Description

The present invention relates to a memory card that is used by being inserted into a terminal such as a PC or a mobile phone, and an access method for the memory card.

Conventionally, a memory card is inserted into a terminal, and the terminal stores data.
An example of a conventional memory card will be given below (for example, see Patent Document 1 below).

The card has a command terminal (CMD line) for receiving various commands from the terminal and returning a response to the command, and a data terminal (DAT line) for receiving data input and outputting data.

In the example of the conventional memory card shown in FIG. 46, the terminal 4602 is a CMD line, the terminals 4607, 4608, and 4609 are DAT lines, which are DAT0, DAT1, and DAT2, respectively. A terminal 4601 is a CD / DAT 3 that serves both as data input / output and card detection (CD). As for DAT0 to DAT3, there are a mode in which only DAT0 is used and a mode in which DAT0 to DAT3 are simultaneously used and a transfer rate four times that in the case of using only DAT0 is realized.

Next, the in-card module configuration of the conventional card will be described with reference to FIG.

The in-card module includes processing command receiving means 4701 for receiving commands and sending responses connected to the CMD line 4602, and data transmitting / receiving means 4702 for sending and receiving data connected to the DAT lines 4607, 4608, 4609 and 4601. The storage area 4704 and storage area access means 4703 for reading and writing data to and from the storage area 4704 according to the received command.

Next, the processing operation at the time of data reading in the conventional memory card will be described. Here, the data output is set to a mode that uses only the DAT0 terminal 4607, but a mode in which the DAT1 terminal 4608, the DAT2 terminal 4609, and the DAT3 terminal 4601 are used together may be used.

First, the terminal transmits a data read command to the CMD line 4602 of the card. This read command has the format shown in FIG. 7 and is composed of a 6-bit command code 401 and a 32-bit command argument 402. The command argument in the data read command stores a read start address.

The processing command receiving unit 4701 that has received the command from the terminal refers to the command code 401 and recognizes that it is a data read command.

Next, the processing command receiving means 4701 refers to the command argument 402 to check whether the specified address is correct, that is, whether the specified address is within the range supported by the card. If is not correct, a response code indicating an error is returned as a response. If the address is correct, a response code indicating that the address is normal is returned.

The processing command receiving means 4701 sends a response to the terminal, and then makes a read request to the storage area access means 4703 together with the designated address.

The storage area access unit 4703 reads data from the specified address in the storage area 4704 and transmits it to the data transmission / reception unit 4702.

The data transmission / reception means 4702 outputs read data to the terminal through the DAT0 line 4607.

Such a memory card can be freely read and written by designating an address from a terminal.
JP 2003-91704 A

In the memory card as described above, when it is desired to restrict access using a specific area of the flash memory as a security protection area and access is possible only from a specific terminal to which access is permitted, it is possible to perform flexible authentication using card commands. However, the APDU (Application Protocol Data Unit), which is the standard command format for IC cards, can only send and receive 256 bytes of data, and because of the half-duplex protocol, it receives a response each time a command is sent from the host. Therefore, high-speed data transfer is difficult. Therefore, a method of performing data transfer using a memory card command after performing authentication processing using a method flexibly matched to a security policy using an IC card command can be considered. It is difficult to confirm that the applications on the host that issued the card command are the same.

Therefore, if the information generated during the authentication process using the IC card command is included in the memory card command as verification data for verifying the identity of the IC card command and the issuer of the memory card command, the command argument is accessed. The area designation information (address to be accessed, etc.) and verification data for authentication are included, but the size of the command argument 402 of the data read command is fixed to 32 bits as described above, so authentication is performed to improve security. If the size of the verification data is increased, the length of the access area designation information is shortened and the accessible area is limited. On the other hand, if the size of the verification data is reduced, the security strength is lowered.

If the format of the conventional data read command is changed to solve this problem, there is a possibility that the conventional memory card cannot be accessed.

In addition, if the conventional data read command and the data read command to the memory card having the security protection area coexist separately, it is necessary to switch the command depending on the type of the memory card on the terminal side. Access to the card is complicated, making it difficult for the terminal to use. Therefore, it is necessary to define a command for transmitting verification data and a memory card command for reading or writing data, and to access the security protection area by combining the two commands. The identity of the command issuer cannot be confirmed between.

Therefore, in the present invention, when accessing an area where access is not restricted in the memory card, a memory card command represented by the above-mentioned data read command is used. After the access area designation information is sent to the memory card by the memory card command for designating the access area, it is shared between the host and the memory card using a flexible authentication process using the IC card command or is shared in advance. Sending the memory card command for reading or writing the security protection area including the key information and the verification data for authentication generated using the access area specification information to the memory card, and sending the data to the security protection area Write, data from security protection area An access method that enables access to the security protection area without changing the format of the memory card command and reducing the security even with a small number of command arguments by adopting a two-stage command configuration of reading. The purpose is to provide.

A first invention is an access method from a device to a memory device, wherein the device transmits designation information designating an access area to the memory device, a processing instruction to the access area, and the designation information verification information, and the memory device receives the specified information; receives the processing instruction and the verification information; and verifies the specified information using the verification information And a step of executing the processing instruction when the verification is successful.

According to the present invention, the access area designation and security protection area access commands are separated, and the verification data is included in the security protection area access command so that the access area designation and the security protection area access command are performed. The memory device can verify that the device application that holds the verification key shared between the device application that issued the certificate and the memory card, that is, the device application that has the authority to access the security protection area is the same. It becomes. In addition, with the two-stage configuration of access area designation and security protection area access commands, using memory card commands for conventional memory access avoids the complexity of the command, and security with fewer command arguments It is possible to access the security protection area without degrading the security level.

A second invention is a method for accessing a memory device from a device, wherein the device shares with the memory device, the available area information related to an accessible area to the memory device, and the available area information. The step of transmitting designation information for designating an access area to the memory device, a process command for processing to the access area, and verification information relating to the designation information, and the memory device, Receiving the designation information; receiving the processing instruction and the verification information; verifying the designation information using the verification information; and executing the processing instruction if the verification is successful. And an access method

According to the present invention, it is possible to explicitly set whether or not each area in the security protection area can be accessed by the security protection area access command.

A third invention is a method for accessing a memory device from a device, wherein the device shares a verification key with the memory device, and designation information for designating an access area to the memory device. Transmitting the processing instruction to the access area, and verification data obtained by encrypting the verification information related to the specified information with the verification key; and the memory device is configured to transmit the specified information. Receiving the processing instruction and the verification data, verifying the designation information using the verification data and the verification key, and executing the processing instruction if the verification is successful And an access method.

According to the present invention, the strength of security can be improved by updating the verification key as necessary.

A fourth invention is a method for accessing a memory device from a device, wherein the device shares with the memory device shared area information regarding an accessible area to the memory device, and the memory device And a step of sharing a verification key corresponding to the accessible area, referring to the accessible area information, transmitting designation information for designating an access area to the memory device, and Transmitting a processing command and verification data obtained by encrypting verification information related to the specified information with the verification key; the memory device receiving the specified information; the processing command; Receiving verification data and verifying the specified information using the verification data and the verification key; If successful in verification, an access method and a step of executing the processing instructions.

According to the present invention, when access is not made to an area in which only the device can read and write, access by a security protection area access command can be invalidated, security strength can be improved, and a verification key can be obtained. The security strength can be improved by updating as necessary.

A fifth invention is a method for accessing a memory device from a device, wherein the device uses the first processing command to obtain possible area information relating to an accessible area to the memory device. A step of sharing, a step of referring to the possible area information and using a second processing system command to transmit designation information specifying an access area to the memory device, and the second processing system command Using the processing command to the access area and the verification information related to the designation information in combination, the memory device receiving the designation information, the processing command and the verification information. Receiving the verification information using the verification information, and executing the processing instruction if the verification is successful. Tsu and up, which is an access method having a.

According to the present invention, it becomes possible to separate sharing of information about accessible areas by a command processing system different from the access area designation and security protection area access commands, and the device application that has designated the access area and security protection. The memory device can verify that the device application that has issued the area access command is the same as the device application that has the authority to access the security protection area.

A sixth invention is an access method from a device to a memory device, wherein the device shares a verification key with the memory device using a first processing command, A step of transmitting designation information for designating an access area to the memory device using a processing command; a processing instruction for the access area using the second processing command; and verification of the designation information A step of transmitting verification data obtained by encrypting information with the verification key, a step of receiving the designation information, a step of receiving the processing information and the verification data, and the designation information being received by the memory device. And using the verification data and the verification key, and executing the processing instruction when the verification is successful. It is Seth method.

According to the present invention, verification key sharing processing can be separated by a command processing system different from the command for accessing the security protection area, and the security strength is further improved by updating the verification key limited to that area. can do.

A seventh invention is an access method from a device to a memory device, wherein the memory device has a tamper-resistant first region in which access from the device is restricted, and a non-access in which access from the device is restricted. A tamper-resistant second area, and a third area accessible from the device, and at least a first processing command that is a processing command to the first area; and at least the third A second processing command that is a processing command to the area, and the device can access the memory device by using the first processing command with the memory device. Sharing the possible area information with respect to, and referring to the possible area information, and using a second processing command, sending designation information for designating an access area to the second area And a step of transmitting a processing instruction to the access area and verification information related to the designation information using a second processing command, and the memory device receives the designation information An access method comprising: a step of receiving the processing instruction and the verification information; verifying the designation information using the verification information; and executing the processing instruction when the verification is successful It is.

According to the present invention, the accessibility setting necessary for access to the non-tamper resistant area is performed at the discretion of the tamper resistant area, and data read / write is performed using a command suitable for the non-tamper resistant area. Flexibility and read / write performance.

An eighth invention is an access method from a device to a memory device, the memory device having a tamper-resistant first region in which access from the device is restricted, and a non-access in which access from the device is restricted. A tamper-resistant second area, and a third area accessible from the device, and at least a first processing command that is a processing command to the first area, and at least the third A step of determining a second processing command that is a processing command to the area, and the device shares a verification key with the memory device using the first processing command A step of transmitting designation information for designating an access area to the second area using a second processing command, and a processing instruction for the access area using a second processing command Transmitting verification information encrypted with the verification key together with verification information related to the designation information, the memory device receiving the designation information, the processing instruction and the verification data An access method comprising: receiving and verifying the designation information using the verification data and the verification key; and executing the processing instruction when the verification is successful.

According to the present invention, the accessibility setting and verification key sharing necessary for access to the non-tamper resistant area are performed at the discretion of the tamper resistant area, and data read / write is performed using a command suitable for the non-tamper resistant area. By using it, it is possible to achieve both security flexibility and read / write performance.

A ninth invention is a memory device that is read from and written to a device, and receives processing information that receives specification information specifying an area to be accessed and receives verification information based on the specification information together with a read or write command Means, a specification information verification means for performing verification processing using the verification information, a storage area for storing data, and, if the verification processing is successful, the storage in accordance with the processing instruction A storage area access means for reading or writing to the designated area of the area, a data transmission means for transmitting data read by the storage area access means to the device, a data receiving means for receiving write data from the device, A memory device.

According to the present invention, it is possible to confirm that the two commands are transmitted from the same terminal even when the command for specifying the access area and the command for accessing the memory are different.

A tenth invention is the memory device according to the ninth invention, wherein the verification processing of the specified information verification means is performed using the verification information and a verification key.

According to this invention, by using the key, the terminal can be authenticated using the shared secret information with the terminal.

An eleventh invention is the memory device according to the tenth invention, further comprising verification key sharing means for sharing the verification key with the device.

According to the present invention, the strength of security can be improved by updating the verification key as necessary.

A twelfth invention is a memory device according to the ninth invention, further comprising possible area information sharing means for sharing possible area information indicating an accessible area to the memory device with the device.

According to the present invention, it is possible to explicitly set whether or not each area in the security protection area can be accessed by the security protection area access command.

A thirteenth aspect of the present invention is an information device that reads and writes a memory device, determines an area to be read or written, specifies designation information that designates the area, and specifies the verification information from the designation information. Verification information generation means for performing generation processing; processing instruction transmission means for transmitting the specification information, and the verification information and a processing instruction for reading or writing; and if the processing instruction is a write, the memory Data transmitting means for transmitting data to the device, and when the processing instruction is read, data receiving means for receiving data from the memory device, storing data to be transmitted to the memory device, or from the memory device And a data storage unit that stores received data.

According to the present invention, data stored in the security protection area of the memory card can be read and written.

A fourteenth aspect of the invention is the information device according to the thirteenth aspect of the invention, wherein the verification information generating unit performs the verification information generation process using the designation information and the verification key.

According to this invention, by performing verification using the card and the secretly supplied key, data can be stored in an area where only the information device can read and write.

A fifteenth aspect of the invention is the information equipment according to the fourteenth aspect of the invention, comprising verification key sharing means for sharing the verification key with the memory device.

According to the present invention, the strength of security can be improved by updating the verification key as necessary.

An information device according to a sixteenth aspect is the information device according to the thirteenth aspect, further comprising possible area information sharing means for sharing possible area information indicating an accessible area to the memory device with the memory device. It is.

According to the present invention, when access is not made to an area in which only the information device can read and write, access by a security protection area access command can be invalidated, and security strength can be improved.

A seventeenth aspect of the invention is an access method from a device to a memory device, wherein the device transmits specification information for specifying an access area to the memory device, a processing instruction for the access area, and the specification A verification data obtained by encrypting verification information related to information with a verification key, the memory device receiving the designation information, the processing command and the verification data, An access method comprising: verifying designated information using the verification data and a verification key; and executing the processing instruction when the verification is successful.

According to the present invention, by performing verification using the verification key shared by the device and the memory device, it is possible to permit access only to the device having the right to access.

An eighteenth aspect of the invention is an access method from a device to a memory device, wherein the device uses a first processing command to share possible area information regarding an accessible area to the memory device; The step of sharing the verification key corresponding to the accessible area using one processing system command and the designation information specifying the access area to the memory device are transmitted using the second processing system command A step of transmitting a processing command to the access area using a second processing command, and verification data obtained by encrypting verification information related to the designation information with the verification key, and the memory The device receives the designation information, receives the processing instruction and the verification data, and sends the designation information to the verification data and the previous data And verifying by using the verification key, if successful in the verification is an access method and a step of executing the processing instructions.

According to the present invention, the security strength can be further improved by enabling the access by the security protection area access command to the area in the security protection area and updating the verification key limited to the area. it can.

A nineteenth aspect of the invention is an access method from a device to a memory device, wherein the memory device includes a tamper-resistant first region in which access from the device is restricted, and a non-access in which access from the device is restricted. A first processing system command having at least a tamper-resistant and large-capacity second area and a large-capacity third area that can be accessed from the device and is a processing command to at least the first area; And at least a second processing command that is a processing command to the third area, and the device uses the first processing command with the memory device to store the memory The step of sharing the available area information related to the accessible area to the device and the step of sharing the verification key corresponding to the accessible area using the first processing command. A step of transmitting designation information for designating an access area to the second area using a second processing command, and a processing instruction for the access area using a second processing command And verification data obtained by encrypting verification information related to the designation information with the verification key, the memory device receiving the designation information, the processing instruction, and the verification data And the verification information is verified using the verification data and the verification key, and if the verification is successful, the processing instruction is executed.

According to the present invention, access enablement setting and verification key sharing necessary for access to a non-tamper resistant area are performed at the discretion of the tamper resistant area, and data read / write uses commands suitable for a large capacity area. This makes it possible to achieve both security flexibility and read / write performance.

According to the present invention, the access area designation command and the security protection area access command are separated, and the verification application is included in the security protection area access command so that the access area designation command and the security protection area access command are specified. It is possible for the card to verify that the terminal application that holds the verification key shared between the terminal application that issued the card and the memory card, that is, the terminal application that has the authority to access the security protection area is the same. Become. In addition, with the two-stage configuration of access area designation and security protection area access commands, using memory card commands for conventional memory access avoids the complexity of the command, and security with fewer command arguments It is possible to access the security protection area without degrading the security level.

(Embodiment 1)
The in-card module configuration in the present invention will be described with reference to FIG. Although the terminal arrangement of the card 100 is shown in FIG. 2, the terminal configuration is the same as that shown in FIG. 46, but the reference numerals attached to the terminals are different.

The in-card module includes a controller 106 and a flash memory 105. The controller 106 uses a session key for a command receiving unit 101 connected to the CMD line for receiving commands and sending responses, a data transmitting / receiving unit 102 connected to the DAT line, and data transmitted / received by the data transmitting / receiving unit 102 using a session key. An encryption / decryption unit 107 that performs encryption / decryption processing, performs encryption / decryption with a flash memory storage key, and transfers data to / from the memory access unit 104; a memory access unit 104 that reads / writes data to / from the flash memory 105. In response to the received command, the memory access unit 104, the session key sharing unit 110, the parameter verification unit 108, the data control unit 103 that makes a processing request to the encryption / decryption unit 107, and the security protection area received from the terminal 200 are accessed. Parameter to store parameters Data storage unit 109, parameter verification unit 108 that verifies that the parameters are correct, session key sharing unit 110 that exchanges authentication and encryption / decryption session keys with terminal 200, session key, and session key And an area / session key management unit 111 for storing a security protection area associated with.

Next, the configuration of terminal 200 in Embodiment 1 will be described using FIG.

The terminal 200 encrypts and receives data transmitted from the command transmission unit 204 that transmits a memory card command to the card 100, data transmission / reception means 207 that transmits data to the DAT line of the card 100, and data transmission / reception means 207. The encryption / decryption unit 206 that decrypts data, the session key sharing unit 202 that performs session key sharing processing between the card 100, and the area to be accessed by the security protection area access command, and generates area designation information , A designation information determination unit 201, a verification data generation unit 203 that generates verification data from the area designation information and the session key, and a data storage unit 205 that stores data to be transmitted or received.

Next, an outline of processing performed between the card 100 of FIG. 1 and the terminal 200 of FIG. 3 will be described with reference to FIG.

4, first, between the terminal 200 and the card 100, as a process using the card 100 IC card command, an authentication process for authenticating the terminal 200 and the card 100 and a key sharing process for sharing a session key. Then, an area number assignment process for assigning an area number (area No. x in the figure) of an accessible area from the terminal 200 to the memory in the card 100 is executed (step S401).

After the authentication process is performed and the validity is mutually confirmed, the key sharing process and the area number assignment process are performed. As a result, in the terminal 200 and the card 100, the area No. A verification and encryption session key that enables access to the security protection area indicated by x is held in association with the area number (area No. x).

Next, between the terminal 200 and the card 100, as processing using the memory card command, an access area designation command transmission process (step S402) and a data transfer command transmission process (step S403) from the terminal 200 to the card 100, An encrypted data transmission process (step S404) from the card 100 to the terminal 200 is executed.

In the access area designation command transmission processing, the area No. is designated to designate the area within the security protection area to be accessed. An access area designation command including data in which x, a block address, and a block length are set is transmitted from the terminal 200 to the card 100. In the card 100, the area number extracted from the received access area designation command. Based on x, a process for verifying whether to access the security protection area is executed.

In the data transfer command transmission process, the terminal 200 uses the area No. Verification data is created using x, the block address and the block length, and the verification key shared with the card 100 in step S401, and a data transfer (Read) command including this verification data is transmitted to the card 100. The The card 100 uses the verification key shared with the terminal 200 from the received data transfer (Read) command to store the area No. By confirming that the verification data is created based on x, the block address, and the block length, it is verified whether the access to the security protection area designated in step S402 is possible.

Further, in the encrypted data transmission process, the area No. The data stored in x is encrypted using the encryption key shared with the terminal 200, and this encrypted data is transmitted to the terminal 200.

In the following description, the processing procedure will be described in detail in the above processing outline.

The command form transmitted / received between the terminal 200 and the session key sharing unit 110 is assumed to conform to an APDU format used in a general IC card. That is, session key sharing unit 110 takes the form of an IC card application.

Here, an APDU transmission / reception method will be described with reference to the sequence diagram of FIG.

First, command APDU transmission processing from the terminal 200 to the card 100 will be described. Here, the command APDU means a command to be executed on the memory card side and sent from the terminal 200 in the APDU format. Specifically, an IC card command is used.

First, terminal 200 creates a command APDU to be transmitted to session key sharing unit 110. Next, terminal 200 transmits an APDU transmission command to CMD line 22 of card 100 in FIG. 2 (step S501).

This APDU transmission command has the format shown in FIG. 7 as with the conventional data read command, and is composed of a 6-bit command code 401 and a 32-bit command argument 402.

As shown in FIG. 16, the command argument 402 in the APDU transmission command includes a flag 1401 indicating that the data input to the DAT0 line 27 is a command APDU and 1403 indicating the number of transmission data. When the flag 1401 and the number of transmission data 1403 are less than 32 bits, an unused field 1402 exists.

The data input to the DAT0 line 27 in FIG. 2 is in 512-byte units, and the transmission data number 1403 indicates how many times the input in 512-byte units is performed.

Next, the command receiving unit 101 of the card 100 receives the command transmitted from the terminal 200 (step S502), recognizes that it is an APDU transmission command, and sends a response to the terminal 200 via the CMD line 22. At the same time, it returns (step S503) and notifies the data control unit 103 that the APDU transmission command has been received (step S504).

Next, the terminal 200 receives a response to the APDU transmission command from the CMD line 22 of the card 100 (step S503), and inputs the command APDU 1602 in the format shown in FIG. 18 to the DAT0 line 27 (step S505).

In FIG. 18, the length indicated by 1601 indicates the length of the subsequent APDU 1602. The command argument transmission data number 1403 is set in accordance with the total length of the length field 1601 and the APDU 1602. Since the total length is not necessarily a multiple of 512 bytes, padding 1603 is added so as to be a multiple of 512 bytes.

Next, the data transmitting / receiving unit 102 inside the card 100 receives the command APDU input from the terminal 200 to the DAT0 line 27 (step S505), and notifies the data control unit 103 that the command APDU has been received (step S505). S506). Next, the data control unit 103 reads the command APDU from the data transmission / reception unit 102 (step S507), and passes the command APDU to the session key sharing unit 110 (IC card application) (step S508).

Next, the session key sharing unit 110 performs processing as described in the command APDU (step S509), and passes the data and status information generated as a result of the processing to the data control unit 103 as a response APDU (step S510). This status information is a status word defined by ISO7816, and is a 2-byte value indicating whether the process ended normally or abnormally. Next, response APDU transmission processing from the card 100 to the terminal 200 will be described with reference to the sequence diagram of FIG. Here, the response APDU means that the processing result of the command APDU executed by the card 100 is transmitted from the card 100 to the terminal 200.

Here, it is assumed that the response APDU output from the session key sharing unit 110 is held by the data control unit 103 as shown in the command APDU transmission method.

First, the terminal 200 transmits an APDU reception command to the CMD line 22 of the card 100 (step S601). Similar to the APDU transmission command, this APDU reception command has the same format as the conventional data read command shown in FIG. 7, and includes a 6-bit command code 401 and a 32-bit command argument 402.

The command argument 402 in the APDU reception command includes an unused field 1501 and a transmission data number 1502 as shown in FIG. When the number of transmission data 1502 is less than 32 bits, an unused field 1501 exists.

The data output from the DAT0 terminal 27 in FIG. 2 is in 512-byte units, similar to the input data in the APDU transmission command, and the transmission data number 1502 indicates how many times the data is output in 512-byte units.

Next, the command receiving unit 101 of the card 100 receives the command transmitted from the terminal 200 (step S602), recognizes that it is an APDU reception command, and sends a response to the terminal 200 via the CMD line 22. While returning (step S603), it notifies the data control unit 103 that the APDU reception command has been received (step S604).

Next, the data control unit 103 passes the response APDU received from the session key sharing unit 110 to the data transmission / reception unit 102 (step S605).

Next, the terminal 200 receives a response to the APDU reception command from the CMD line 22 of the card 100 (step S603), and reads the response APDU from the data transmission / reception unit 102 via the DAT0 line 27 (step S606). The read response APDU is output in the format shown in FIG. The details of each field are the same as when input in the APDU transmission command, and thus the description thereof is omitted.

As shown in FIG. 8, the flash memory 105 mounted on the card 100 is a normal area (non-resistant) that can be accessed from at least the terminal 200 with memory card commands represented by conventional read commands and write commands. A tamper-resistant memory area) 62 and a security protection area (tamper-resistant memory area) 61 that cannot be accessed by the conventional command. Further, as shown in FIG. 8, the card 100 has a tamper resistant module (TRM) 80 that can be accessed by an IC card command.

The security protection area 61 is normally accessible only from the card application. Access to the conventional read command and write command from the terminal 200 is excluded by the command receiving unit 101.

The memory card according to the present invention can be loaded with a plurality of card applications. As shown in FIG. 9, the security protection area 61 is a separate area (AP1 area 71 to AP3 for each application). Area 73) can be allocated.

The security protection area 61 is encrypted with a storage encryption key (Ks) managed by the data control unit 103. This encryption key may be one Ks for the entire security protection area 61, or the storage encryption keys Ks_1 to Ks_3 may be individually prepared in the AP1 area 71 to AP3 area 73 for each application. . In this embodiment, storage encryption keys Ks_1 to Ks_3 are prepared for the applications AP1 to AP3

Next, the internal configuration of the AP1 area 71 to AP3 area 73 for each application in the security protection area 61 will be described with reference to FIG.

Here, an area 71 for the card application AP1 is given as an example. The inside of the AP1 area 71 is data management using a hierarchical structure using directories DIR1 and DIR2 and files FILE1 to FILE3.

The card application AP1 moves the directory in the AP1 area 71, and reads / writes the files FILE1 to FILE3 on the directories DIR1 and DIR2 in which the target file exists.

For example, when the card application AP1 accesses the file FILE3, the card application AP1 moves to the directory DIR1, then moves to the directory DIR2, and then reads and writes the file FILE3. Further, in each of the directories DIR1 and DIR2, it is possible to create and delete subordinate directories or files.

Next, a session key sharing procedure performed between the session key sharing unit 110 in the card 100 and the terminal 200 will be described with reference to FIGS.

Each of the card application and the terminal 200 holds a pair of a public key and a secret key used in public key cryptography, and holds the other party's public key.

The command form in the session key sharing procedure uses the APDU shown above. In the following description, description regarding the command form is not performed, but simply described as a command APDU and a response APDU.

First, the terminal 200 selects the card application AP1 by transmitting a SELECT command APDU (step 901). The SELECT command APDU is a command APDU that specifies to which application in the card 100 the subsequent IC card command (command APDU) is to be transmitted, and is transmitted using the APDU transmission command in the same manner as other command APDUs.

If the selection of the card application AP1 designated from the terminal 200 is normally completed, the card 100 returns a normal completion response APDU, and if not complete, the card 100 returns an abnormal termination response APDU (step 902).

Next, the terminal 200 executes a process 903. Briefly describing the processing 903, the processing 903 is processing for generating DATA2 that enables access to the selected card application AP1. Details of this processing 903 will be described with reference to the flowchart of FIG.

The terminal 200 generates a random number Rh (step S9031), combines the random number Rh with the file name of the file FILE3 shown in FIG. 10 that the terminal 200 wants to access, and corresponds to the secret key PriS held by the card application AP1. DATA1 is generated by encryption with the public key PubS (step S9032), and the identifier info_PubH indicating the public key PubH corresponding to the private key PriH held by the terminal 200 and DATA1 are combined to generate DATA2 (step S9033).

Returning to FIG. 11, next, the terminal 200 uses the REQ_AREA_INFO command including DATA2 generated in step S9033 in order to share a session key with the card application and share area information accessible by the terminal 200. Transmit to the application (step 904).

The card application AP1 that has received the REQ_AREA_INFO command executes processing 905. Details of the processing 905 will be described with reference to the flowchart of FIG.

The card application AP1 extracts DATA1 from DATA2, decrypts it with the private key PriS held by the card application AP1, and obtains a random number Rh and a file name FILE3 (step S9051).

Next, the public key is identified from DATA2, the identifier info_PubH is extracted, and it is confirmed by referring to the access authority setting of the file FILE3 whether access by the terminal 200 associated with the public key PubH indicated by info_PubH is permitted. To do. If there is no authority, an error to that effect is returned to the terminal 200 as a response APDU. If there is an authority to access, the file size SIZE3 of FILE3 is acquired (step S9052).

Next, a random number Rs is generated (step S9053), and is registered in the access valid table 4500 shown in FIG. 45 so that the file FILE3 can be accessed from the terminal 200 using the security protection area access command. Assigns an area number X for use when accessing using the security protection area access command to the file FILE3 and stores it in the area / session key management unit 111 together with the file size SIZE3 (step S9054). The area number is information included in access area designation information transmitted by the access area designation command when the terminal 200 performs access by the security protection area access command.

Next, the random number Rs, the area number X, and the file size SIZE3 are combined to generate DATA3 (step S9055), and DATA3 is encrypted with the public key PubH of the terminal 200 to generate DATA4 (step S9056)

Next, an exclusive OR is performed on the random number Rs and the random number Rh to generate a random number R (step S9057), and an encryption session key Kd and a verification session key Km are generated from the random number R (step S9058).

Next, the session keys Kd and Km are associated with the area number X and stored in the area / session key management unit 111 (step S9059).

Returning to FIG. 11, when the processing up to here is completed, the card 100 transmits a response APDU including DATA4 to the terminal 200 to the terminal 200 (step 906).

The terminal 200 that has received the response APDU extracts DATA4 from the response APDU, and executes the process 907. Details of the processing 907 will be described with reference to the flowchart of FIG.

The terminal 200 decrypts DATA4 using the private key PriH of the terminal 200 and acquires DATA3 (step S9071). Next, the terminal 200 acquires a random number Rs from DATA3, performs an exclusive OR operation on the random number Rs and the random number Rh, and generates a random number R (step S9072). From the random number R, the encryption session key Kd, the verification session A key Km is generated (step S9073).

By performing the above steps 901 to 907, mutual authentication is performed between the terminal 200 and the card 100, and if the terminal 200 has access authority for the file designated, the terminal 200 can be accessed and accessed. It is possible to share the necessary area number, the file size SIZE3 assigned to the area number, the verification session key Km, and the encryption session key Kd.

Note that the file name transmitted from the terminal 200 to the card 100 in step 904 need not directly indicate the file managed by the card application, but may be in any form that can recognize which file the card application points to. .

In addition, in step S9054, the area number assigned when the terminal 200 is set to be accessible in the step S9054 is always the same as the file that the terminal 200 wants to access. By recognizing in advance between the cards 100, the notification of the file name that the terminal 200 wants to access in step 904 and the notification of the area number assigned to the file in step 906 can be omitted.

Furthermore, in this description, each card application has a hierarchical structure consisting of directories and files as shown in FIG. 10, and data is managed by directory names and file names. However, each card application is assigned to a card application. An area may be divided into appropriate sizes, and an identifier such as a number assigned to each divided area may be managed. In that case, the identifier is used instead of the file name FILE3 used in the processing procedure shown in FIG.

Next, processing when the terminal 200 accesses the security protection area will be described with reference to FIGS. 15 and 1. The solid line in FIG. 15 represents transfer on the CMD line 22, and the dotted line represents transfer on the DAT0 line 27.

First, the terminal 200 transmits an access area designation command which is a memory card command to the card 100 (step 1301). This access area designation command has the format shown in FIG. 7, and is composed of a 6-bit command code 401 and a 32-bit command argument 402.

As shown in FIG. 16, the command argument 402 in the access area designation command includes a flag 1401 indicating that the data input to the DAT0 line 27 is access area designation information and 1403 indicating the number of transmission data. When the flag 1401 and the number of transmission data 1403 are less than 32 bits, an unused field 1402 exists.

The data input to the DAT0 line 27 is in 512-byte units, and the transmission data number 1403 indicates how many times the input in 512-byte units is performed.

Next, the command receiving unit 101 of the card 100 receives the command transmitted from the terminal 200, recognizes that it is an access area designation command, returns a response to the terminal, and sends the response to the data control unit 103. It is notified that the access area designation command has been received (step 1302).

Next, the terminal 200 receives a response to the access area designation command from the CMD line 22 of the card 100, and inputs the access area designation information 1702 in the format shown in FIG. 19 to the DAT0 line 27 (step 1303).

The length indicated by 1701 in FIG. 19 indicates the length of the access area designation information 1702 that follows. The number of transmission data 1403 of the command argument 402 is set in accordance with the total length of the length field 1701 and the access area designation information 1702. Since the total length is not necessarily a multiple of 512 bytes, padding 1703 is added so as to be a multiple of 512 bytes.

As shown in FIG. 20, the access area designation information 1702 is an area number 1801 for designating the area number X notified from the card in step 906 in FIG. 11, and 0 or more, and the file size also notified from the card. An access start address 1802 that can be selected in the range of SIZE3 and an access data size 1803 that is 1 or more and can be selected in the range of (file size SIZE3-access start address 1802).

Next, the data transmitting / receiving unit 102 inside the card receives the access area designation information 1702 input from the terminal, and notifies the data control unit 103 that the access area designation information 1702 has been received

Next, the data control unit 103 reads the access area designation information 1702 from the data transmission / reception unit 102, and determines whether the area number 1801 is the area number X assigned in step S9054 of FIG. 13 or the access start address and access data. It is checked whether the size is within the file size range of the file corresponding to the area number X, and if there is an abnormality, an error flag held in the card is set to ON.

If there is no abnormality, the data control unit 103 stores the access area designation information 1702 (specifically, the area number 1801, the access start address 1802, and the access data size 1803) in the parameter storage unit 109 shown in FIG.

The above is the process for designating the access area.

Next, processing when reading is performed on the security protection area 61 of FIG. 8 will be described.

In FIG. 15, the terminal 200 transmits a security protection area read command to the card 100 (step 1304). This security protection area read command has the format shown in FIG. 6 and is composed of a 6-bit command code 401 and a 32-bit command argument 402.

The command argument 402 in the security protection area read command indicates whether the terminal that transmitted the security protection area read command is the same as the terminal 200 that transmitted the access area designation command, or the area indicated by the area number X through the session key sharing procedure it is composed of verification data for verifying whether or not it is the same as the terminal 200 that has been confirmed to have the access authority to.

This verification data generation method will be described with reference to FIG.

The access area designation information 1702 is a parameter input to the DAT0 line 27 in the access area designation command. The verification key 2101 is the verification session key Km generated in step 907 in FIG.

The verification data generation unit 203 inside the terminal 200 is a module that performs cryptographic operations, and generates verification data to be included in a security protection area access (read or write) command. Here, a MAC (Message Authentication Code) generation process called DES-MAC is performed. MAC generation processing using DES encryption is performed using the verification key 2101 using 2102 obtained by adding padding data 2105 to the access area designation information 1702 as input data, and MAC data is created as verification data 2104.

The padding data 2105 may be transmitted together with the access area designation information 1702 when the access area designation command is transmitted from the terminal 200 to the card 100, or the padding generation determined in advance between the terminal and the card. You may give the padding data produced | generated based on the rule.

in the present embodiment, verification data is created using DES-MAC, but other algorithms may be used. Furthermore, the verification algorithm may be selectable according to the application.

If it is not necessary to authenticate whether the terminal 200 is valid and only the association with the access area designation command is to be confirmed, the SHA1 (Secure Hash Algorithm 1) or MD5 (Message Digest 5) is simply used without using encryption processing.) Hash data using an algorithm may be used as verification data.

The terminal 200 generates 32-bit verification data by the above-described verification data generation process and uses it as an argument of the security protection area read command.

Next, the command receiving unit 101 of the card 100 receives the command transmitted from the terminal 200, recognizes that it is a security protection area read command, and the error flag related to the access area designation information 1702 is set to ON. If so, an error is returned as a response. If the error flag related to the access area designation information 1702 is not set to ON, a normal response is returned to the terminal as shown in FIG. 15 (step 1305) and the security protection area is read to the data control unit 103. It notifies that the command has been received, and passes the verification data 2104 given as the command argument 402 to the parameter verification unit 108.

Next, the terminal 200 receives a response to the security protection area read command from the CMD line 22 of the card 100 and waits for data to be output from the DAT 0 line 27.

Hereinafter, data output processing of the security protection area by the card 100 will be described.

The parameter verification unit 108 of the card 100 reads the access area designation information 1702 given from the terminal 200 by the access area designation command from the parameter storage unit 109 and stores the access area designation information 1702, and the area number X (1801), the verification session key Km stored in step S9059 of FIG. 13 is acquired from the area / session key management unit 111.

Next, the parameter verification unit 108 of the card 100 performs the verification data generation process shown in FIG. 22 using the verification session key Km and the access area designation information 1702 to generate verification data 1904. The verification data generation process is the same as the verification data generation process by the terminal 200 shown in FIG.

Next, the parameter verification unit 108 of the card 100 compares the verification data 1904 generated in the verification data generation process with the verification data 2104 given by the argument of the security protection area read command from the terminal 200, and if they do not match. An error occurs, and the data reading process is not performed. If they match, the data control unit 103 is notified that the process proceeds to the next data reading process.

Next, the data control unit 103 of the card 100 reads the access area designation information 1702 from the parameter storage unit 109, acquires the area number X included therein, and corresponds to the area number from the area / session key management unit 111. Recognize file FILE3.

Next, the data control unit 103 of the card 100 confirms that the file FILE3 is an area for the application AP1, and acquires the storage encryption key Ks_1.

Next, the data control unit 103 of the card 100 acquires the access start address 1802 and the access data size 1803 from the access area designation information 1702, and offsets the access start address 1802 with respect to the area managed as the file FILE3. A data read request is made to the memory access unit 104 with the access data size 1803 as the read size.

Next, the data control unit 103 of the card 100 requests the encryption / decryption unit 107 to decrypt the data read by the memory access unit 104 with the storage encryption key Ks_1.

Next, the data control unit 103 of the card 100 requests the encryption / decryption unit 107 to encrypt the data decrypted by the encryption / decryption unit 107 with the encryption session key Kd.

Next, the data control unit 103 of the card 100 requests the data transmission / reception unit 102 to transmit to the terminal 200 the data encrypted by the encryption / decryption unit 107 with the encryption session key Kd.

Through the above processing, data in the security protection area can be output from the card 100 in a state encrypted with the session key Kd.

The terminal 200 recognizes that data can be output from the card 100, and acquires data in a state encrypted with the session key Kd from the DAT0 line 27 as shown in FIG. 15 (step 1306). The data is decrypted with the encryption session key Kd held by, and the data in the area designated by the access area designation information 1702 is obtained

Next, processing when writing to the security protection area will be described with reference to FIG.

Regarding the transmission of the access area designation command from the terminal 200 (step 2001), the response from the card 100 to the command (step 2002), and the transmission of the access area designation information (step 2003), the security protection shown in FIG. Since this is the same as steps 1301 to 1303 in the reading process for the region, the description is omitted. After performing steps 2001 to 2003, the terminal 200 transmits a security protection area write command to the card 100 (step 2004). This security protection area write command has the format shown in FIG. 6 and includes a 6-bit command code 401 and a 32-bit command argument 402.

The command argument 402 in the security protection area read command indicates that the terminal 200 that has transmitted the security protection area read command is the same as the terminal 200 that has transmitted the access area designation command, and the area number X is set through the session key sharing procedure. It consists of verification data 2104 for verifying whether or not it is the same as the terminal 200 that has been confirmed to have access authority to the indicated area.

Since the verification data generation method is the same as that for the security protection area read command, a detailed description thereof will be omitted.

The terminal 200 generates 32-bit verification data by the verification data generation process, and uses it as an argument of the security protection area write command.

Next, the command receiving unit 101 of the card 100 receives the command transmitted from the terminal 200, recognizes that it is a security protection area write command, and an error flag related to the access area designation information 1702 is set. In this case, an error is returned as a response.

When the error flag related to the access area designation information 1702 is not set, a normal response is returned from the CMD line 22 to the terminal 200 (step 2005).

At the same time, it notifies the data control unit 103 that the security protection area write command has been received, and passes the verification data 1904 given as a command argument to the parameter verification unit 108.

Next, the terminal 200 receives a response to the security protection area write command from the CMD line 22 of the card 100 and inputs data to the DAT 0 line 27. Here, the data input to the DAT0 line 27 is encrypted with the encryption session key Kd generated in step 907 of FIG. The input data size is the same as the access data size specified by the access area specifying information 1702.

Hereinafter, data storage processing in the security protection area by the card will be described.

The parameter verification unit 108 of the card 100 reads the access area designation information 1702 given from the terminal 200 by the access area designation command from the parameter storage unit 109 and stores the access area designation information 1702, and the area number X (1801), the verification session key Km stored in step 9059 of FIG. 13 is acquired from the area / session key management unit 111.

Next, the verification data generation unit 1903 inside the parameter verification unit 108 of the card 100 uses the verification session key Km and the access area designation information 1702 to perform the verification data generation process shown in FIG. Generate. Since the verification data generation process is the same as the verification data generation process by the terminal shown in FIG. 21, detailed description thereof is omitted.

Next, the parameter verification unit 108 of the card 100 compares the verification data 1904 generated above with the verification data 2104 given by the argument of the security protection area write command from the terminal 200. Does not transition to write processing. If they match, the data control unit 103 is notified that the process proceeds to the next data writing process.

Next, the data control unit 103 of the card 100 reads the access area designation information 1702 from the parameter storage unit 109, acquires the area number X included therein, and corresponds to the area number from the area / session key management unit 111. Recognize file FILE3.

Next, the data transmission / reception unit 102 of the card 100 receives data input from the terminal 200.

Next, since the file FILE3 exists in the application AP1 area 71, the data control unit 103 of the card 100 acquires the storage encryption key Ks_1 corresponding to the application AP1 area 71.

Next, the data control unit 103 of the card 100 requests the encryption / decryption unit 107 to decrypt the data received by the data transmitting / receiving unit 102 with the encryption session key Kd.

Next, the data control unit 103 of the card 100 requests the encryption / decryption unit 107 to encrypt the data decrypted by the encryption / decryption unit 107 with the storage encryption key Ks_1.

Next, the data control unit 103 of the card 100 acquires the access start address 1802 and the access data size 1803 from the access area designation information 1702, and offsets and accesses the access start address 1802 for the area managed as the file FILE3. A data write request is made to the memory access unit 104 with the data size 1803 as the write size.

As described above, the data encrypted with the session key Kd input by the terminal 200 is encrypted with the storage key Ks_1 and stored in the flash memory 105

In this embodiment, sharing of session keys and sharing of information regarding accessible areas are performed simultaneously with one command, but they may be performed as separate commands.

In this embodiment, the session key sharing procedure is included in FIG. 11, but when it is considered that the session key does not need to be updated every time as a security policy, the terminal 200 and the card 100 preliminarily receive the verification key and the encryption key. May be used and used as a session key.

As described above, in a memory card that can receive an IC card command and a memory access command as in the present invention, the card application uses it and is usually accessible only via the card application, and access from the terminal is limited. When the card application and the terminal mutually authenticate to the security protection area and the card application makes an accessible setting, the terminal can be accessed using a memory access command.

In addition, mutual authentication between the card application and the terminal for the card application to make the accessible setting is based on the data security level by using the IC card command instead of the memory access command for limited use. The mutual authentication method can be selected flexibly.

Even if the argument size included in the memory access command is as small as 32 bits, as in the present invention, the access area designation and security protection area access commands are separated and verified as the security protection area access commands. By including data, the card can verify that the terminal application that specified the access area, the terminal application that issued the security protected area access command, and the terminal application that holds the verification key are the same. .

In addition, by performing the verification and encryption session key sharing process for each access to the security protection area, a suitable value is set as the verification data to be included in the security protection area access to protect against attacks that repeatedly perform unauthorized access. Can be increased.

Further, by notifying the card of a file to be accessed from the terminal, assigning an area number to the card, and notifying the terminal from the card, it is possible to set an area accessible by the terminal. In addition, by performing processing on a plurality of files, it is possible to create a state in which a plurality of files can be accessed simultaneously.

(Embodiment 2)
In the present embodiment, a sequence will be described in which the terminal recognizes in advance the area number designated by the area designation command.

First, the in-card module configuration will be described with reference to FIG. Note that the terminal configuration of the card 500 of FIG. 24 is the same as that shown in FIG.

The module in the card 500 is connected to the CMD line, and receives a processing command receiving unit 501 that receives a command and transmits a response, a storage area 506 that stores data, and a storage area access unit that performs access processing to the storage area 506 505, a data transmission unit 502 connected to the DAT line and transmitting data read by the storage area access unit 505 to an external device, a data reception unit 503 also connected to the DAT line and receiving data from the external device, And a designated information verification unit 504 that verifies the designation information received by the processing command reception unit 501.

Next, the module configuration in the terminal 600 will be described with reference to FIG.

The module in the terminal 600 includes a processing command transmission unit 604 that performs command transmission and response reception to the card 500, a data transmission unit 605 that performs data transmission to the card 500, and a data reception unit 606 that performs data reception from the card 500. Designation information determining means 601 for determining an area to be accessed; verification information generating means 602 for generating verification information from the specified information; data storage means 603 for storing data to be transmitted to the card 500 and data received from the card 500; It consists of

Next, processing when the terminal 600 accesses the security protection area of the card 500 will be described with reference to FIGS. 24 and 25 and the flowchart shown in FIG.

First, the terminal 600 determines an area for read access or write access by the designation information determination means 601 (step S2601), and generates access area designation information (step S2602). Next, this access area designation information is stored in the data storage means 603, and an area designation command is transmitted from the processing command transmission means 604 to the card 500 (step S2603).

An example of the data portion of the area designation command is shown in FIG.

The data input to the DAT0 line 27 is in 512-byte units, and the data portion of the area designation command is such that the total length of the length field 2701 of the access area designation information 2702 and the access area designation information field 2702 is less than 512 bytes. If not, padding 2703 is added. In the portable device of this embodiment, the length field 2701 has a length of 2 bytes, and the access area designation information 2702 has a 1-byte area number 2801, a 3-byte access start address 2802, and 3 as shown in FIG. It consists of a byte access data size 2803. That is, since it is 9 bytes in total and less than 512 bytes, 503 bytes of padding 2703 is added.

Next, returning to FIG. 26, when the card 500 receives the area designation command at the processing command receiving means 501 (step S2604), the designation information verification means 504 confirms the access area designation information 2702, and the designated area is identified. Whether it is correct is determined based on whether there is an area corresponding to the area number 2801 or whether the access start address 2802 and the access data size 2803 are within the area indicated by the area number 2801 (step S2605). If the designated area is not correct, the designation information verification unit 504 treats the area designation command as invalid (step S2606). If the designated area is correct, the access area designation information 2702 is stored, and comparison information is generated using the access area designation information 2702 and the key shared between the terminal 600 and the card 500 (step S2607).

An example of a method for generating comparison information is shown in FIG.

The verification data generation unit 2902 is a module that performs cryptographic operations, and in this embodiment, performs a process of generating a MAC (Message Authentication Code) called DES-MAC. The input is a data portion 2704 of the area designation command and a verification key 2901 shared between the terminal 600. Although the output result of DES-MAC is 64 bits, in this embodiment, since the verification information transmitted from the terminal 600 to be compared is 32 bits, only the first half 32 bits, which are 2903 truncated from the output, is used as comparison information 2904. The verification key 2901 may be an individual and fixed key corresponding to the area number, or may be a single key regardless of the area number.

Further, as shown in FIG. 30, a verification key sharing means 701 is provided inside the card 700, and a verification key sharing means 801 is provided inside the terminal 800 as shown in FIG. 31, and between the card 700 and the terminal 800, The verification key may be changed each time the security protection area is accessed. 30 and 31, the same parts as those shown in FIGS. 24 and 25 are denoted by the same reference numerals.

Next, a verification key sharing method will be described with reference to FIGS. 30 and 31, the sequence shown in FIG. 32, and the verification key generation method shown in FIG.

In FIG. 32, the terminal 800 generates a random number Ra in the verification key sharing means 801, creates a session key sharing request command APDU including the random number Ra, and sends an APDU transmission command from the processing command transmission means 604 to the card 700. In addition to the transmission (step S3201), the data transmission means 605 transmits a session key sharing request command APDU to the card 700 (step S3202).

Next, the card 700 receives the APDU transmission command from the terminal 800 by the processing command receiving unit 501, and passes the session key sharing request command APDU received from the terminal 800 by the data receiving unit 503 to the verification key sharing unit 701

The verification key sharing unit 801 generates a random number Rb and, as shown in FIG. 33, a master that is shared with the terminal 800 in advance for a combination of the random number Ra and the random number Rb received from the terminal 800. An encryption process (DES-MAC process) is performed using the key K, and a session key R is generated. Next, the card 700 generates a response APDU including the random number Rb.

Next, the terminal 800 transmits an APDU reception command from the processing command transmission unit 604 to the card 700 (step S3203).

Next, the card 700 receives an APDU reception command from the terminal 800 by the processing command receiving unit 501 and transmits a response APDU including the previously generated random number Rb from the data transmitting unit 502 to the terminal 800 (step S3204).

Next, the terminal 800 receives the response APDU from the card 700 by the data receiving unit 606 and passes it to the verification key sharing unit 801. As shown in FIG. 33, the verification key sharing means 801 is a master that is shared in advance with the card 700 for the combination of the random number Ra generated by itself and the random number Rb included in the response APDU. An encryption process (DES-MAC process) is performed using the key K, and a session key R is generated.

The above is the verification key sharing procedure between the terminal 800 and the card 700 when the session key is changed each time the security protection area is accessed.

In the present embodiment, DES-MAC is used, but other encryption algorithms may be used. Further, when it is not necessary to verify whether the terminal 800 is valid, that is, whether it has the same key, for example, only verification that the access area designation information 2702 of the area designation command is what the terminal intended. When performing, the verification data generation unit 3401 as shown in FIG. 34 uses the result of the SHA-1 calculation, the hash calculation using the MD5 algorithm, or the checksum calculation as comparison information without using cryptographic processing. it can. Even when these algorithms are used, if the comparison target is 32 bits long, the output result is truncated 3402, and only a part of the 32 bits is used as comparison information 3403.

Next, returning to FIG. 26, the terminal 800 generates verification information from the access area designation information 2702 and the verification key 2901 shared between the terminal 800 and the card 700 by the verification data generation unit (step S2608).).

The generation of the verification information is shown in FIG. The verification information generation unit 3502 performs a cryptographic process using the verification key 3501 and the data portion 2704 of the area designation command to generate verification information 3504. The generation method is exactly the same as the generation method of the comparison information 2904 in the card 700 shown in FIG.

Next, returning to FIG. 26, the terminal 800 places the generated verification information 3504 in the argument of the access command (read), and transmits the access command from the processing command transmission unit 604 (step S2609).

The access instruction has a format shown in FIG. 36, and the lengths of the command code 3601 and the command argument 3602 are 6 bits and 32 bits, respectively. In the access instruction, verification information 3504 is stored in the command argument 3602.

Next, returning to FIG. 26, the card 700 receives the access command (reading) by the processing command receiving unit 501 (step S2610), and whether the area designation command has been normally completed in advance by the designation information verification unit 504. Whether or not is confirmed (step S2611). If the area designation command has not been received or has not been completed normally because the designated area is incorrect, the access command is notified to the terminal 800 as an error (step S2612). At this time, the terminal 800 receives an error from the card 700 (step S2612A).

If the area designation command has been normally completed in advance, the designation information verification unit 504 compares the comparison information 2904 created by the card 700 with the verification information 3504 stored in the command argument of the access command (step S2613).). If the verification information 3504 is invalid as a result of the comparison, the access command is notified to the terminal 800 as an error (step S2614). At this time, the terminal 800 receives an error from the card 700 (step S2614A). If the verification information is normal, the designation information verification unit 504 notifies the storage area access unit 505 of the access area designation information 2702, and the storage area access unit 505 is designated by the access area designation information 2702 in the storage area 506. The data is read from the area and the data is transmitted from the data transmission means 502 to the terminal 800 (step S2615).

Next, the terminal 800 receives the read data transmitted from the card 700 by the data receiving unit 606 (step S2616) and stores it in the data storage unit 603.

As described above, even when the argument size included in the memory access command is as small as 32 bits, the access area designation command and the security protection area access command are separated as in the present invention, and the security protection area access command is separated. By including verification data in the card, the card can verify that the terminal application that specified the access area, the terminal application that issued the security protected area access command, and the terminal application that holds the verification key are the same. It becomes.

A method of using the random number information output from the card in addition to the area designation information and the verification key for generating verification data will be described below with reference to the flowchart shown in FIG. In addition, in each step shown in FIG. 37, the same step as the step of the flowchart shown in FIG.

As shown in FIG. 37, a random number acquisition command is transmitted from the terminal 800 to the card 700 (step S 3701), the card 700 generates a random number T, and this random number T is sent to the designated information verification means 504 inside the card 700. The data is held and transmitted from the data transmission means 502 to the terminal 800 (step S3702). The terminal 800 receives the random number T transmitted from the card 700 by the data receiving unit 606 (step S3703).

The comparison information generation process (step S2607) in the card 700 and the verification information generation process (step S2608) in the terminal 800 when the random number T is used for the verification information generation process are shown in FIGS. 38 and 39, respectively. In addition, encryption processing is performed on the combination of the random number T and the data portion 2704 of the area designation command, and comparison information 3804 and verification information 3904 are output.

As described above, by using the random number information for generating the verification information, even if the verification information is created using the same region designation information and the verification key, the verification information output by changing the random number information Since it changes, the security strength can be further improved.

(Embodiment 3)
In the present embodiment, an example of a sequence including key sharing processing will be described.

First, the in-card module configuration will be described with reference to FIG. Since the terminal configuration of the card is the same as that shown in FIG. 2, its illustration and description are omitted.

The in-card module is connected to the CMD line, and receives a processing command receiving unit 901 that receives a command and transmits a response, a storage area 906 that stores data, and a storage area access unit 905 that performs access processing to the storage area 906. A data transmission unit 902 that is connected to the DAT line and transmits data read by the storage area access unit 905 to the external device, a data reception unit 903 that is also connected to the DAT line and receives data from the external device, and a terminal 1000, using the verification key, verifies the specification information received via the data receiving means 903 and the possible area information sharing unit 907 that shares information related to the area that can be accessed by the security protection area access command Designated information verification means 904.

Next, the in-terminal module configuration will be described with reference to FIG.

The in-terminal module includes a processing command transmission unit 1004 that transmits a command to the card 900 and a response reception, a data transmission unit 1005 that transmits data to the card 900, a data reception unit 1006 that receives data from the card 900, Specification information determining means 1001 for determining an area to be accessed, possible area information sharing unit 1007 for sharing information related to an area accessible by the security protection area access command, and verification information generating means 1002 for generating verification information from the specified information And data storage means 1003 for storing data transmitted to the card 900 and data received from the card 900.

Next, processing when the terminal 1000 accesses the security protection area in the card 900 will be described with reference to the flowcharts shown in FIGS. 40 and 41 and FIGS.

First, the terminal 1000 determines the area A in which read access or write access is performed by the designated information determining unit 1001 (step S4201), and the possible area information sharing unit 1007 uses a security protection area access command for the area A. An area release request command, which is a command APDU requesting permission for access, is transmitted from the processing command transmission unit 1004 to the card 900 (step S4202). The area release request command includes an identifier Info_PubH representing the public key of the terminal 1000, and data obtained by encrypting the identifier a representing the area A with the public key PubS of the card 900. Note that the command APDU transmission method is the same as the method described in the first embodiment, and a detailed description thereof will be omitted.

Next, when the card 900 receives the area release request command (step S4203), the possible area information sharing unit 907 decrypts the encrypted data included in the command with the private key PriS of the card 900 itself (step S4204). . Next, whether or not the terminal 1000 is permitted to access the area A by identifying the terminal 1000 that has transmitted the command from the public key identifier Info_PubH of the terminal 1000 and referring to the access authority of the area A indicated by the identifier a. Is confirmed (step S4205)

If access is not permitted, data indicating failure to release the area is transmitted as a response APDU from the data transmission unit 902 to the terminal 1000 (step S4206). When access is permitted, the access valid table 4400 (in the specified information verification means 904, which has the identifier a of the area A and the area

number X assigned to the area A, and sets whether access is permitted by the security protection area access command) (See FIG. 44) (step S4207). Next, the verification key R corresponding to the area A is registered in the access validity table 4400 (step S4208).

Next, the area number X and the size of the area A are encrypted with the public key PubH of the terminal 1000 and transmitted as a response APDU from the data transmission unit 902 to the terminal 1000 (step S4209).

Next, the terminal 1000 transmits an APDU reception command from the processing command transmission unit 1004 to the card 900, and acquires a response APDU from the card 900 using the data reception unit 1006 (step S4210). Since the response APDU acquisition method is the same as the method described in the first embodiment, detailed description thereof is omitted.

Next, the possible area information sharing unit 1007 of the terminal 1000 decrypts the encrypted data included in the response APDU with the private key PriH of the terminal 1000 itself (step S4211), and the area A indicated by the area number X and the area number X Get size. Next, the terminal 1000 registers a session key corresponding to the area A in the verification information generation unit 1002. The area number X is registered in the designation information determination unit 1001 to generate access area designation information (step S4212). Thereafter, the process proceeds to the flowchart of FIG.

Next, the terminal 1000 generates access area designation information using the area number X registered by the possible area information sharing means 1007 in the designation information determining means 1001 (step S4213). Next, this access area designation information is stored in the data part 2704 (see FIG. 27), and an area designation command is transmitted from the processing command transmission means 1004 to the card 900 (step S4214). Since the access area designation information in the area designation command is the same as that in the second embodiment, detailed description thereof is omitted.

Next, when the processing instruction receiving unit 901 receives an area designation command from the terminal 1000 (step S4215), the card 900 confirms the access area designation information by the designation information verification unit 904, and the area number X is the access validity table. Whether it is registered in 4400 or within the range of the area A based on the access start address 2802 and the access data size 2803 shown in FIG. 28 is determined (step S4216). If the designated area is not correct, the designation information verification unit 904 treats the area designation command as invalid (step S4217). If the designated area is correct, the access area designation information is saved, and comparison information is generated using the access area designation information and the verification key R corresponding to the area A registered in the access validity table 4400 (step S4218). . Since the method for generating comparison information is the same as that in the second embodiment, detailed description thereof is omitted.

Next, the terminal 1000 generates verification information using the access area designation information and the session key R registered by the possible area information sharing unit 1007 in the verification information generation unit 1002 (step S4219), and an access command (read)) And an access command is transmitted from the processing command transmitting means 1001 to the card 900 (step S4220). Since the verification information generation method and the access command transmission method are the same as those in the second embodiment, detailed description thereof is omitted.

Next, the card 900 receives an access command (reading) by the processing command receiving unit 901 (step S4221), and checks whether or not the area designation command has been normally completed by the designation information verification unit 904 in advance (Step S4222). If the area designation command has not been received or has not been completed normally because the designated area is incorrect, the access command is notified to the terminal 1000 as an error (step S4223). At this time, the terminal 1000 receives an error from the card 900 (step S4223A).

When the area designation command is normally completed in advance, the designation information verification unit 904 compares the comparison information created by the card 900 with the verification information stored in the argument of the access command (step S4224). If the verification information is invalid as a result of the comparison, the access command is notified to the terminal 1000 as an error (step S4225) At this time, the terminal 1000 receives an error from the card 900 (step S4225A).

If the verification information is normal, the designation information verification unit 904 notifies the storage area access unit 905 of the designation information, and the storage area access unit 905 receives data from the area designated by the area designation command in the storage area 906 And data is transmitted from the data transmission means 902 to the terminal 1000 (step S4226).

Next, the terminal 1000 receives the read data transmitted from the card 900 by the data receiving unit 1006 and stores it in the data storage unit 1003 (step S4227).

Next, the terminal 1000 creates an area invalid command APDU for invalidating the area number X corresponding to the area A when access by the security protection area access command to the area A becomes unnecessary, and the data transmission unit 1005 To the card 900 (step S4228).

Next, the card 900 that has received the area invalid command APDU searches the access valid table 4400, and if the area number X is found, the area number X together with the area identifier a and the session key R assigned to the area number X in the table. And the access by the security protection area access command to the area A in which the area number X is designated is invalidated (step S4229).

As described above, a certain area in the security protection area can be accessed by the security protection area access command only when necessary by an area release request, and when it becomes unnecessary, the area can be accessed by an area invalidation request. The security strength can be improved by making the access impossible.

The access method according to the present invention uses a memory card command and an IC card command together, and by using the memory card command for memory access, it is possible to authenticate the terminal safely with a small number of command arguments while avoiding complexity. That is.

The figure which shows the internal module structure of the memory card in Embodiment 1 of this invention. Diagram showing card terminal configuration The figure which shows the internal structure of the terminal in this Embodiment 1. The figure which shows the outline | summary of the process performed between the card | curd and terminal in this Embodiment 1. FIG. The figure which shows the sequence of the transmission / reception method of APDU in this Embodiment 1. FIG. The figure which shows the sequence of the transmission process of the response APDU in this Embodiment 1. The figure which shows the command format of the memory card in this Embodiment 1. The figure which shows the internal structure of the flash memory in this Embodiment 1. The figure which shows the internal structure of the security protection area | region in this Embodiment 1. The figure which shows the internal structure of each application | use area | region in the security protection area | region in this Embodiment 1. The figure which shows the session key sharing and accessible area sharing procedure in this Embodiment 1. Flowchart for explaining details of processing in step 903 of FIG. Flowchart for explaining details of processing in step 905 of FIG. Flowchart for explaining details of processing in step 907 of FIG. The figure which shows the command sequence for reading a security protection area from the terminal in this Embodiment 1. The figure which shows the argument format of the APDU transmission command in this Embodiment 1. The figure which shows the argument format of the APDU reception command in this Embodiment 1. The figure which shows the format of the input data of the APDU transmission command in this Embodiment 1, and the output data of an APDU reception command The figure which shows the input data format of the access area designation | designated command in this Embodiment 1. The figure which shows the access area designation | designated information in this Embodiment 1. The figure which shows the production | generation method by the terminal of the verification data for performing the validity verification of the terminal in this Embodiment 1 The figure which shows the production | generation method by the card | curd of the verification data for performing the validity verification of the terminal in this Embodiment 1 The figure which shows the command sequence for writing in a security protection area

from the terminal in this Embodiment 1. The figure which shows the internal module structure of the memory card in Embodiment 2 of this invention. The figure which shows the internal structure of the terminal in this Embodiment 2. The flowchart which shows the process at the time of accessing the security protection area | region of a card | curd from the terminal in this Embodiment 2. The figure which shows an example of the data part of the area | region designation | designated instruction in this Embodiment 2. The figure which shows the format of the access area designation | designated information of FIG. The figure which shows an example of the production | generation method of the comparison information in this Embodiment 2. The figure which shows a card | curd structure in the case of providing the key sharing means for a verification in the inside in this Embodiment 2. The figure which shows a terminal structure when the key sharing means for a verification is provided in the inside in this Embodiment 2. FIG. The figure which shows the sequence of the sharing method of the verification key in this Embodiment 2. The figure for demonstrating the key generation method for verification in this Embodiment 2. The figure which shows the comparison information production | generation method using SHA-1 calculation in this Embodiment 2. The figure which shows the verification information generation method in this Embodiment 2. The figure which shows the format of the access command in this Embodiment 2. The flowchart which shows the verification data generation process using the random number information in this Embodiment 2. The figure which shows the comparison information generation method using the random number in this Embodiment 2. The figure which shows the verification information generation method using the random number in this Embodiment 2. The figure which shows the internal module structure of the memory card in Embodiment 3 of this invention. The figure which shows the internal structure of the terminal in this Embodiment 3. The flowchart which shows a part of access processing from the terminal in this Embodiment 3 to the security protection area in a card | curd 42 is a flowchart showing a part of the access processing following FIG. The figure which shows an example of the access effective table in this Embodiment 3. The figure which shows an example of the access effective table in this Embodiment 1. The figure which shows the terminal composition of the conventional memory card A diagram showing a conventional module configuration in a card

Explanation of symbols

100, 500, 700, 900 card 200, 600, 800, 1000 terminal 101 command receiving unit 102 data transmitting / receiving unit 103 data control unit 104 memory access unit 105 flash memory 106 controller 107 encryption / decryption unit 108 parameter verification unit 109 parameter storage unit 110 Session key sharing unit 111 Area / session key management unit 201, 601, 1001 Designated information determination unit 202 Session key sharing unit 203 Verification data generation unit 204 Command transmission unit 205, 603, 1003 Data storage unit Data storage unit 206 Encryption / decryption unit 207 Data transmission / reception means 501, 901 Processing instruction reception means 502, 605, 902, 1005 Data transmission means 503, 606, 903, 1006 Data reception means 504, 04 Designated information verification means 505, 905 Storage area access means 506, 906 Storage area 602, 1002 Verification information generation means 604, 1004 Processing command transmission means 801 Verification key sharing means 907, 1007 Possible area information sharing means 4400, 4500 Access valid table

Patent Citations (70)

Publication number	Priority date	Publication date	Assignee	Title
JPH01147686A *	1987-12-02	1989-06-09	Toshiba Corp	Portable electronic device
US5623637A *	1993-12-06	1997-04-22	Telequip Corporation	Encrypted data storage card including smartcard integrated circuit for storing an access password and encryption keys
JPH09259045A *	1996-03-25	1997-10-03	Mitsubishi Electric Corp	Security system device for memory card and the memory card
JPH11306088A *	1998-04-27	1999-11-05	Toppan Printing Co Ltd	ic card and ic card system
JP2001014441A *	1999-04-27	2001-01-19	Matsushita Electric Ind Co Ltd	Semiconductor memory card and reader
Family To Family Citations				
US4621321A *	1984-02-16	1986-11-04	Honeywell Inc.	Secure data processing system architecture
US4713753A *	1985-02-21	1987-12-15	Honeywell Inc.	Secure data processing system architecture with format control
US4816653A *	1986-05-16	1989-03-28	American Telephone And Telegraph Company	Security file system for a portable data carrier
US4816654A *	1986-05-16	1989-03-28	American Telephone And Telegraph Company	Improved security system for a portable data carrier
DE69127560T2 *	1990-01-30	1998-04-23	Toshiba Kawasaki Kk	Mutual recognition system
US5293576A *	1991-11-21	1994-03-08	Motorola, Inc.	Command authentication process
US5533125A *	1993-04-06	1996-07-02	International Business Machines Corporation	Removable computer security device
JP3568970B2	1993-04-12	2004-09-22	株式会社東芝	IC card issuing device
JPH0778126A	1993-09-08	1995-03-20	Kyodo Printing Co Ltd	Microcomputer for ic card
JP3176209B2 *	1994-02-25	2001-06-11	富士通株式会社	Card-type storage medium and card-type storage medium issuing device
DE19508723A1 *	1995-03-10	1996-09-12	Siemens Ag	Multi-user data processing system with memory protection

US6226749B1 *	1995-07-31	2001-05-01	Hewlett-Packard Company	Method and apparatus for operating resources under control of a security module or other secure processor
FR2743910B1 *	1996-01-19	1998-02-27	Solaic Sa	METHOD FOR IMPLEMENTING A SECURE PROGRAM IN A MICROPROCESSOR CARD AND MICROPROCESSOR CARD COMPRISING A SECURE PROGRAM
JPH10105408A *	1996-09-30	1998-04-24	Toshiba Corp	Information processor
US6526145B2 *	1997-01-29	2003-02-25	David M. Marzahn	Data encryptor/decryptor using variable in-place I/O
JP4268690B2 *	1997-03-26	2009-05-27	ソニー株式会社	Authentication system and method, and authentication method
US5974499A *	1997-04-23	1999-10-26	Micron Technology, Inc.	Memory system having read modify write function and method
JPH11175402A *	1997-12-10	1999-07-02	Fujitsu Ltd	Card type storage medium and access control method for the same and computer readable recording medium for recording access control program for card type storage medium
JPH11203266A *	1998-01-07	1999-07-30	Mitsubishi Electric Corp	Microcomputer
JP3611964B2 *	1998-04-16	2005-01-19	富士通株式会社	Storage device, storage control method, and storage medium
JP2000003424A *	1998-04-17	2000-01-07	Hitachi Ltd	Ic card provided with memory content shift control part, and data storing method for ic card
US20010011337A1	1998-09-15	2001-08-02	Massoud Shamshirian	Programmable multiple sequential sector locking for semicondutor memories
JP3545627B2 *	1999-02-08	2004-07-21	株式会社東芝	Portable electronic devices
JP4204133B2 *	1999-02-26	2009-01-07	ローム株式会社	Communications system
CA2338634C *	1999-05-28	2007-06-26	Matsushita Electric Industrial Co., Ltd.	A semiconductor memory card, playback apparatus, recording apparatus, playback method, recording method, and computer-readable recording medium
WO2000078082A1 *	1999-06-14	2000-12-21	Ntt Docomo, Inc.	Wireless communication unit connected detachably with external unit
JP4079550B2 *	1999-06-24	2008-04-23	富士通株式会社	Non-volatile memory that prevents unauthorized reading
JP3749640B2	1999-10-15	2006-03-01	株式会社東芝	IC card using device, IC card and storage medium
JP4413406B2 *	2000-10-03	2010-02-10	株式会社東芝	Nonvolatile semiconductor memory and test method thereof
JP2002132583A *	2000-10-20	2002-05-10	Sony Corp	Data processing apparatus, data storage device and data processing method, and program providing medium
US6807602B1 *	2000-10-30	2004-10-19	Hewlett-Packard Development Company, L.P.	System and method for mapping bus addresses to memory locations utilizing access keys and checksums
JP2002229861A *	2001-02-07	2002-08-16	Hitachi Ltd	Recording device with copyright protecting function
JP2002278838A *	2001-03-15	2002-09-27	Sony Corp	Memory access control system, device managing device, partition managing device, memory packaged device, memory access control method and program storage medium
US6526491B2 *	2001-03-22	2003-02-25	Sony Corporation Entertainment Inc.	Memory protection system and method for computer architecture for broadband networks
US7093104B2 *	2001-03-22	2006-08-15	Sony Computer Entertainment Inc.	Processing modules for computer architecture for broadband networks
AUPR471401A0 *	2001-05-02	2001-05-24	Keycorp Limited	Method of manufacturing smart cards
US7185145B2 *	2001-06-04	2007-02-27	Renesas Technology Corp.	Memory card
US7073059B2 *	2001-06-08	2006-07-04	Hewlett-Packard Development Company, L.P.	Secure machine platform that interfaces to operating systems and customized control programs
JP3900863B2 *	2001-06-28	2007-04-04	シャープ株式会社	Data transfer control device, semiconductor memory device and information equipment
JP3865629B2	2001-07-09	2007-01-10	株式会社ルネサステクノロジ	Storage device
JP2003051819A *	2001-08-08	2003-02-21	Toshiba Corp	Microprocessor
GB2385951A *	2001-09-21	2003-09-03	Sun Microsystems Inc	Data encryption and decryption
JP4226816B2 *	2001-09-28	2009-02-18		Microprocessor

			株式会社東芝	
US6745307B2 *	2001-10-31	2004-06-01	Hewlett-Packard Development Company, L.P.	Method and system for privilege-level-access to memory within a computer
FR2834361B1 *	2001-12-28	2004-02-27	Bull Sa	DATA SECURITY MODULE BY ENCRYPTION / DECRYPTION AND / OR SIGNATURE / VERIFICATION OF SIGNATURE
US7313705B2 *	2002-01-22	2007-12-25	Texas Instrument Incorporated	implementation of a secure computing environment by using a secure bootloader, shadow memory, and protected memory
DE60305752T2 *	2002-01-24	2007-01-25	Matsushita Electric Industrial Co., Ltd., Kadoma	memory card
JP3861878B2 *	2002-03-29	2006-12-27	ソニー株式会社	Data recording / reproducing method and data recording / reproducing apparatus
US20030225962A1 *	2002-05-31	2003-12-04	Hitachi, Ltd.	Memory card and memory card system
EP1505765A4 *	2002-06-07	2006-10-04	Sony Corp	Data processing system, data processing device, data processing method, and computer program
JP4118092B2 *	2002-06-19	2008-07-16	株式会社ルネサステクノロジ	Storage device and information processing device
JP2004030102A *	2002-06-25	2004-01-29	Sony Corp	Information storage device, system and method for memory access control, and computer program
JP4115789B2 *	2002-07-01	2008-07-09	株式会社東芝	Method and program for using shared library in tamper resistant processor
AU2002346316A1 *	2002-07-09	2004-01-23	Fujitsu Limited	Open type general-purpose attack-resistant cpu, and application system thereof
JP2004104539A *	2002-09-11	2004-04-02	Renesas Technology Corp	Memory card
US7567880B2 *	2002-12-02	2009-08-11	Silverbrook Research Pty Ltd	Temperature based filter for an on-chip system clock
JP4322021B2 *	2003-02-06	2009-08-26	株式会社ルネサステクノロジ	Memory card
JP2005056305A *	2003-08-07	2005-03-03	Matsushita Electric Ind Co Ltd	information storage device with split area in memory area
US7139894B1 *	2003-09-12	2006-11-21	Microsoft Corporation	System and methods for sharing configuration information with multiple processes via shared memory
WO2005048111A1 *	2003-11-13	2005-05-26	Matsushita Electric Industrial Co., Ltd.	Semiconductor memory card
JP4282472B2 *	2003-12-26	2009-06-24	株式会社東芝	Microprocessor
US7607177B2 *	2004-02-23	2009-10-20	Micron Technology, Inc.	Secure compact flash
US7162602B2 *	2004-03-16	2007-01-09	Hitachi, Ltd.	More granular and more efficient write protection for disk volumes
JP2007219802A *	2006-02-16	2007-08-30	Hitachi Global Storage Technologies Netherlands Bv	Storage, its controller, and its control method
JP2008123482A *	2006-10-18	2008-05-29	Matsushita Electric Ind Co Ltd	Storage medium control method

* Cited by examiner, † Cited by third party

Cited By (30)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
DE60305752T2 *	2002-01-24	2007-01-25	Matsushita Electric Industrial Co., Ltd., Kadoma	memory card
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
JP4591163B2 *	2005-04-07	2010-12-01	パナソニック株式会社	Bus access control device
GB0517615D0 *	2005-08-30	2005-10-05	Ecebs Ltd	Improved smartcard system

JP4827919B2 *	2006-04-28	2011-11-30	パナソニック株式会社	Communication terminal device and access method
JP2007304847A	2006-05-11	2007-11-22	Megachips Lsi Solutions Inc	Memory device
JP2009537042A *	2006-05-12	2009-10-22	サムスン エレクトロニクス カンパニー リミテッド	Apparatus and method for managing security data
FI118841B *	2006-09-13	2008-03-31	Eads Secure Networks Oy	Mobile device authentication
JP2008123482A *	2006-10-18	2008-05-29	Matsushita Electric Ind Co Ltd	Storage medium control method
US20110271044A1 *	2007-03-30	2011-11-03	Tyfone, Inc.	Memory card having one or more secure elements accessed with hidden commands
US9176897B2 *	2007-09-04	2015-11-03	Nintendo Co., Ltd.	Writing area security system
US20090097657A1 *	2007-10-05	2009-04-16	Scheidt Edward M	Constructive Channel Key
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US8812858B2 *	2008-02-29	2014-08-19	Red Hat, Inc.	Broadcast stenography of data communications
US8401192B2 *	2008-02-29	2013-03-19	Red Hat, Inc.	Mechanism for securely ordered message exchange
JP2009276916A	2008-05-13	2009-11-26	Sony Corp	Communication device, communication method, reader/writer, and communication system
US20100033310A1 *	2008-08-08	2010-02-11	Narendra Siva G	Power negotation for small rfid card
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
JP5293113B2 *	2008-11-25	2013-09-18	大日本印刷株式会社	SEMICONDUCTOR DEVICE, SEMICONDUCTOR DEVICE CONTROL METHOD, AND SEMICONDUCTOR DEVICE CONTROL PROGRAM
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
JP5824849B2 *	2011-04-22	2015-12-02	ソニー株式会社	Information processing apparatus and information processing method
US8386691B1 *	2011-08-19	2013-02-26	Key Asic Inc.	Multimedia storage card system
US9171259B2 *	2011-09-14	2015-10-27	Mastercard International Incorporated	In-market personalization of payment devices
JP5832963B2 *	2012-06-29	2015-12-16	株式会社東芝	Memory system
JP5779148B2 *	2012-07-06	2015-09-16	株式会社東芝	Memory system
JP5779147B2 *	2012-07-06	2015-09-16	株式会社東芝	Memory system
JP5908869B2 *	2013-07-02	2016-04-26	ソニー株式会社	Communication device
US9665421B2 *	2015-01-21	2017-05-30	Oracle International Corporation	Communication protocol bridge for card computing devices
KR102267735B1 *	2020-11-18	2021-06-22	주식회사 체이사인	Decentralized identity verification system using zero-knowledge proof and method thereof

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
JP4624732B2	2011-02-02	how to access
US9954826B2	2018-04-24	Scalable and secure key management for cryptographic data processing
US7415729B2	2008-08-19	Storage device
US8789195B2	2014-07-22	Method and system for access control and data protection in digital memories, related digital memory and computer program product therefor
JP4763368B2	2011-08-31	COMMUNICATION CARD, CONFIDENTIAL INFORMATION PROCESSING SYSTEM, CONFIDENTIAL INFORMATION TRANSFER METHOD, AND PROGRAM
US7469837B2	2008-12-30	Storage device

US7313828B2	2007-12-25	Method and apparatus for protecting software against unauthorized use
CN1269071C	2006-08-09	Storage card
US9100187B2	2015-08-04	Authenticator
JP5604929B2	2014-10-15	Memory device and memory system
KR20020065855A	2002-08-14	Storage device including a non-volatile memory
US20080288747A1	2008-11-20	Encryption-based security protection method for processor and apparatus thereof
US20140351583A1	2014-11-27	Method of implementing a right over a content
WO2013002833A2	2013-01-03	Binding of cryptographic content using unique device characteristics with server heuristics
WO2006031030A1	2006-03-23	Method and apparatus for searching for rights objects stored in portable storage device using object identifier
US9449193B2	2016-09-20	Information processing apparatus
JP3963938B2	2007-08-22	Access method, memory device, and information device
US20080205654A1	2008-08-28	Method and Security System for the Secure and Unequivocal Encoding of a Security Module
KR20180031584A	2018-03-28	Memory system and binding method between the same and host
CN107967432B	2020-10-16	Safe storage device, system and method
CN100583060C	2010-01-20	Access method, device and information machine
JP6340916B2	2018-06-13	Data output method, data read method, storage medium device, and data read device
JP2007122379A	2007-05-17	Authentication apparatus and application issuing method
JP2006066960A	2006-03-09	Storage device, storing method and program

Priority And Related Applications

Child Applications (1)

Application	Priority date	Filing date	Relation	Title
JP2006341650A	2003-07-16	2006-12-19	Division	Access method, memory device, and information device

Priority Applications (2)

Application	Priority date	Filing date	Title
JP2003275672		2003-07-16	
JP2004197453A	2003-07-16	2004-07-02	how to access

Applications Claiming Priority (9)

Application	Filing date	Title
JP2004197453A	2004-07-02	how to access
TW096126811A	2004-07-15	
KR1020057004944A	2004-07-15	Access method
US10/527,820	2004-07-15	Memory, information apparatus for access to the memory, and method for the information apparatus
KR1020067026371A	2004-07-15	Access method
PCT/JP2004/010432	2004-07-15	Access method
TW093121132A	2004-07-15	
EP04747821.9A	2004-07-15	Access method
IL167269A	2005-03-07	Access method

Legal Events

Date	Code	Title	Description
2007-04-20	A621	Written request for application examination	**Free format text:** JAPANESE INTERMEDIATE CODE: A621 **Effective date:** 20070419
2010-04-21	A131	Notification of reasons for refusal	**Free format text:** JAPANESE INTERMEDIATE CODE: A131 **Effective date:** 20100420
2010-06-15	A521	Written amendment	**Free format text:** JAPANESE INTERMEDIATE CODE: A523 **Effective date:** 20100614
2010-10-04	TRDD	Decision of grant or rejection written	
2010-10-13	A01	Written decision to grant a patent or to grant a registration (utility model)	**Free format text:** JAPANESE INTERMEDIATE CODE: A01 **Effective date:** 20101012
2010-10-14	A01	Written decision to grant a patent or to grant a registration (utility model)	**Free format text:** JAPANESE INTERMEDIATE CODE: A01
2010-11-11	A61	First payment of annual fees (during grant procedure)	**Free format text:** JAPANESE INTERMEDIATE CODE: A61 **Effective date:** 20101104
2010-11-12	R150	Certificate of patent or registration of utility model	**Ref document number:** 4624732 **Country of ref document:** JP **Free format text:** JAPANESE INTERMEDIATE CODE: R150 **Free format text:** JAPANESE INTERMEDIATE CODE: R150
2010-11-15	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20131112 **Year of fee payment:** 3

Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

Patents FR2788646

Contactless memory chip/integrated antenna connection construction having micromodule isolated support cavity placed and two central contact planes connecting support lanes and antenna ends.

Abstract

The open loop antenna chip card attachment has an open loop antenna and a cavity (1) holding a micromodule connected to the antenna (31,32), and having an electrically isolated holder (2). The two contact planes (22,23) are in a central region with wires connected across the two support planes and connected to the two ends of the antenna.

FR2788646A1

France

Download PDF Find Prior Art Similar

Other languages: French

Inventor: Roland Carpier, Loc H Alain Le, Christine Lauvernier

Current Assignee : Bull CP8 SA

Worldwide applications

1999 FR 2000 EP BE US DN WO JP 2001 HK

Application FR9900486A events

1999-01-19 Application filed by Bull CP8 SA

1999-01-19 Priority to FR9900486A

2000-07-21 Publication of FR2788646A1

2007-02-09 Application granted

2007-02-09 Publication of FR2788646B1

2014-11-12 First worldwide family litigation filed

2019-01-19 Anticipated expiration

Status Expired - Fee Related

Info: Patent citations (8), Cited by (77), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Classifications

G06K19/07769 Constructional details, e.g. mounting of circuits in the carrier the record carrier being capable of non-contact communication, e.g. constructional details of the antenna of a non-contact smart card comprising at least a second communication arrangement in addition to a first non-contact communication arrangement the further communication means being a galvanic interface, e.g. hybrid or mixed smart cards having a contact and a non-contact interface

View 13 more classifications

Claims (11)

Hide Dependent

1. Chip card comprising a body based on layers of plastic material, said chip card carrying on one of its layers an open loop antenna, said body being provided with a cavity intended to receive a micromodule comprising a specific interface intended to be connected to said open loop antenna by two input and / or output terminals, said micromodule comprising a semiconductor component fixed in a central region of a support, on a first face, characterized in that, said open loop antenna (6a) comprising at least one turn (61 to 63), said support (2) of semiconductor component (3) is provided with at least first (22) and second (23) contact pads , each comprising first ends, situated in a central zone of said support in a region close to said input and / or output terminals (31, 32), in that the first of said areas (22) extends up to a peripheral zone of said support (2) which is opposite it, passing over said semiconductor component (3), and the second of said pads (23) extends from said region to a peripheral zone of said support (2), close to this region, so that second ends of these pads (22, 23) are located in opposite peripheral zones, in that said contact pads (22, 23) are each connected to an input terminal and / or output (31, 32) by their first end, and in that the ends (600a, 610a) of said loop antenna (6a) open out under the second ends of said contact pads (22, 23) and there are

electrically connected.

2. Chip card according to claim 1, characterized in that said input and / or output terminals (31, 32) are connected to said first ends of said first and second contact pads via first openings (220 ', 230 ') made in said support (2) and in that said ends (600a, 610a) of said loop antenna (6a) are connected to these contact pads (23, 24) by second openings (220, 230) made in said support (2), orifices (5110, 5111) being produced in a layer of material

underlying insulation.

3. Chip card according to claim 2, characterized in that said layer of insulating material

is a pre-drilled layer.

4. Chip card according to claims 1,

characterized in that, said antenna (6a) comprising at

at least two turns (61a-63a), two successive turns (61a-

63a) of this antenna (6a) are connected by a conductive interconnection segment (64, 65) passing between said

ends (600a, 610a) of the loop antenna (6a).

5. Chip card according to claim 4, characterized in that, said cavity (51) comprising a central cup (510) intended to receive said semiconductor component (3) and a shallow peripheral groove (511), on which rests the periphery of said component support (2) (3), said interconnecting conductive segments (64, 65) connecting two consecutive turns (61a-63a) are produced on one of said level layers (513) intermediate between the bottom of said peripheral groove (511) and the bottom of said central bowl (510), and pass between said ends (600a, 610a) of the loop antenna (6a) and the

edge of said central bowl (510).

6. Chip card according to claim 5, characterized in that said open loop antenna (6a) comprises three turns (61a-63a), in that said first (22) and second (23) contact pads are placed, symmetrically, on either side of said component support (2) (3), and in that a first of said interconnecting conductive segments (64), connecting a first turn (61a) to a second turn (62a) , is arranged on the edge of said central cup (510) on a first side of said semiconductor component (3), and a second conductive segment (65) is arranged on the edge of said central cup (510), on the side opposite of said

semiconductor component (3).

7. Chip card according to claim 4, characterized in that, said cavity (51) comprising a central cup (510) intended to receive said semiconductor component (3), and a shallower peripheral groove (511), on which rests the periphery of said component support (2) (3), said interconnecting conductive segments (64b, 65b) connecting two consecutive turns (61b-63b), pass under said semiconductor component (3) between said ends

(600a, 610a) of the loop antenna (6a).

8. Smart card according to claim 4, characterized in that said open loop antenna (6c) consists of at least two open turns (66, 67), in that said component support (2c) comprises at least a third contact pad (24, 25, 26) produced on the face of this support (2c) carrying said contact pads and passing between said first (22) and second (23) contact pads, in that the ends (661, 670) of said two turns (66, 67) open out under the third contact pad (24,25,26), and are connected to the latter, the third contact pad (24,25,26) constituting one of said interconnecting conductive segments of two consecutive turns

(66, 67).

9. Smart card according to claim 1, characterized in that it is of the so-called mixed type and in that said support (2) comprises contact pads (21) connected to input-output terminals of said semi component -conductor (3) intended to make possible exchanges by galvanic contacts with a card reader.

10. Smart card according to claim 1, characterized in that said specific interface is a high frequency interface, for carrying out exchanges

electromagnetically at a frequency of 13.56 MHz.

11 Micromodule for smart card, comprising a semiconductor component fixed in a central region and

on a first face of a support, the semi-component

conductor comprising a specific interface intended to be connected to an antenna of the card by two input and / or output terminals, characterized in that said support (2) of semiconductor component (3) is provided with at least first (22) and second (23) contact pads, each comprising first ends, located in a central zone of said support in a region close to said input and / or output terminals (31, 32), in that the first of said pads (22) extends to a peripheral zone of said support (2) which is opposite it, passing over said semiconductor component (3), and the second of said pads (23) s' extends from said region to a peripheral area of said support (2), close to this region, so that second ends of these areas (22, 23) are located in opposite peripheral areas, in that said areas contact (22, 23) are each connected to a input and / or output terminal (31, 32) by their first end, ends (600a, 610a) of said antenna (6a) being intended to open out under the second ends of said contact pads (22, 23) and to be there

electrically connected.

Description

TITLE: CHIP CARD WITH A LOOP ANTENNA, AND

ASSOCIATED MICROMODULE

The present invention relates to a smart card provided with an open loop antenna, in particular a smart card of the type known as "with mixed connections", which will be defined below. In the context of the invention, the term "card" must be understood in its most general sense: memory card ("CAM"), "chip" card, etc. Regarding the mode of communication with the outside world, there are two main categories of

smart cards: smart cards with and without contacts.

In the second case, various methods can be used. An optical coupling or an electromagnetic coupling can be used, in particular, using a spiral loop antenna. In the context of the invention,

we will be interested in this second type of coupling.

The majority of smart cards are of the first type, that is to say with contacts. These smart cards are manufactured from "micromodules", that is to say assemblies comprising a printed circuit or a metal grid having contacts against which are glued and wired components of the integrated circuit type: memories, micro- processors, microcontrollers, etc. These components are then protected by a coating resin so as to make the micromodules usable for the final insertion operation. The latter consists of sticking the micromodules in a plastic support comprising a

cavity intended to receive this micromodule.

Cards of the second type, called "contactless", are coupled with the external environment by electromagnetic induction. The frequencies used fall into two ranges: a low frequency range, the nominal frequency being typically 125 kHz, and a high frequency range, the nominal frequency being typically 13.56 MHz. To do this, an antenna is provided which is usually in the form of a spiral loop, connected at its ends to the aforementioned micromodule. To obtain sufficient sensitivity, it is necessary to provide an antenna comprising a hundred turns, if working at low frequency, and 2 to 3

turns if you work at high frequency.

The current technologies used for the manufacture of smart cards make it possible to integrate the above-mentioned antennas into the material of the smart card,

more precisely between two layers of plastic material.

The turns are in fact placed on layers of plastic material of the "PVC" or "PET" type. The metal layers can be printed on the plastic (for example by screen printing) or produced by depositing a metal wire, directly produced by thermal welding on

the plastic layer.

Finally, there are so-called "mixed" smart cards, which constitute the preferred field of application of the invention. This type of smart card has the advantage of allowing access, both via "conventional" contacts, which makes it possible to use them in standard readers, or by passing close to suitable transceiver members, the micromodules comprising a high frequency interface. The term

"reader" should be understood in a general sense, that is,

say a device for reading and / or writing

digital information in a smart card.

In what follows, we will place ourselves in this preferred application, that is to say in the case of a card

"mixed" chip.

Generally, smart cards are standardized and comply with standards, from both an electrical and mechanical point of view, in particular the following standards: ISO 7816 for contact smart cards, ISO 14443 for contactless, proximity cards. In the latter case, the frequency used is generally equal to 13.56 MHz, which reduces the size of the antenna, the latter no longer comprising

that two or three turns.

The availability of components for "mixed" smart cards leads to the design of new assembly processes. Keeping in mind that this type of component is the object of mass production, it is necessary that the final cost price be as low as possible. Furthermore, it is also necessary to obtain high reliability, as in the case of a

conventional smart card with contacts.

For all these reasons, it is therefore desirable to continue to use, as far as possible, assembly methods and technologies of the known art which have proven themselves. Among these methods, we can cite, in a non-exhaustive manner: - assembly of the semiconductor micromodule on a support of the printed circuit type, provided with galvanic contact pads; - The manufacture of the plastic material support of the smart card itself, by pressing a stack of layers of plastic material, and - inserting by gluing the micromodule into a

support cavity in plastic material.

However, it remains necessary to connect the semiconductor component, or "chip", to the antenna, and more precisely to the ends of the antenna, which poses a specific problem. The connection is made via connection pads which must be connected to the aforementioned ends. In the known art, it has been proposed to carry out this

connection using a double-sided printed circuit,

that is to say comprising metallized tracks, for example made of copper, on either side of an insulating support. The support is then a double-sided printed circuit. This solution has the disadvantage of a high cost. Therefore, it

does not meet at least one of the recalled requirements.

In addition, even if a high frequency is used (typically 13.56 MHz), the antenna consists of an open loop generally comprising at least two or three turns. There is therefore necessarily, at one place or another on the surface of the chip card, a crossing of two conductive tracks, directly above each other. It follows that an insulating

zone and a conductive "bridge" must be provided between two antenna sections. The main object of the invention is therefore to set up optimized connectors making it possible to connect conductive pads of the chip card micromodule to the ends of the antenna. It makes it possible, in particular, to minimize the number of metal layers, either at the level of the micromodule, or even at the level of the antenna. It preferably applies to "mixed" type smart cards. To do this, according to an important characteristic of the invention, the active face of the support carrying the integrated semiconductor component is used, that is to say on the contact pad side, to establish electrical connections between inputs-outputs. component and

coupling antenna terminations.

In a second embodiment, contact pads of the active face of the support are also used to establish electrical connections between

antenna portions.

The subject of the invention is therefore a smart card comprising a body based on layers of plastic materials, said smart card carrying on one of its layers an open loop antenna, said body being provided with a cavity intended to receive a micromodule comprising a specific interface intended to be connected to said open loop antenna by two input and / or output terminals, said micromodule comprising a semiconductor component fixed in a central region of a support, on a first face, characterized in that, said open loop antenna comprising at least one turn, said semiconductor component support is provided with at least first and second contact pads, each comprising first ends, located in a central area of said support in a region close to said input and / or output terminals, in that the first of said ranges extends to a peripheral zone of said support who

is opposite, passing over said semi-component

conductive, and the second of said areas extends from said region to a peripheral area of said support, close to this region, so that second ends of these areas are located in opposite peripheral areas, protruding from said coating, in that said contact pads are each connected to an input and / or output terminal by their first end, and in that terminations of said loop antenna open out under the second ends of said pads

contact and are electrically connected to it.

The invention also relates to the associated micromodule.

The invention will be better understood and other characteristics and advantages will appear on reading

the description which follows with reference to the appended figures,

among which: - Figure 1 schematically illustrates an embodiment of a micromodule, component side; FIGS. 2A to 2C illustrate, respectively, a smart card provided with an antenna connected to a micromodule, a micromodule of the type of FIG. 1, in bottom view, and this same smart card, in side view and section along AA of FIG. 2A; - Figures 3A and 3B illustrate, respectively, a smart card provided with an antenna connected to a micromodule and this same smart card, in side view and section along AA of Figure 3A, according to an additional alternative embodiment; - Figures 4A and 4B illustrate, respectively, a smart card provided with an antenna connected to a micromodule and this same smart card, in side view and section along AA of Figure 4A, according to a second additional embodiment ; - Figures 5A and 5B illustrate, respectively, a smart card provided with an antenna connected to a micromodule and this same smart card, in side view and section along AA of Figure 5C, according to a third additional embodiment ; and - and FIG. 5C illustrates, in top view, a micromodule modified to suit the third variant

of additional achievement.

Figure 1 schematically illustrates an example of micromodule 1 usable in the context of the invention. In reality, it has two main parts. Micromodule 1 is seen from below, i.e. from the side

opposite to the electrical contact pads.

The first part consists of the electronic "chip" 3 proper, that is to say an integrated semiconductor component, generally of rectangular parallelepiped shape and of small thickness, for example a microprocessor or equivalent. The

microprocessor 3 has legs or input terminals-

outputs 30, arranged on the periphery. The configuration, the function and the number of these inputs-outputs naturally depends on the precise component 3 used. The

microprocessor 3 includes in particular two input terminals-

specific outputs, 31 and 32, generally contiguous and communicating with an interface called "HF" (not shown). The second part consists of a support 2 consisting of a single-sided printed circuit 20, on which the semiconductor component 3 is bonded. This comprises conductive pads 21 (shown in dotted lines, since they are arranged on the top face), the number and configuration of which generally follows the above-mentioned ISO standards. The necessary connections between the pads 30 to 32 and the pads 21 are conventionally provided by thin conductive wires 300. More specifically, openings 210 are provided in the insulating layer of the support 2 to access the conductive pads 21, and

connect the two faces of the support 2.

Once the connections between the input-output terminals 30 of the semiconductor component 3 and the pads 21 have been made, the rear of the support 2 is coated with a resin, so as to guarantee good mechanical strength, and, incidentally, to isolate it electrically. We represented,

under reference 4, the delimitation of the coating.

Up to now, the operations described have been entirely conventional and common to the known art. To be able to connect the ends of the antenna loop 6 (terminations 600 and 610, FIG. 2A), two additional conductive pads are provided at the periphery of the support 2, 22 and 23 respectively. These areas are advantageously arranged symmetrically on either side of the component 3. There are also two openings, 220 and 230 through the support providing access to the opposite faces of the conductive areas. Tracks 22 and 23 are electrically isolated from each other and from

other conductive pads 21.

According to an important characteristic of the invention, at least one of the contact pads, the contact pad 22 in the example described in FIG. 1,

extends substantially from one edge to the other of the support 2.

This range has an opening 220 ', inside

the coating zone 4, on the side opposite the opening 220.

The opening 220 ' plays, for the input-output terminal 31, the role of the openings 210. Similarly, the additional contact pad 23 includes an opening 230 ', inside the coating area 4, but located on the same side as the opening 230. As a result, one of the input-output terminals, terminal 31, can be connected on one side of the support (bottom side in FIG. 1), via a wire 310 and metallized area 22-22 ', while the other, terminal 32, can be connected on the other side of the support (high side

in FIG. 1), via a wire 320 and the metallized area 23.

We will now describe an embodiment of a smart card according to the invention with reference to Figures 2A to 2C. The smart card 5 is of mixed type. It implements a micromodule 1 of the type illustrated by the

figure 1.

The latter is represented in FIG. 2B in top view, that is to say on the electrical contact side 21. As has been indicated, in addition to the "conventional" contact pads 21, intended to allow a dialogue between an organ of the type "card reader" (not shown), also conventional, two additional areas are provided, 22 and 23, for connecting the terminations, 600 and 610, of a

loop antenna 6 (Figure 2A).

It has been assumed that the frequency used is chosen from the high frequency range (13.56 MHz). The antenna includes at least one turn, more generally two or three, if the above frequency is used. In the example described, it has been assumed that the antenna, referenced 6, comprises three turns, 61 to 63. This antenna 6 is substantially planar, the turns, 61 to 63 being concentric and advantageously surrounding the zone where the micromodule is placed. 1, so as to present the largest possible surface, and thereby maximum sensitivity. In the example described, the turns 61 to 63 are substantially rectangular, that is to say likewise

form as the smart card 5.

The position of micromodule 1 is determined, a

a priori, by the specifications of the aforementioned standards,

i.e. in an area located in the upper left quarter of the smart card (in top view, as illustrated by the

Figure 2A).

An open cavity 51 is provided in the body 50 of the chip card 5, in which the module 1 is arranged. More precisely, as shown in FIG. 2C (in side view and in section along AA of the FIG. 2A), this cavity 51 comprises two zones, a central bowl 510, intended to contain the component 3 and its resin coating 4, and a shallower peripheral groove 511, on the bottom of which rests the periphery of the support 2. The openings, 220 and 230 are arranged at

vertical to the bottom of the peripheral groove 511.

Finally, according to a characteristic of the invention, the terminations 600 and 610 open onto the bottom of this groove 511. They advantageously take the form of

relatively wide conductive pads.

It is therefore easy to make a connection between these antenna termination pads 600 and 610, and the pads, 22 and 23, of the support 2. The arrangement adopted by the invention allows great manufacturing tolerance. We also note that there is, in this central region,

than a metallization level.

The establishment of the electrical conductivity between the micromodule 1 and the ends of the antenna 6 can be obtained by conventional means per se: conductive adhesive, conductive elastomer, welding, deformation and thermal welding of the metal of the support 2 against the pads

600 and 610.

The smart card 5 of the variant embodiment which has just been described with reference to FIGS. 2A to 2C responds

therefore well to the objectives which the invention set for itself.

However, there remains a drawback. In fact, the antenna 6 generally comprises a minimum of two or more turns. Whatever the configuration adopted, there must be, at one place or another on the surface of the chip card 5, one or more crossings of conductive tracks. In FIG. 2A, it can be seen that the terminal part of the turn 63 crosses the turns 61 and 62, in an area referenced ZC. To avoid a short circuit, it is necessary to provide insulation between these different conductive tracks. This can be achieved by performing several metallization levels, for example, by providing an insulating layer and a conductive "bridge". This solution is not

however not always satisfactory.

Also according to another important aspect of the invention, the intermediate sections of the turns of the antenna 6 are passed between its terminations, 600 and 610, that is to say in the central zone where the cavity 51 is located. We will describe a first variant according to this second embodiment, with reference to Figures 3A and 3B. FIG. 3A schematically illustrates the smart card, here referenced 5a, in top view, and FIG. 3B, illustrates this same smart card 5a, in side view and in section

according to AA of FIG. 3A, the micromodule 1 being assembled.

The elements common, or at least similar, to those represented in the preceding figures bear the same reference and will be re-described only as necessary. They are however associated with the letter 'a' if

there are structural changes.

According to the main characteristic of this embodiment, the antenna segments 6a establishing a connection between two successive turns, 61a to 63a for example, the segments 64 and 65 pass between the antenna terminations 600a and 610a. More precisely (FIG. 3B), provision is made for metallization of the turns of the antenna on a level 513, intermediate between the bottom of the peripheral groove 511 of the cavity 51, and the bottom of the central bowl 510 of this cavity. The antenna terminations open in the form of two areas, 600a and 610a, under the bottom of the peripheral groove 511, and contact is established with the contact areas

additional 22 and 23, respectively. The turns themselves

same, 61a to 63a, are also drawn on this level, which corresponds to the upper face of a layer of material

plastic of the smart card 5a.

Holes 5110 and 5111 are provided in the bottom of the peripheral groove 511 and perpendicular to the additional conductive pads, 22 and 23, respectively, and the corresponding openings, 220a and 230a. The connections between the contact pads, 22 and 23, and the antenna termination pads, 600a and 610a, are physically made by conductive pads, 221a and 231a, respectively. These pads could be replaced, in an alternative embodiment not shown, by a deformation of the contact pads towards the antenna terminations or on the contrary by a rise in

these terminations towards the contact pads.

This operation does not require great precision. Indeed, the layer of insulating material overhanging the level 513, on which the antenna metallizations are made, can be pre-drilled, which avoids any risk of destroying the areas, 600a and 610a. This risk would be real, if the drilling was carried out after the insulating layer had been carried out, the thickness of the

metallization being very weak.

It is assumed that the zone of metallization level 513 which is located directly above the bottom of the peripheral groove 511 has a width sufficient to allow free passage to at least one additional track between the internal edge, overlooking the

central bowl 510, and the ranges 600a and 610a above.

In the example described, the conductive track segment 64 is disposed between the termination 600a and the semiconductor component 3, and the conductive track segment 65 is disposed between the termination 610a and this same semiconductor component 3. In d In other words, the segments 64 and 65 are located on either side of the semiconductor component 3. In a variant not shown, the two segments, 64 and 65, could have been arranged on the same side of the semiconductor component. 3, in

the extent that the space left free is sufficient.

It is easy to see that all the metallizations forming the antenna are strictly in the same plane, that is to say at the bottom of the peripheral groove 511. The metallization

It is easy to see that all the metallizations forming the antenna are already in the same plane, that is to say on the bottom of the peripheral groove 511. The metallization of trace which has just been described

more particularly suitable when the semi-component

conductor 3 is relatively reduced in length. Otherwise, alternative embodiments will be preferred.

which will now be described.

A first additional variant embodiment will now be described by reference

in Figures 4A and 4B.

FIG. 4A schematically illustrates the smart card, here referenced 5b, in top view, and in FIG. 4B, this same smart card 5a, in side view and in section

according to AA of FIG. 4A, the micromodule 1 being assembled.

The elements common, or at least similar, to those represented in the preceding figures bear the same reference and will be re-described only as necessary. However, they are associated with the letter 'b' if

there are structural changes.

The connection segments, 64b and 65b, between turns, 61b to 63b, of the antenna 6b pass under the bottom of the cavity 51, on a level plate referenced 514. The turns themselves, 6lb to 63b, are traced also on this level, which corresponds to the upper face of one of the layers of plastic material of the smart card 5b. The studs, 221b and 231b, are slightly longer than the corresponding studs, 221a and 231a (Figure 3B), which does not

is not a significant drawback.

It is clear that this arrangement allows a greater latitude of wiring, since it is possible to have the entire surface of the bottom of the cavity 51, whatever the dimensions of the semiconductor component 3. As before, the metallization of the antenna 6b is produced

on a single level (level 514).

There remains, however, a minor aesthetic drawback. This provision does not leave

no room for a "crystal PVC" type material,

i.e. transparent on the outside of the smart card, except at

leave the antenna coils visible.

A second additional variant embodiment, making it possible to overcome this drawback, is described with reference to FIGS. 5A to 5C. FIG. 5A schematically illustrates the smart card, here referenced c, in top view, and FIG. 5B illustrates this same smart card, in side view and in section along AA of FIG. 5A, the micromodule, here referenced lc , being

assembled. FIG. 5C illustrates, in top view, that is to say

say on the conductive contact side, this modified lc micromodule

to suit this particular variant.

The elements common, or at least similar, to those represented in the preceding figures bear the same reference and will be re-described only as necessary. They are however associated with the letter 'c' if

there are structural changes.

In the example described, it was assumed that the antenna, here referenced 6c, included two turns 66 and 67. These two turns are cut, so that their ends can be interconnected on pads of

support contact 2c.

In fact, according to the main characteristic of this second additional variant embodiment, the connection between turns, 66 and 67, is made by means of a metallized area 26 made

directly on the support 2c.

The metallized tracks forming the turns, 66 and 67, of the antenna 6c can be produced in the manner described with reference to FIG. 3B, that is to say on a level plate 515 situated at an intermediate level between the bottom of the central bowl 510 of the cavity 51 and the bottom of the peripheral groove 511 of this same cavity, that is to say on the surface of one of the layers of material

plastic constituting the body 50c of the smart card 5c.

One of the ends, 660 or 671, of the turns, 66 or 67, of the antenna 6c, or antenna terminations, is connected to the micromodule lc in a similar, if not identical, manner to what has been described for the variant described with reference to FIG. 3B above, via two contact pads, 22c or 23c, and openings, 220c or 230c, respectively. On the other hand, a contact area is made up comprising two wide zones 24, 25 connected by a thin and elongated zone 26. Zones 24 and 25 are located one to the right (in FIG. 5C), the other to the left of antenna connection pads 22c and 23c, between the contact pads 21. In a variant not shown, the zone 26 could be provided with a greater width, by reducing the extent of the pads 22c and 23c. The connections between zones 24 and 25 and the antenna terminations 670 and 661, are made via the openings, 240 and 250, holes in the insulating layer overhanging the metallization level 515 (one of which, 5112, is visible on Figure 5B) and conductive pads (one of which, 241, is visible in Figure 8) It should be clear that, although the tracks, 66 and 67, of the antenna 6c are made on a first level (plate 515), and zones 24-25-26 between two turns on a second level, this does not create an additional level of metallization. Indeed, the interconnection level 24-25-26 is common to the metallization level already used for the contact pads, 21

to 23 (upper surface of the support pad 2c).

One can also imagine, in a variant not illustrated, making several connection metallizations of type 25, connecting pairs of additional contact pads. In this way, more than two successive turns can be interconnected. However, it is realized that, in practice, the number of possible interconnections made between the pairs of contacts 22 and 23 is very limited. This variant is however perfectly suited to an antenna configuration with two or three turns, which is generally the case for a frequency of 13.56 MHz. Reading the above, it is easy to see that the invention does achieve the goals it

settled down.

It should be clear, however, that the invention is not limited to only the examples of embodiments explicitly described, in particular in relation to the

Figures 1 to 5C.

In particular, the numerical values have been specified only to fix ideas. They essentially depend on the precise application targeted. The materials that can be used are those generally used in the field. In this sense, the invention remains compatible with current technologies, which is an additional advantage. The invention preferably applies to smart cards of the "mixed" type, but cannot in any case be limited to this single application. It also applies to contactless smart cards, although the benefits that can be derived are less than in

the first case.

Indeed, the advantages presented by the invention are numerous, in particular for "mixed" type smart cards, and among which the following: low cost price; - use of a support (printed circuit) of single-sided semiconductor component; - direct access to the additional contacts, and therefore to the high frequency interface, which makes it possible to carry out electrical tests by contact on the antenna connectors and to test the inputs-outputs of this interface; perfect compatibility with the processes implemented in the known art for the manufacture of micromodules and the inserting; and - the specific cavities provided for access to the antenna terminations allow a large tolerance on the volume of conductive material used to produce

the connection pads.

In an alternative embodiment (not shown), the input and / or output terminals of the high frequency interface of the semiconductor component are not grouped on the same side of the component, but distributed on two opposite sides. According to this variant, the connections with the contact pads are made on either side of the semiconductor component. The contact pad 22 (FIG. 1) therefore no longer necessarily extends above the semiconductor component to join the opposite side. This variant embodiment can naturally apply to the embodiments described with reference to FIGS. 3A-3B,

4A-4B and 5A-5C.

Patent Citations (8)

Publication number	Priority date	Publication date	Assignee	Title
WO1997034247A2 *	1996-03-14	1997-09-18	Pav Card Gmbh	Smart card, connection arrangement and method of producing a smart card
US5671525A *	1995-02-13	1997-09-30	Gemplus Card International	Method of manufacturing a hybrid chip card
DE19632115C1 *	1996-08-08	1997-12-11	Siemens Ag	Combination chip module for smart cards allowing both contacting- and contactless communication with external data station
Family To Family Citations				
FR2590051B1 *	1985-11-08	1991-05-17	Eurotechnique Sa	CARD COMPRISING A COMPONENT AND MICROMODULE WITH SIDING CONTACTS
JPH07117385A *	1993-09-01	1995-05-09	Toshiba Corp	Thin ic card and manufacture thereof
DE19654902C2 *	1996-03-15	2000-02-03	David Finn	Smart card
DE19632813C2 *	1996-08-14	2000-11-02	Siemens Ag	Method for producing a chip card module, chip card module produced using this method and combination chip card containing this chip card module
US6161761A *	1998-07-09	2000-12-19	Motorola, Inc.	Card assembly having a loop antenna formed of a bare conductor and method for manufacturing the card assembly

* Cited by examiner, † Cited by third party

Cited By (77)

Publication number	Priority date	Publication date	Assignee	Title
EP1093082A2 *	1999-10-12	2001-04-18	Fujitsu Limited	Combination card having an IC chip module
EP2239692A1 *	2009-04-11	2010-10-13	Cardag Deutschland GmbH	Chip card and method for its manufacture
FR3001332A1 *	2013-01-21	2014-07-25	Oberthur Technologies	Method for manufacturing body of dual-type smart card of electronic device, involves electrically conductively inserting insert in opening to establish electric connection between cavity and face of smart card

EP2340530A1 *	2010-08-23	2015-02-25	Gemalto SA	Electronic memory device
Family To Family Citations				
US6658979B2 *	2000-11-15	2003-06-24	Skyworks Solutions, Inc.	Structure and method for fabrication of a leadless chip carrier with embedded antenna
FR2820548A1 *	2001-02-02	2002-08-09	Schlumberger Systems & Service	PORTABLE CHIP AND ANTENNA OBJECT, MODULE FOR FORMING PORTABLE CHIP AND ANTENNA OBJECT AND METHODS OF MAKING SAME
JP4684430B2 *	2001-02-06	2011-05-18	大日本印刷株式会社	Contact / non-contact IC module and manufacturing method thereof
JP4724923B2 *	2001-02-08	2011-07-13	大日本印刷株式会社	Contact / non-contact IC module and manufacturing method thereof
JP2002341965A *	2001-05-14	2002-11-29	Alps Electric Co Ltd	Information apparatus provided with card
US20030037065A1 *	2001-07-30	2003-02-20	Alena Svab	Method and apparatus for using medical ID smart card
DE10147140A1 *	2001-09-25	2003-04-17	Giesecke & Devrient Gmbh	Chip card with display
US6634565B2 *	2001-11-06	2003-10-21	Litronic, Inc.	Smart card having additional connector pads
FR2834103B1 *	2001-12-20	2004-04-02	Gemplus Card Int	CHIP CARD WITH EXTENDED SURFACE MODULE
KR100910769B1 *	2002-06-11	2009-08-04	삼성테크윈 주식회사	IC card and manufacturing method thereof
US20050212690A1 *	2002-08-26	2005-09-29	Dai Nippon Printing Co., Ltd.	Sim, sim holder, ic module, ic card and ic card holder
EP1540581A2 *	2002-09-17	2005-06-15	Axalto S.A.	Hybrid card
DE10304824A1 *	2003-01-31	2004-08-12	Varta Microbattery Gmbh	Thin electronic chip card
NL1022766C2 *	2003-02-24	2004-09-21	Enschede Sdu Bv	Identity card as well as travel document.
US7051429B2 *	2003-04-11	2006-05-30	Eastman Kodak Company	Method for forming a medium having data storage and communication capabilities
JP4037332B2 *	2003-07-10	2008-01-23	シャープ株式会社	IC module and IC card
TWI284842B *	2003-07-14	2007-08-01	Nec Tokin Corp	Communication medium capable of carrying out contactless communication and method of producing the same
JP4518921B2 *	2003-11-20	2010-08-04	シャープ株式会社	IC card and manufacturing method thereof
US20050263596A1 *	2004-05-12	2005-12-01	Solicore, Inc.	Portable charger, including portable sleeve, for an electronically readable card
FR2872945B1 *	2004-07-07	2007-01-12	Oberthur Card Syst Sa	ELECTRONIC ENTITY COMPRISING AN ANTENNA, INLAY AND MODULE FOR SUCH AN ENTITY
JP4718192B2 *	2005-01-17	2011-07-06	新光電気工業株式会社	Reader / Writer
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
DE102005036303A1 *	2005-04-29	2007-08-16	Giesecke & Devrient Gmbh	Method for initializing and / or personalizing a portable data carrier
US7777317B2 *	2005-12-20	2010-08-17	Assa Abloy Identification Technologies Austria GmbH (Austria)	Card and manufacturing method
KR100723491B1 *	2005-07-14	2007-05-30	삼성전자주식회사	Universal PCB and smart card using the same
FR2890212B1 *	2005-08-30	2009-08-21	Smart Packaging Solutions Sps	ELECTRONIC MODULE WITH A DOUBLE COMMUNICATION INTERFACE, IN PARTICULAR FOR A CHIP CARD
AT428153T *	2005-12-30	2009-04-15	Incard Sa	IC CARD WITH IMPROVED CIRCUIT BOARD
EP1816593A1 *	2006-02-03	2007-08-08	Axalto SA	Chip card connector
US7991156B2 *	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
WO2009060425A2 *	2007-11-08	2009-05-14	On Track Innovations Ltd.	Electronic interface apparatus and method and system for manufacturing same
HK1109708A2 *	2007-04-24	2008-06-13	On Track Innovations Ltd	Interface card and apparatus and process for the formation thereof
KR101103186B1	2007-11-08	2012-01-04	스마트랙 아이피 비.브	Electronic interface apparatus and method and system for manufacturing same

			이.	
US7980477B2 †	2007-05-17	2011-07-19	Féinics Amatech Teoranta	Dual interface inlays
US9741027B2 *	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US8030746B2 *	2008-02-08	2011-10-04	Infineon Technologies Ag	Integrated circuit package
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US20100078485A1 *	2008-09-29	2010-04-01	Dynacard Co., Ltd.	Subscriber identity module card
EP2401708A4 *	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
US9272378B2	2010-08-12	2016-03-01	Féinics Amatech Teoranta	Laser ablating structures for antenna modules for dual interface smartcards
DE102009058435A1 *	2009-12-16	2011-06-22	Giesecke & Devrient GmbH, 81677	Attaching and electrically connecting a chip module to a chip card
US8678282B2	2010-08-12	2014-07-29	Feinics Amatech Teoranta	RFID antenna modules and methods of making
WO2015071086A1 *	2013-11-13	2015-05-21	Féinics Amatech Teoranta	Connection bridges for dual interface transponder chip modules
US8991712B2	2010-08-12	2015-03-31	Féinics Amatech Teoranta	Coupling in and to RFID smart cards
US9489613B2 *	2011-08-08	2016-11-08	Féinics Amatech Teoranta	RFID transponder chip modules with a band of the antenna extending inward
FR2976382B1 *	2011-06-10	2013-07-05	Oberthur Technologies	MICROCIRCUIT MODULE AND CHIP CARD COMPRISING THE SAME
US8842046B2 *	2011-07-22	2014-09-23	Texas Instruments Incorporated	Loop antenna
US11106877B2	2014-03-08	2021-07-20	Féinics AmaTech Teoranta Lower Churchfield	Connection bridges for dual interface transponder chip modules
US8864982B2	2011-11-07	2014-02-11	Blackberry Limited	Universal integrated circuit card apparatus and related methods
US8691610S1	2011-11-07	2013-10-15	Blackberry Limited	Device smart card
US8955681B2	2011-11-07	2015-02-10	Blackberry Limited	Universal integrated circuit card apparatus and related methods
DE102011056328B4 *	2011-12-13	2019-04-04	Infineon Technologies Ag	Chip card contact field configuration
CN102569947A *	2012-01-17	2012-07-11	华为终端有限公司	Integrated module, integrated system board and electronic equipment
USD703208S1	2012-04-13	2014-04-22	Blackberry Limited	UICC apparatus
US8936199B2	2012-04-13	2015-01-20	Blackberry Limited	UICC apparatus and related methods
USD701864S1 *	2012-04-23	2014-04-01	Blackberry Limited	UICC apparatus
US8758372S1	2013-03-13	2016-06-07	Nagrastar Llc	Smart card interface
USD759022S1 *	2013-03-13	2016-06-14	Nagrastar Llc	Smart card interface
USD729808S1 *	2013-03-13	2015-05-19	Nagrastar Llc	Smart card interface
US9167691B2 *	2013-04-16	2015-10-20	Identive Group, Inc.	Dual interface module and dual interface card having a dual interface module manufactured using laser welding
EP2811427A1 *	2013-06-07	2014-12-10	Gemalto SA	Method for manufacturing an anti-cracking electronic device
US20150028108A1 *	2013-07-24	2015-01-29	Alien Technology Corporation	Double loop inductor rfid
JPWO2015099026A1 *	2013-12-27	2017-03-23	トッパン・フォームズ株式会社	Non-contact type data receiving / transmitting body, and wireless IC tag and wireless IC holding body including the same
EP2892012A1	2014-01-06	2015-07-08	Gemalto SA	Electronic module, method for manufacturing same and electronic device including such a module
USD780763S1 *	2015-03-20	2017-03-07	Nagrastar Llc	Smart card interface

US8644968B1	2015-04-30	2019-10-29	Echostar Technologies L.L.C.	Smart card interface
WO2016206801A1 *	2015-06-23	2016-12-29	Pretema Gmbh	Smart card blank with at least one interface for contactless transmission of information
CN107025481B *	2016-02-02	2021-08-20	上海伯乐电子有限公司	Flexible printed circuit board, smart card module using same and smart card
DE102016114419B4	2016-08-01	2021-07-22	Infineon Technologies Ag	CHIP CARD MODULE, CHIP CARD, CHIP CARD ARRANGEMENT, METHOD FOR DESIGNING A CHIP CARD MODULE AND METHOD FOR DESIGNING A CHIP CARD
US10282654B2 *	2017-07-09	2019-05-07	Interlake Research, Llc	Tag assembly methods
WO2019045638A1 *	2017-08-28	2019-03-07	Smartflex Technology Pte Ltd	Integrated circuit modules and smart cards incorporating the same
US10763203B1	2019-02-08	2020-09-01	Nxp B.V.	Conductive trace design for smart card
US11010652B2 *	2019-05-09	2021-05-18	Capital One Services, Llc	Orientationless chip layout for a transaction card

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
FR2788646A1	2000-07-21	Contactless memory chip/integrated antenna connection construction having micromodule isolated support cavity placed and two central contact planes connecting support lanes and antenna ends.
CA1319430C	1993-06-22	Flexible printed circuit, especially for electronic cards, and card incorporating such a circuit
EP3143557B1	2019-07-03	Method for producing a circuit for a chip card module and circuit for a chip card module
FR2756955A1	1998-06-12	METHOD FOR PRODUCING AN ELECTRONIC CIRCUIT FOR A CONTACTLESS MEMORY CARD
EP2143048A2	2010-01-13	Chip card with a dual communication interface
EP0424262B1	1992-06-17	Portable electronics with connectable components
EP0424263B1	1992-08-05	Chip card system with offset, portable electronic unit
FR2765010A1	1998-12-24	ELECTRONIC MICROMODULE, ESPECIALLY FOR CHIP CARDS
EP2718877B1	2016-12-07	Microcircuit module and smart card comprising same
EP0925553B1	2001-08-29	Method for making an assembly of electronic modules for contactless memory cards
FR2634095A1	1990-01-12	Flexible printed circuit, especially for a card having electronic microcircuits, and card incorporating such a circuit
FR2785071A1	2000-04-28	Method for manufacturing contactless IC with internal aerial by using adhesive current conducting foil on contact pads for making contact with antenna and fixing chip
FR2625067A1	1989-06-23	METHOD FOR ATTACHING AN ELECTRONIC COMPONENT AND CONTACTS TO IT
FR2780534A1	1999-12-31	Fabrication method for portable objects incorporating electronic components, particularly non-contact smart cards
FR3079645A1	2019-10-04	ELECTRONIC DOCUMENT HAVING AN ELECTRICAL CONNECTION BETWEEN A CHIP PORT AND AN EXTERNAL ELECTRIC CONTACT BEACH ESTABLISHED VIA AN INLAY
FR2781588A1	2000-01-28	Non-contact card using electromagnetic wave transmission between the cards integrated circuits and a read/write device and method of card fabrication
EP3114612A1	2017-01-11	Simplified electronic module for a smartcard with a dual communication interface
FR2837013A1	2003-09-12	Display module credit card/payment card/money payment having display module and chip module with conductor track conjugate contact zones and electronic control chip tracks connected/encapsulated
FR2745931A1	1997-09-12	SMARTCARD
EP3695966A1	2020-08-19	Electronic card comprising an adhesive receiving sub-cavity for inserting a module and method for manufacturing such an electronic card
FR3093228A1	2020-08-28	DOUBLE CONTACT AND NON-CONTACT INTERFACE MODULE WITH ONE OR MORE ADDITIONAL INTERFACES
FR2796203A1	2001-01-12	CONTACTLESS ELECTRONIC MODULE AND METHOD FOR OBTAINING THE SAME
EP2954462A1	2015-12-16	Method for connecting a microcircuit to accessible conductive areas in a support
FR3095284A1	2020-10-23	Electronic module for smart card comprising a display screen
FR2938380A1	2010-05-14	Support layer for wire antenna of microcircuit card, has contact pads comprising set of connection zones arranged outside standard area,

on which connection with end of corresponding wire connection element is realized

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
FR9900486A	1999-01-19	1999-01-19	CHIP CARD HAVING A LOOP ANTENNA, AND ASSOCIATED MICROMODULE

Applications Claiming Priority (8)

Application	Filing date	Title
FR9900486A	1999-01-19	CHIP CARD HAVING A LOOP ANTENNA, AND ASSOCIATED MICROMODULE
US09/646,402	2000-01-19	Chip card equipped with a loop antenna, and associated micromodule
PCT/FR2000/000110	2000-01-19	Chip card equipped with a loop antenna, and associated micromodule
EP00900614A	2000-01-19	Chip card equipped with a loop antenna, and associated micromodule
CN00800800360A	2000-01-19	Chip card equipped with loop antenna, and assiciated micromodule
JP2000595803A	2000-01-19	Micromodule combined with chip card with loop antenna
DE60042718T	2000-01-19	CHIP CARD WITH A GRINDING ANTENNA AND ASSOCIATED MICROMODULES
HK01106874A	2001-09-28	Chip card equipped with a loop antenna, and asociated micromodule.

Legal Events

Date	Code	Title	Description
2004-03-12	TP	Transmission of property	
2004-03-12	CA	Change of address	
2009-11-27	ST	Notification of lapse	**Effective date:** 20091030

Data provided by IFI CLAIMS Patent Services

Patents JPH1097599

Portable terminal equipment for ic card

Abstract

PROBLEM TO BE SOLVED: To provide a portable terminal equipment for IC card, into which a plurality of IC cards can be inserted and which is convenient for carrying, by inserting the plurality of IC cards so that respective partial parts differ in the equipment. SOLUTION: The plurality of IC cards 100, 110 and 120 are shifted and overlapped in a body and insertion is completed. Thus, the electric contact terminals 16-18 of a substrate 19 are respectively brought into contact with the electric contact terminals 102, 112 and 122 of the plurality of IC cards 100, 110 and 120 inserted into a card insertion port 12. A guide device 20 comprising a spring material or the like is provided in the body 10. The plurality of IC cards 100, 110 and 120 are guided to prescribed positions 130, 140 and 150 in an insertion order by always pressing the IC card to be inserted to a lower side by the guide device 20. The electric contact terminals in the card insertion port are arranged on the same substrate and the plurality of IC cards 100, 110 and 120 are shifted and inserted.

Classifications

⊗ G07F7/1008 Active credit-cards provided with means to personalise their use, e.g. with PIN-introduction/comparison system

View 7 more classifications

JPH1097599A

Japan

Find Prior Art Similar

Other languages: Japanese

Inventor: Maki Ito, 真樹 伊藤, Yuhei Abe, 雄平 阿部

Worldwide applications

1996 JP 1997 CA US AU BE EP CN 1999 US

Application JP8251183A events

1996-09-24 Application filed by Hitachi Ltd, 株式会社日立製作所

1996-09-24 Priority to JP8251183A

1998-04-14 Publication of JPH1097599A

Status Granted

Info: Patent citations (20), Cited by (51), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (12)

Hide Dependent

[Claims]

1. An IC card portable terminal device for reading or writing the contents of each of a plurality of IC cards, said plurality of IC cards each having an electric contact portion. By inserting the C card so that at least a part of each of them overlaps inside the device, the plurality of IC cards are inserted into the plurality of device-side electrical contact portions provided inside the device corresponding to the insertion positions of the plurality of IC cards. A portable terminal device for an IC card, wherein the plurality of IC card-side electrical contact portions are brought into one-to-one contact with each other.

    2. 2. A plurality of IC cards to be inserted are mounted inside the device so that the electrical contact portion on the IC card side is not prevented from contacting the electrical contact portion on the device side by another IC card. The portable terminal device for an IC card according to claim 1, wherein the portable terminal devices are shifted from each other and overlapped.

    3. 3. The portable terminal device for an IC card according to claim 1, wherein said plurality of IC cards are inserted from one card insertion slot.

    4. 4. The portable terminal device for an IC card according to claim 3, wherein the plurality of IC cards are guided to a predetermined position in the order of insertion by a guide provided inside the device. .

    5. 5. The method according to claim 1, wherein the plurality of IC cards are separately inserted from a plurality of card insertion slots.
    3. The mobile terminal device for an IC card according to claim 1.

    6. 6. The IC card portable according to claim 5, wherein the first card is inserted from the first card insertion slot, and the second card is inserted from the second card insertion slot. Terminal device

    7. 7. The apparatus according to claim 1, wherein the plurality of electrical contacts on the device side are provided on the same substrate inside the device.
    3. The mobile terminal device for an IC card according to claim 1.

    8. 8. The portable terminal device for an IC card according to claim 1, further comprising an opening for extruding and extracting said plurality of IC cards.

9. 9. When a plurality of IC cards are inserted into the device, the electrical contact portions provided on the IC card side and the electrical contact portions provided on the device side come into contact with each other, and Display of information of each IC card or the plurality of IC cards
In a portable terminal device for an IC card for transferring information between cards, the plurality of IC cards are inserted from the outer shape of the device by inserting the plurality of IC cards so that at least a part of each IC card overlaps inside the device. A portable terminal device for an IC card, wherein the portable terminal device is stored without protruding.

10. 10. When a plurality of IC cards are inserted into the device, the electrical contact portions provided on the IC card side and the electrical contact portions provided on the device side come into contact with each other, and In the portable terminal device for an IC card for reading or writing the contents of each of the IC cards, the thickness of the device main body is reduced by inserting the plurality of IC cards so that at least a part of each IC card overlaps inside the device. A portable terminal device for an IC card.

11. 11. When a plurality of IC cards are inserted into the device, the electrical contact portions provided on the IC card side and the electrical contact portions provided on the device side come into contact with each other, and in the portable terminal device for an IC card for reading or writing the contents of each of the IC cards, the width of the device main body is reduced by inserting the plurality of IC cards so that at least a part of each IC card overlaps inside the device. IC having a width substantially equal to the width of the IC card
Mobile terminal for cards.

12. 12. When a plurality of IC cards are inserted into the device, the electrical contact portions provided on the IC card side and the electrical contact portions provided on the device side come into contact with each other, and in the portable terminal device for an IC card which reads or writes the contents of each of the IC cards, the length of the device body is reduced by inserting the plurality of IC cards so that at least a part of each IC card overlaps inside the device. A portable terminal device for an IC card, which is substantially equal in length to the IC card.

Description

DETAILED DESCRIPTION OF THE INVENTION

[0001]

BACKGROUND OF THE INVENTION 1. Field of the Invention The present invention relates to an apparatus for reading or writing electronic information recorded on an IC card or the like by inserting the IC card or the like.

[0002]

2. Description of the Related Art As an example of the prior art, Japanese Utility Model Laid-Open Publication No.
There is a "reader and writer with door for IC card" described in Japanese Patent No. 957. According to the present invention, only one IC card can be inserted into one card insertion slot, and when a plurality of IC cards are inserted, the number of card insertion slots and the inside must be increased. The problem arises. In the case of the present invention, only electronic money is displayed.

As another example, Japanese Patent Application Laid-Open No. 6-2010
No. 6, there is a "data transfer system and a data transfer terminal device". According to the present invention, two IC cards can be inserted into the two card insertion slots. However, as described above, the number of the card insertion slots and the number of the insides are increased, so that the size of the apparatus is increased. Originally, it is based on the premise that electronic payment is made from an individual to a store at a storefront, and therefore, portability is not involved. In the case of the present invention, display and exchange of electronic money are performed as described above.

[0004] As another example, there is an "electronic money information transfer device" already filed by the Company. In the present invention,
Since two IC cards can be inserted into two card insertion slots, and two IC cards are inserted facing each other on the same plane, the device can be made thinner and more portable. In. However, since it is assumed that one of the two cards is an IC card of another person and that electronic money is exchanged between the other person and oneself, it is sufficient that this one piece can be partially inserted. When inserted, most of them protrude outside the device. In the case of the present invention, display and exchange of electronic money are performed as described above.

[0005]

SUMMARY OF THE INVENTION An object of the present invention is to display and exchange electronic information on a plurality of IC cards.
A portable terminal device for a C card, firstly, a portable terminal device for an IC card that can be easily carried by inserting a plurality of IC cards, and secondly, a plurality of IC cards do not protrude outside the device. A portable terminal device for an IC card which can be inserted and is easy to carry. Thirdly, the present invention is directed to an IC card portable terminal device which is easy to use in inserting and removing an IC card in the above IC card portable terminal device.

[0006]

In order to achieve the above first and second objects, a portable terminal device for an IC card according to the present invention comprises a plurality of IC cards each having an electric contact portion. It shall be inserted so that a part may overlap inside an apparatus. In particular, multiple inserted ICs
The cards are shifted from each other and overlapped inside the device so that the electrical contact portions on the IC card side are not prevented from contacting the electrical contact portion on the device side by another IC card

Accordingly, the electrical contact portions on the plurality of devices provided inside the device corresponding to the insertion positions of the plurality of IC cards respectively correspond to the electrical contact portions on the plurality of IC cards. Touch with 1. The plurality of electrical contacts on the device side are provided on the same substrate inside the device.
As a result, the contents of each of the plurality of IC cards can be read or written.

[0008] In order to achieve the first object, a plurality of IC cards may be inserted from one card insertion slot.

In order to achieve the second object, a portable terminal device for an IC card in which a plurality of IC cards are separately inserted from a plurality of card insertion slots may be provided. In particular, the first card is inserted from the first card slot, and the second card is inserted from the second card slot.
What is necessary is just to be a portable terminal device for C cards.

[0010] In order to achieve the third object,
The portable terminal device for an IC card according to the present invention has a guide portion provided inside the card insertion slot of the device.

Thus, a plurality of IC cards are guided to a predetermined position in the order of insertion.

Further, in order to achieve the third object,
The portable terminal device for an IC card of the present invention has an opening provided on the surface of the device.

Thus, a plurality of IC cards can be pushed out and taken out.

[0014]

FIG. 1 is a perspective view showing an external appearance of an example of a portable terminal device for an IC card according to the present invention. This IC card portable terminal device has a box-shaped main body 10, a display unit 80, and a balance confirmation button 82. The main body 10 has a card insertion slot 12 into which an IC card is inserted. A plurality of IC cards 100, 110, 120 are inserted into the card insertion slot 12.

By pressing the balance check button 82,
The balance of the electronic currency recorded on each IC card can be confirmed on the display unit 80. The display unit 80 is, for example, a liquid crystal display device. Switching of the balance display of each IC card may be performed by the balance display button 82. Or you may make it perform by the button which added further. In addition, the electronic currency can be exchanged between the cards by another added button. Thus, electronic currency can be exchanged between another person and oneself, for example, between a parent and child, between friends, or between two cards for oneself, for example, between a savings card and a consumption card.

FIG. 2 is a view of one example of the portable terminal device for an IC card according to the present invention as viewed from the back side. An opening 76 communicating with the card insertion slot 12 is provided on the back surface of the main body 10. By putting a finger on the inserted IC card which is visible from the opening and pushing out the card, the card can be easily taken out.

FIG. 3 is a sectional view of the portable terminal device for IC card according to the first embodiment of the present invention. In the main body 10, a single substrate 19 having electrical contact terminals 16, 17, 18 on the device side is disposed. Multiple IC cards 10
0, 110, and 120 are shifted from each other in the main body and overlap each other to complete the insertion. Therefore, the electrical contact terminals 16, 17, 18 of the substrate 19 come into contact with the electrical contact terminals 102, 112, 122 of the plurality of IC cards 100, 110, 120 inserted into the card insertion slot 12, respectively.
In this state, the contents of each of the plurality of IC cards can be read or written. further,
A guide device 20 made of a spring material or the like is provided in the main body 10, and a plurality of IC cards 100 and 11 are pressed by pressing down an IC card into which the guide device 20 is always inserted.
0, 120 are inserted at predetermined positions 130, 140, 15 in the order of insertion.
Guide to 0. As described above, the electric contact terminals inside the card insertion slot are arranged on the same substrate, and a plurality of IC cards are shifted and inserted, so that the body 10 can be thinned accordingly. In the portable terminal device for an IC card according to the present embodiment, the second and third IC cards protrude and are inserted. Therefore, in the insertion direction, the length of the device itself is equal to the length of the IC card. It is almost the same.

FIG. 4 is a sectional view of a portable terminal device for an IC card according to a second embodiment of the present invention. In the main body 10, a single substrate 19 having electric contact terminals 16 and 17 on the device side is provided. Multiple IC cards 100, 1
10 are shifted from each other in the main body and overlap each other to complete the insertion. Therefore, the electrical contact terminals 16 and 17 of the substrate 19
Contacts the electrical contact terminals 102, 112 of the plurality of IC cards 100, 110 inserted into the card insertion slot 12, respectively. In this state, the contents of each of the plurality of IC cards can be read or written. Further, the guiding device 20 is utilized by utilizing the elasticity of the main body 10.
is provided. Further, the guide device 20 may be a separate component. The guide device 20 guides the IC cards 100 and 110 to predetermined positions 130 and 140 in the insertion order by pressing the inserted IC card upward. Thus, the electrical contact terminals inside the card insertion slot are arranged on the same substrate,
Since the plurality of IC cards are inserted while being shifted, the body 10 can be made thinner. Further, since the second and subsequent IC cards are inserted with their leading ends pushed into the center of the main body, the main body 10 can be made thinner.
The portable terminal device for an IC card according to the present embodiment also has a second I
Because the C card protrudes and is inserted,
in the insertion direction, the length of the device itself is almost the same as the length of the IC card.

FIG. 5 is a cross-sectional view of an IC card portable terminal device having a plurality of card insertion slots sharing the inside according to a third embodiment of the present invention. The main body 10 has a plurality of card insertion ports 12 and 13. In the main body 10, a single substrate 19 having electric contact terminals 16 and 17 on the device side is provided. The plurality of IC cards 100 and 110 are shifted from each other and overlap each other in the main body, and the insertion is completed. Therefore, when the first IC card 100 is inserted through the card insertion slot 12, the IC card 100 is guided to a predetermined position 130, and the terminal 102 of the IC card 100 and the terminal 16 of the base board 19 come into contact. When the second IC card 110 is inserted from the card insertion slot 13, the IC card 110 is guided to a predetermined position 140 while the leading end of the IC card 110 is pushed toward the center of the main body, using the first IC card as a guide. I
The terminal 112 of the C card 110 contacts the terminal 17 of the base 19. In this state, the contents of each of the plurality of IC cards can be read or written.
In this embodiment, the number of card insertion ports is two, but a card insertion port may be further added. As described above, the electric contact terminals inside the card insertion slot are arranged on the same substrate, and a plurality of IC cards are shifted and inserted, so that the body 10 can be thinned accordingly. Since the second and subsequent IC cards are inserted without protruding into the portable terminal device for an IC card according to the present embodiment, electronic currency can be exchanged between two or more cards for oneself when carrying. If you want to do it, it is convenient.

FIG. 6 is also a cross-sectional view of a portable terminal device for IC card having a plurality of card insertion slots sharing the inside according to the third embodiment of the present invention. The portable terminal device for IC card of FIG. is added. With this shear plate 25, the IC card can be inserted into or removed from any of the plurality of card insertion ports 12, 13 in any order.

[0029]

The following effects can be obtained by inserting a plurality of IC cards such that at least a part of each IC card overlaps inside the apparatus.

One is the above-mentioned prior art disclosed in Japanese Unexamined Patent Publication No.
The present invention relates to an IC for a data transfer system and a data transfer terminal device described in
The thickness of the main body of the apparatus can be reduced by the amount of the stacked cards.

On the other hand, the present invention does not need to open a spread IC card portable terminal device or the like as much as the IC card is stacked, and does not require a hinge for spread, so that the width of the device body is reduced. It is closer to the width of the IC card.

One is that the present invention does not insert two IC cards on the same plane, facing each other, such as the "electronic money information transfer device" already applied for by the Company.
The length of the main body of the apparatus can be made closer to the length of the IC card by an amount equivalent to the insertion of the IC card.

As described above, according to the present invention, the apparatus main body can be made as close as possible to the size of an IC card, so that it is convenient to carry.

Further, by inserting a plurality of IC cards so that at least a part of each of them overlaps inside the apparatus, particularly by inserting a plurality of IC cards separately from a plurality of card insertion ports, more detailed description is given. Can insert a first card from the first card insertion slot and insert a second card from the second card insertion slot to accommodate a plurality of IC cards without protruding from the outer shape of the device. it can.

This is, of course, convenient for carrying around, but the above-mentioned "electronic money information transfer device" already applied for by the Company assumes the exchange of electronic money between another person and his / her own card, The present invention can completely store only one card for oneself, while the present

invention can completely store plural cards for oneself while carrying, and in this state, electronic money can be transferred between a plurality of cards owned by oneself. Can communicate and is highly convenient.

Further, a plurality of IC cards can be inserted so that at least a part of each IC card overlaps inside the apparatus, that is, a plurality of IC cards can be stored inside the apparatus, and a card holder can be inserted. As convenient.

[Brief description of the drawings]

FIG. 1 shows a portable terminal device for an IC card according to the present invention.
Perspective view showing the appearance of the example

FIG. 2 shows a portable terminal device for an IC card according to the present invention.
View from the back of the example

FIG. 3 is a sectional view of the portable terminal device for an IC card according to the first embodiment of the present invention.

FIG. 4 is a sectional view of a portable terminal device for an IC card according to a second embodiment of the present invention.

FIG. 5 is a cross-sectional view of a portable terminal device for an IC card having a plurality of card insertion ports sharing the inside according to a third embodiment of the present invention.

FIG. 6 is a cross-sectional view of a portable terminal device for an IC card having a plurality of card insertion openings and a sharp plate sharing the inside according to a third embodiment of the present invention.

[Explanation of symbols]

DESCRIPTION OF SYMBOLS 10 ... IC card portable terminal device main body 12, 13 .. Card insertion slot 16, 17, 18 ... Electrical contact terminal on the board side 19 ... Board 20 ... Guide device 25 ... Shikiri board 76 ··· Opening 80 · Liquid crystal display 82 · Balance check button 100, 110, 120 ··· IC card 102, 112, 122 ··· IC card electrical contact terminals 130, 140 , 150... Predetermined position

Patent Citations (20)

Publication number	Priority date	Publication date	Assignee	Title
JPH04155471A *	1990-10-19	1992-05-28	Oki Electric Ind Co Ltd	Transaction authentication system
JPH04236686A *	1991-01-18	1992-08-25	Ricoh Co Ltd	Ic card loading device
JPH0554201A *	1990-11-28	1993-03-05	Ricoh Co Ltd	Multistage ic card connector
JPH05238555A *	1992-02-20	1993-09-10	Fujitsu Ltd	One-board computer
JPH0619945A *	1991-12-13	1994-01-28	Matsushita Electric Ind Co Ltd	Data transfer system portable terminal equipment
JPH0684022A *	1993-06-25	1994-03-25	Canon Inc	Electronic apparatus
JPH0863556A *	1994-07-13	1996-03-08	Schlumberger Ind	Portable interface for electric smart card
JPH0877313A *	1994-09-02	1996-03-22	Mitsuo Hirase	Magnetic card case fitting inner plate
JPH08202660A *	1995-01-27	1996-08-09	Matsushita Electric Ind Co Ltd	Portable information terminal equipment
Family To Family Citations				
US4277837A *	1977-12-30	1981-07-07	International Business Machines Corporation	Personal portable terminal for financial transactions
DE3736258A1 *	1987-10-27	1989-05-11	Mannesmann Kienzle Gmbh	DATA CARD ARRANGEMENT
US5296692A *	1988-10-24	1994-03-22	Sharp Kabushiki Kaisha	IC card adapter for use in memory card slot with or without superimposed memory card
US5434395A *	1990-03-05	1995-07-18	Jean-Rene Storck	Method and device for effecting a transaction between a first and at least one second data carrier and carrier used for this purpose
KR0125095B1 *	1991-12-13	1997-12-15	다니이 아끼오	Data transfer method
JPH082781SB2 *	1991-12-13	1996-03-21	松下電器産業株式会社	Electronic asset data transfer method
DE69314466T2 *	1992-08-12	1998-05-07	Oki Electric Ind Co Ltd	Chip card
FR2715783B1 *	1994-02-02	1996-04-05	Laracom	IT tool for direct communication between individuals and operating system.
MY114883A *	1994-11-14	2003-02-28	Ibm	Method and apparatus for providing a remotely located outrigger card electrically coupled to a control card

GB2298743B *	1995-03-10	1998-10-14	Kenven Developments Limited	A connector for making surface electrical connections to IC cards
JPH0950497A *	1995-08-09	1997-02-18	Hitachi Ltd	Electronic money information transfer device

* Cited by examiner, † Cited by third party

Cited By (51)

Publication number	Priority date	Publication date	Assignee	Title
JPH10302030A *	1997-02-28	1998-11-13	Toshiba Corp	Connection device and information processor
Family To Family Citations				
JPH0950497A *	1995-08-09	1997-02-18	Hitachi Ltd	Electronic money information transfer device
DE19624079D1 *	1996-06-17	1998-01-29	Bosch Gmbh Robert	Card readers for chip cards
JP3130086B2 *	1998-08-31	2001-06-25	株式会社ソーメディア	Mobile communication device, information transmission system and method, non-contact IC media usable in mobile communication device
GB2343091B *	1998-10-19	2004-05-19	Ibm	Electronic business card exchange
JP3522549B2	1998-10-22	2004-04-26	富士通株式会社	Data transfer control method and data transfer control device
JP2000172796A *	1998-12-09	2000-06-23	Hitachi Ltd	Electronic pocketbook and its operating method
JP2000276543A *	1999-03-26	2000-10-06	Fujitsu Ltd	Numerical data processor and numerical data processing method
EP1079324A1 *	1999-08-25	2001-02-28	Smartdata SA	Electronic apparatus comprising a group of smart cards
US6250985B1 *	1999-10-04	2001-06-26	Wolfgang Neifer	Chip card reading apparatus
US6394343B1 *	1999-10-14	2002-05-28	Jon N. Berg	System for card to card transfer of monetary values
JP3617404B2 *	2000-03-07	2005-02-02	日本電気株式会社	Mobile phone
US7252240B1 *	2000-07-06	2007-08-07	Onspec Electronics, Inc.	Memory module which includes a form factor connector
US7493437B1	2000-07-06	2009-02-17	Mcm Portfolio Llc	Flashtoaster for reading several types of flash memory cards with or without a PC
US7278585B2 *	2000-07-06	2007-10-02	Onspec Electronic, Inc.	Field-operable, stand-alone apparatus for media recovery and regeneration
US7295443B2 *	2000-07-06	2007-11-13	Onspec Electronic, Inc.	Smartconnect universal flash media card adapters
US6438638B1 *	2000-07-06	2002-08-20	Onspec Electronic, Inc.	Flashtoaster for reading several types of flash-memory cards with or without a PC
JP4501241B2 *	2000-07-10	2010-07-14	ソニー株式会社	IC card and IC card data communication method
US6824063B1	2000-08-04	2004-11-30	Sandisk Corporation	Use of small electronic circuit cards with different interfaces in an electronic system
DE60101778T2 *	2001-02-14	2004-12-02	Smartdata S.A.	Modular chip card system
US6402558B1 *	2001-03-13	2002-06-11	Ritek Corporation	Memory card adapter
US7412558B2 *	2002-01-10	2008-08-12	O2Micro International Limited	Enhanced protocol conversion system capable of providing offloaded protocol instruction processing
US6941405B2 *	2001-08-21	2005-09-06	O2Micro International Limited	System and method capable of offloading converter/controller-specific tasks to a system microprocessor
DE50206259D1 *	2001-11-16	2006-05-18	Omnikey	CONTACTING DEVICE FOR CARRYING INFORMATION CARRIER AND HEREIN EQUIPPED

			Gmbh	READING UNIT
US6738259B2 *	2001-11-19	2004-05-18	Imation Corp	Apparatus supporting multiple memory card formats
JP4351826B2 *	2002-01-23	2009-10-28	アルプス電気株式会社	Card connector device
DE10227558A1 *	2002-06-20	2004-01-15	Infineon Technologies Ag	System for data exchange between at least two contactless data carriers
JP4049625B2 *	2002-06-28	2008-02-20	モレックスインコーポレーテッド	Card connector
US20040198444A1 *	2002-08-02	2004-10-07	Yen-Hung Chen	Mobile phone IC card holder
DE10246350A1 *	2002-10-04	2004-04-15	Siemens Ag	Device for receiving and contacting contact-type intelligent cards e.g. for digital tachographs in vehicles, has card receptacles displaced in height for cards to overlap on one side of circuit board
US6976623B1 *	2002-11-18	2005-12-20	Onspec Electronic, Inc.	Flash juke box
TWM243737U *	2002-11-28	2004-09-11	Carry Computer Eng Co Ltd	Card adapter
JP3742384B2 *	2002-12-25	2006-02-01	株式会社東芝	Electronics
JP4019965B2 *	2003-02-10	2007-12-12	ソニー株式会社	IC card adapter device
JP4046659B2 *	2003-07-31	2008-02-13	日本圧着端子製造株式会社	Memory card connector
US8484671B1	2003-10-07	2013-07-09	The Directv Group, Inc.	Receiver interface with multiple access cards
US6999738B2 *	2003-12-24	2006-02-14	Michael Arnouse	Dual-sided smart card reader
JP2006023962A *	2004-07-07	2006-01-26	Fujitsu Ltd	Non-contact ic tag system
US7441701B2 *	2004-07-29	2008-10-28	Zih Corp.	Universal card reader apparatus and method
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
US20060226217A1 *	2005-04-07	2006-10-12	Tyfone, Inc.	Sleeve for electronic transaction card
US7252231B2 *	2005-06-03	2007-08-07	Wieson Technologies Co., Ltd.	Card adapter
DE102006019630A1 *	2006-04-25	2007-10-31	Lumberg Connect Gmbh	Smart cards e.g. subscriber identity module card and memory card, contact device for e.g. mobile telephone, has contact groups that are consecutively arranged on common carrier, and have height offset corresponding to thickness of cards
US7991158B2 *	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
US20080244208A1 *	2007-03-30	2008-10-02	Narendra Siva G	Memory card hidden command protocol
US9741027B2 *	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US20100059593A1 *	2008-09-10	2010-03-11	Defranco Dominic	Stored value card jacket and counter
EP2401708A4 *	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
US9183420B1 *	2014-06-20	2015-11-10	Nokia Technologies Oy	Reader for electronic cards

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
JPH1097599A	1998-04-14	Portable terminal equipment for ic card
JP3682757B2	2005-08-10	Data card housing
US6102743A	2000-08-15	Data card connector
JP3935975B2	2007-06-27	Multiple application portable cards for personal computers
US6454164B1	2002-09-24	Pocket-size information transfer apparatus having dual IC card insertion slots and IC card using the same
US6029892A	2000-02-29	Method for electronically transferring personal information on credit gaining card, and mini IC card, adapter card, terminal adapter, slip issuing device, portable terminal used therein
US7742009B2	2010-06-22	Antenna for the plug-in dual-interface smart card
JP2002117922A	2002-04-19	Card connector
WO2000052666A3	2000-12-21	Portable electronic charge and authorization devices and methods therefor
CN100378743C	2008-04-02	Access device for data-holding body and electronic equipment incorporating the access device
CN106133757B	2019-05-28	Card reader
JP4530318B2	2010-08-25	Plug-in type IC card adapter
KR20120065287A	2012-06-20	Cellular phone battery cover
JP2005149355A	2005-06-09	Uim adapter
WO2002103923A1	2002-12-27	Portable telephone having smartcard which non-contact interface is transferred into break contact point
JP2002032715A	2002-01-31	Memory card loading device, electronic equipment equipped with memory card loading device, and memory card adapter device
CN207440818U	2018-06-01	A kind of intelligent student card with call function
JP3776310B2	2006-05-17	IC card
JP3807719B2	2006-08-09	IC card
JP2006157801A	2006-06-15	Portable terminal
JP3932178B2	2007-06-20	Information terminal
CN207020781U	2018-02-16	Pos
JP3819153B2	2006-09-06	IC card data display device
WO1997010566A1	1997-03-20	Smartcard to pc communication through pcmcia interface
JP4703137B2	2011-06-15	Charging stand for portable information terminals

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
JP8251183A	1996-09-24	1996-09-24	Portable terminal equipment for ic card

Applications Claiming Priority (8)

Application	Filing date	Title
JP8251183A	1996-09-24	Portable terminal equipment for ic card
CA002213042A	1997-08-14	A portable terminal device for electronic money ic cards
US08/921,612	1997-09-02	Portable terminal device with stackable IC cards slot opening
AU38376/97A	1997-09-22	A portable terminal device for electronic money IC cards
DE69731860T	1997-09-23	Portable terminal device for an electronic money card
EP0731445A	1997-09-23	A portable terminal device for electronic money IC cards

CN97119690 7A	1997-09-24	Portable terminal installation for electronic currency integrated circuit card
US09/475,027	1999-12-30	Portable terminal device with stackable IC card slot opening

Legal Events

Date	Code	Title	Description
2004-06-30	A02	Decision of refusal	**Free format text**: JAPANESE INTERMEDIATE CODE: A02 **Effective date**: 20040629
2004-08-30	A521	Written amendment	**Free format text**: JAPANESE INTERMEDIATE CODE: A523 **Effective date**: 20040827
2004-09-02	A911	Transfer of reconsideration by examiner before appeal (zenchi)	**Free format text**: JAPANESE INTERMEDIATE CODE: A911 **Effective date**: 20040901
2004-09-27	A912	Removal of reconsideration by examiner before appeal (zenchi)	**Free format text**: JAPANESE INTERMEDIATE CODE: A912 **Effective date**: 20040924

Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

CONTACTLESS OR CONTACT-FREE HYBRID CHIP CARD TO REDUCE THE RISK OF FRAUD

Classifications

G06K19/07 Record carriers with conductive marks, printed circuits or semiconductor circuit elements, e.g. credit or identity cards also with resonating or responding marks without active components with integrated circuit chips

View 8 more classifications

FR2801709B1

France

Find Prior Art Similar

Other languages: French

Inventor: Georges Kayanakis

Current Assignee : ASK SA

Worldwide applications

1999 FR 2000 AU AT BE CH DE ES FI GB GR IE IT LI LU MC NL PT SE TR AT BR CA EP JP US WO AU ID TR AT BR CA US 2001 TW NO ZA 2002 HK

Application FR9915020A events

1999-11-29	Application filed by ASK SA
1999-11-29	Priority to FR9915020A
2001-06-01	Publication of FR2801709A1
2002-02-15	Application granted
2002-02-15	Publication of FR2801709B1
2019-11-29	Anticipated expiration
Status	Expired - Fee Related

Info: Patent citations (28), Cited by (119), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Patent Citations (28)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
FR615285A		1927-01-04		
FR2581480A1	1985-04-10	1986-11-07	Ebauches Electroniques Sa	ELECTRONIC UNIT, IN PARTICULAR FOR A MICROCIRCUIT BOARD AND CARD COMPRISING SUCH A UNIT
EP0211360B1 *	1985-07-27	1993-09-29	Dai Nippon Insatsu Kabushiki Kaisha	Ic card
FI94562C *	1992-11-09	1995-09-25	Tapio Robertsson	Roller identification device and method for its manufacture
ZA941671B	1993-03-11	1994-10-12	Csir	Attaching an electronic circuit to a substrate.
US5495250A	1993-11-01	1996-02-27	Motorola, Inc.	Battery-powered RF tags and apparatus for manufacturing the same
DE4409013C1 *	1994-02-01	1995-06-29	Knorr Bremse Systeme	Arrangement for suspending and supporting block brake units for rail vehicles
DE9422424U1 *	1994-02-04	2002-02-21	Giesecke & Devrient Gmbh	Chip card with an electronic module
FR2716281B1 *	1994-02-14	1996-05-03	Gemplus Card Int	Method of manufacturing a contactless card.
DE19601358C2 *	1995-01-20	2000-01-27	Fraunhofer Ges Forschung	Integrated circuit paper
DE19607212C1	1996-02-26	1997-04-10	Richard Herbst	Prodn. of smart cards and data cards as composite injection moulding
IT240061Y1 *	1996-03-01	2001-03-26	Cruciani Andrea	ADAPTER

JPH10129165A *	1996-03-15	1998-05-19	Hitachi Maxell Ltd	Information carrier and its manufacture
US6223989B1 *	1996-08-05	2001-05-01	Gemplus S.C.A.	Method for making smart cards, and resulting cards
US5898215A	1996-12-16	1999-04-27	Motorola, Inc.	Microelectronic assembly with connection to a buried electrical element, and method for forming same
US5988510A	1997-02-13	1999-11-23	Micron Communications, Inc.	Tamper resistant smart card and method of protecting data in a smart card
DE19710144C2	1997-03-13	1999-10-14	Orga Kartensysteme Gmbh	Method for producing a chip card and chip card produced according to the method
JPH10258596A *	1997-03-19	1998-09-29	Toppan Printing Co Ltd	Card containing precious metal and its manufacture
US5955021A	1997-05-19	1999-09-21	Cardxx, Llc	Method of making smart cards
US6025054A	1997-09-08	2000-02-15	Cardxx, Inc.	Smart cards having glue-positioned electronic components
FR2769440B1	1997-10-03	1999-12-03	Gemplus Card Int	METHOD FOR MANUFACTURING AN ELECTRONIC CHIP AND / OR ANTENNA DEVICE AND DEVICE OBTAINED BY THE METHOD
FR2769390B1 *	1997-10-08	2003-02-14	Gemplus Card Int	METHOD FOR MANUFACTURING CHIP CARDS SUITABLE FOR PROVIDING CONTACT AND NON-CONTACT OPERATION, AND CONTACTLESS CHIP CARDS
FR2775533B1 *	1998-02-27	2003-02-14	Gemplus Sca	ELECTRONIC DEVICE WITH NON-CONTACT ELECTRONIC MEMORY, AND METHOD FOR MANUFACTURING SUCH A DEVICE
FR2778478B1	1998-05-11	2001-11-23	Schlumberger Systems & Service	NON-CONTACT TYPE MEMORY CARD, AND METHOD FOR MANUFACTURING SUCH A CARD
US6161761A *	1998-07-09	2000-12-19	Motorola, Inc.	Card assembly having a loop antenna formed of a bare conductor and method for manufacturing the card assembly
JP2000113155A *	1998-09-30	2000-04-21	Oji Paper Co Ltd	Ic card
JP2000113151A *	1998-10-01	2000-04-21	Tomoegawa Paper Co Ltd	Label-type ic card
JP2000155821A *	1998-11-19	2000-06-06	Dainippon Printing Co Ltd	Non-contact ic card and manufacture of the same

* Cited by examiner, † Cited by third party

Cited By (119)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US7827106B2	2001-07-10	2010-11-02	American Express Travel Related Services Company, Inc.	System and method for manufacturing a punch-out RFID transaction device
US7172112B2	2000-01-21	2007-02-06	American Express Travel Related Services Company, Inc.	Public/private dual card system and method
FR2805066B1 *	2000-02-15	2003-09-12	Bourgogne Grasset	ELECTRONIC CHIP TOKEN AND METHODS OF MANUFACTURING SUCH A TOKEN
WO2001067355A2	2000-03-07	2001-09-13	American Express Travel Related Services Company, Inc.	System for facilitating a transaction
US7725427B2	2001-05-25	2010-05-25	Fred Bishop	Recurrent billing maintenance with radio frequency payment devices
US7650314B1	2001-05-25	2010-01-19	American Express Travel Related Services Company, Inc.	System and method for securing a recurrent billing transaction
US6923378B2 *	2000-12-22	2005-08-02	Digimarc Id Systems	Identification card
DE10117994A1 *	2001-04-10	2002-10-24	Orga Kartensysteme Gmbh	Carrier foil for electronic components to be laminated into smart cards, includes inter-joined part surfaces of connection zones made of conductive material
US6842148B2	2001-04-16	2005-01-11	Skycross, Inc.	Fabrication method and apparatus for antenna structures in wireless communications devices

FR2826154B1 *	2001-06-14	2004-07-23	A S K	CHIP CARD WITHOUT CONTACT WITH AN ANTENNA SUPPORT AND CHIP SUPPORT OF FIBROUS MATERIAL
EP1411465B1 *	2001-06-19	2008-08-06	Nippon Carbide Kogyo Kabushiki Kaisha	Retroreflective product in which integrated circuit is sealed
US8996535B2	2001-07-10	2015-02-24	Iii Holdings 1, Llc	Method and system for resource management and evaluation
US8538863B1	2001-07-10	2013-09-17	American Express Travel Related Services Company, Inc.	System and method for facilitating a transaction using a revolving use account associated with a primary account
US7762457B2	2001-07-10	2010-07-27	American Express Travel Related Services Company, Inc.	System and method for dynamic fob synchronization and personalization
US7360689B2	2001-07-10	2008-04-22	American Express Travel Related Services Company, Inc.	Method and system for proffering multiple biometrics for use with a FOB
US9024719B1	2001-07-10	2015-05-05	Xatra Fund Mx, Llc	RF transaction system and method for storing user personal data
US7889052B2	2001-07-10	2011-02-15	Xatra Fund Mx, Llc	Authorizing payment subsequent to RF transactions
US7303120B2	2001-07-10	2007-12-04	American Express Travel Related Services Company, Inc.	System for biometric security using a FOB
US7668750B2	2001-07-10	2010-02-23	David S Bonalle	Securing RF transactions using a transactions counter
US7111969B2	2001-07-10	2006-10-10	American Express Travel Related Services Company, Inc.	Systems and methods for providing a RF transaction device for use in a private label transaction
US7493288B2	2001-07-10	2009-02-17	Xatra Fund Mx, Llc	RF payment via a mobile device
US7705732B2	2001-07-10	2010-04-27	Fred Bishop	Authenticating an RF transaction using a transaction counter
US8284025B2	2001-07-10	2012-10-09	Xatra Fund Mx, Llc	Method and system for auditory recognition biometrics on a FOB
US7925535B2	2001-07-10	2011-04-12	American Express Travel Related Services Company, Inc.	System and method for securing RF transactions using a radio frequency identification device including a random number generator
US7996324B2	2001-07-10	2011-08-09	American Express Travel Related Services Company, Inc.	Systems and methods for managing multiple accounts on a RF transaction device using secondary identification indicia
US20040236699A1	2001-07-10	2004-11-25	American Express Travel Related Services Company, Inc.	Method and system for hand geometry recognition biometrics on a fob
US8001054B1	2001-07-10	2011-08-16	American Express Travel Related Services Company, Inc.	System and method for generating an unpredictable number using a seeded algorithm
US7503480B2	2001-07-10	2009-03-17	American Express Travel Related Services Company, Inc.	Method and system for tracking user performance
US9454752B2	2001-07-10	2016-09-27	Chartoleaux Kg Limited Liability Company	Reload protocol at a transaction processing entity
US8635131B1	2001-07-10	2014-01-21	American Express Travel Related Services Company, Inc.	System and method for managing a transaction protocol
US7746215B1	2001-07-10	2010-06-29	Fred Bishop	RF transactions using a wireless reader grid
US8548927B2	2001-07-10	2013-10-01	Xatra Fund Mx, Llc	Biometric registration for facilitating an RF transaction
US7239226B2	2001-07-10	2007-07-03	American Express Travel Related	System and method for payment using radio frequency identification in contact and contactless transactions

			Services Company, Inc.	
US7249112B2	2002-07-09	2007-07-24	American Express Travel Related Services Company, Inc.	System and method for assigning a funding source for a radio frequency identification device
US8294552B2	2001-07-10	2012-10-23	Xatra Fund Mx, Llc	Facial scan biometrics on a payment device
US7805378B2	2001-07-10	2010-09-28	American Express Travel Related Services Company, Inc.	System and method for encoding information in magnetic stripe format for use in radio frequency identification transactions
US9031880B2	2001-07-10	2015-05-12	Iii Holdings 1, Llc	Systems and methods for non-traditional payment using biometric data
FR2829857B1 *	2001-09-14	2004-09-17	A S K	CONTACTLESS OR HYBRID CONTACT-CONTACTLESS CHIP CARD WITH REINFORCED HOLDING OF THE ELECTRONIC MODULE
US6701605B2 *	2001-10-09	2004-03-09	Sonoco Development, Inc.	Conductive electrical element and antenna with ink additive technology
US6604681B1 *	2001-10-09	2003-08-12	Vahid Taban	High speed system for embedding wire antennas in an array of smart cards
AU2002350102A1 *	2001-11-02	2003-05-19	Skycross, Inc.	Dual band spiral-shaped antenna
US6817530B2	2001-12-18	2004-11-16	Digimarc Id Systems	Multiple image security features for identification documents and methods of making same
US7712673B2	2002-12-18	2010-05-11	L-L Secure Credentialing, Inc.	Identification document with three dimensional image of bearer
CA2652104C *	2001-12-24	2012-02-14	Digimarc Id Systems, Llc	Contact smart cards having a document core, contactless smart cards including multi-layered structure, pet-based identification document, and methods of making same
US7694887B2	2001-12-24	2010-04-13	L-1 Secure Credentialing, Inc.	Optically variable personalized indicia for identification documents
WO2003056500A1	2001-12-24	2003-07-10	Digimarc Id Systems, Llc	Covert variable information on id documents and methods of making same
CA2470547C	2001-12-24	2008-05-20	Digimarc Id Systems, Llc	Laser etched security features for identification documents and methods of making same
US7793846B2	2001-12-24	2010-09-14	L-1 Secure Credentialing, Inc.	Systems, compositions, and methods for full color laser engraving of ID documents
US7728048B2	2002-12-20	2010-06-01	L-1 Secure Credentialing, Inc.	Increasing thermal conductivity of host polymer used with laser engraving methods and compositions
WO2003088144A2	2002-04-09	2003-10-23	Digimarc Id Systems, Llc	Image processing techniques for printing identification cards and documents
US6885617B2 *	2002-04-19	2005-02-08	Avery Dennison Corporation	Laser imageable RFID label/tag
US7824029B2	2002-05-10	2010-11-02	L-1 Secure Credentialing, Inc.	Identification card printer-assembler for over the counter card issuing
US8543423B2	2002-07-16	2013-09-24	American Express Travel Related Services Company, Inc.	Method and apparatus for enrolling with multiple transaction environments
DE10232568A1 *	2002-07-18	2004-01-29	Agfa-Gevaert Ag	Identity card
JP4039158B2 *	2002-07-22	2008-01-30	ソニー株式会社	Information processing apparatus and method, information processing system, recording medium, and program
US6805287B2	2002-09-12	2004-10-19	American Express Travel Related Services Company, Inc.	System and method for converting a stored value card to a credit card
FR2844621A1 *	2002-09-13	2004-03-19	A S K	Method for manufacturing without contact or hybrid integrated circuit card, comprises application of two thermoplastic layers under temperature and pressure followed by two hot pressed plastic layers
FI20022094A0 *	2002-11-25	2002-11-25	Rafsec Oy	Transponder and method for its manufacture
US7804982B2	2002-11-26	2010-09-28	L-1 Secure Credentialing, Inc.	Systems and methods for managing and detecting fraud in image databases used with identification documents
FR2853115B1 *	2003-03-28	2005-05-06	A S K	METHOD FOR MANUFACTURING A CHIP CARD ANTENNA ON A THERMOPLASTIC CARRIER AND A CHIP CARD OBTAINED BY SAID METHOD

US7225991B2	2003-04-16	2007-06-05	Digimarc Corporation	Three dimensional data storage
US8429041B2	2003-05-09	2013-04-23	American Express Travel Related Services Company, Inc.	Systems and methods for managing account information lifecycles
US7336243B2 *	2003-05-29	2008-02-26	Sky Cross, Inc.	Radio frequency identification tag
US7347382B2 *	2004-02-06	2008-03-25	T-Ink, Llc	System for securing personal cards
US20050194454A1 *	2004-02-06	2005-09-08	T-Ink, Llc	Personal card system featuring integrated circuit
DE102004011702B4	2004-03-10	2006-02-16	Circle Smart Card Ag	Method for producing a card body for a contactless chip card
US7744002B2	2004-03-11	2010-06-29	L-1 Secure Credentialing, Inc.	Tamper evident adhesive and identification document including same
US7113135B2 *	2004-06-08	2006-09-26	Skycross, Inc.	Tri-band antenna for digital multimedia broadcast (DMB) applications
US7318550B2	2004-07-01	2008-01-15	American Express Travel Related Services Company, Inc.	Biometric safeguard method for use with a smartcard
EP1768052B1 *	2004-07-01	2010-12-01	Lintec Corporation	Antenna circuit, ic inlet, and ic tag
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
US20060284770A1 *	2005-06-15	2006-12-21	Young-Min Jo	Compact dual band antenna having common elements and common feed
FR2890212B1 *	2005-08-30	2009-08-21	Smart Packaging Solutions Sps	ELECTRONIC MODULE WITH A DOUBLE COMMUNICATION INTERFACE, IN PARTICULAR FOR A CHIP CARD
US7222427B2 *	2005-10-18	2007-05-29	Avery Dennison Corporation	Label with electronic components and method of making same
US7375975B1 *	2005-10-31	2008-05-20	Amkor Technology, Inc.	Enhanced durability memory card
CN100561506C *	2005-12-19	2009-11-18	清华大学	Non-contact paper base electronic passenger ticket based on electronic label technology
US8232621B2 *	2006-07-28	2012-07-31	Semiconductor Energy Laboratory Co., Ltd.	Semiconductor device
DE102006052517A1 *	2006-11-06	2008-05-08	Bielomatik Leuze Gmbh + Co.Kg	Chip module for an RFID system
US7701352B2 *	2006-11-22	2010-04-20	Avery Dennison Corporation	RFID label with release liner window, and method of making
US7991158B2 *	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
WO2008103870A1	2007-02-23	2008-08-28	Newpage Wisconsin System Inc.	Multifunctional paper identification label
US9367712B1	2007-03-01	2016-06-14	Amkor Technology, Inc.	High density memory card using folded flex
US20080244208A1 *	2007-03-30	2008-10-02	Narendra Siva G	Memory card hidden command protocol
EP2014463B1	2007-06-22	2015-07-29	Agfa-Gevaert N.V	Smart information carrier and production process therefor.
WO2009038511A1 *	2007-09-21	2009-03-26	Telefonaktiebolaget Lm Ericsson (Publ)	All in one card
FR2922342B1 *	2007-10-11	2010-07-30	Ask Sa	REINFORCED RADIOFREQUENCY IDENTIFICATION DEVICE SUPPORT AND METHOD OF MANUFACTURING THE SAME
US9741027B2 *	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US20090160617A1 *	2007-12-24	2009-06-25	Dynamics Inc.	Credit, security, debit cards and the like with buttons
US20090184168A1 *	2008-01-17	2009-07-23	Roger Ricketts	Recyclable plastic cards and methods of making same
US20090216665A1 *	2008-02-21	2009-08-27	The Coca-Cola Company	Systems and Methods for Providing Vending Network Data Management
US8645273B2 *	2008-02-21	2014-02-04	The Coca-Cola Company	Systems and methods for providing a vending network
US20090216675A1 *	2008-02-21	2009-08-27	The Coca-Cola	Commission Centric Network Operation Systems and Methods

			Company	
US9460440B2 *	2008-02-21	2016-10-04	The Coca-Cola Company	Systems and methods for providing electronic transaction auditing and accountability
US20090222309A1 *	2008-03-03	2009-09-03	The Coca-Cola Company	Systems and Methods of Marketing to Defined Consumer Groups
US20090222339A1 *	2008-03-03	2009-09-03	The Coca-Cola Company	Systems and Methods for Providing a Personal Terminal for a Loyalty Program
US8121917B2	2008-03-03	2012-02-21	The Coca-Cola Company	Systems for implementing a loyalty program
US8015588B2 *	2008-03-03	2011-09-06	The Coca-Cola Company	Methods for implementing a loyalty program
US20100033310A1 *	2008-08-08	2010-02-11	Narendra Siva G	Power negotation for small rfid card
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
EP2401708A4 *	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
US8245959B1	2009-06-30	2012-08-21	Emc Corporation	Powered card and method of disposing of the same
US20110084148A1 *	2009-10-14	2011-04-14	Ricketts Roger H	Plastic cards made from post-consumer plastic
DE102009058435A1 *	2009-12-16	2011-06-22	Giesecke & Devrient GmbH, 81677	Attaching and electrically connecting a chip module to a chip card
US8789762B2	2010-08-12	2014-07-29	Feinics Amatech Teoranta	RFID antenna modules and methods of making
DE102010034156A1 *	2010-08-11	2012-02-16	Ovd Kinegram Ag	film element
US8899712B2	2010-08-12	2014-12-02	Feinics Amatech Teoranta	Coupling in and to RFID smart cards
FR2968432B1 *	2010-12-06	2012-12-28	Oberthur Technologies	METHOD FOR INPUTTING A MODULE IN A MICROCIRCUIT CARD
ES1074970Y *	2011-04-28	2011-10-05	Prepaytrans Gestion Empresarial S L	CREDIT CARD
US20130311382A1 *	2012-05-21	2013-11-21	Klaus S. Fosmark	Obtaining information for a payment transaction
US8763912B1 *	2013-03-29	2014-07-01	Identive Group, Inc.	Dual interface module and dual interface card having a dual interface module
DE102013005486B4 *	2013-04-02	2019-02-14	Heraeus Deutschland GmbH & Co. KG	Layer structure with conductive polymer for tamper detection as well as method for its production
EP2843605A1 *	2013-08-30	2015-03-04	Gemalto SA	Method for authenticating transactions
EP3249634A1 *	2016-05-26	2017-11-29	Nxp B.V.	Tamper detection device
RU2639577C1	2016-10-13	2017-12-21	Акционерное общество "Пэй Ринг"	Non-contact smart-card
RU2671303C1 *	2017-08-29	2018-10-30	Эдуард Геннадьевич Новаковский	Non-contact identification smart-card with the possibility of using particular fragments as active self-identified identifiers with a unique code (variants)
RU2735275C2 *	2018-06-06	2020-10-29	Акционерное общество "Пэй Ринг"	Noncontact smart card
RU183111U1 *	2018-06-06	2018-09-11	Акционерное общество "Пэй Ринг"	Contactless smart card
FR3083892B1 *	2018-07-16	2020-07-03	Smart Packaging Solutions	DUAL COMMUNICATION INTERFACE CHIP CARD AND MANUFACTURING METHOD THEREOF

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
FR2801709B1	2002-02-15	CONTACTLESS OR CONTACT-FREE HYBRID CHIP CARD TO REDUCE THE RISK OF FRAUD

FR2844620B1	2005-01-07	METHOD FOR MANUFACTURING CONTACTLESS CONTACTLESS CONTACT OR CONTACT HYBRID CARD WITH REINFORCED PLANE
AU3310900A	2000-10-09	Contactless smart card reader
DE69933963D1	2006-12-28	IC card with contact and contactless interfaces
FR2829857B1	2004-09-17	CONTACTLESS OR HYBRID CONTACT-CONTACTLESS CHIP CARD WITH REINFORCED HOLDING OF THE ELECTRONIC MODULE
DE69801926D1	2001-11-08	CONTACT CHIP CARD / CONTACTLESS CHIP CARD WITH VARIABLE ANTENNA INTERFACE
DE50004245D1	2003-12-04	CONTACTLESS CHIP CARD
DZ3215A1	2001-03-15	TRANSACTION CARD
NO20020015L	2002-02-27	Smart card reader
FR2768880B1	2000-05-05	DEMODULATOR FOR CONTACTLESS CHIP CARD
AT349784T	2007-01-15	SMART CARD READER
DE60045859D1	2011-06-01	smart card
FR2783069B1	2003-01-24	CHIP CARD READER
DE50005764D1	2004-04-29	Smart card reader
FR2859559B1	2005-12-09	CONTACTLESS CARD READER
FR2781587B1	2000-09-08	ADVANCED READER FOR NON-CONTACT BADGES
FR2668764B1	1993-11-12	CONTACTLESS CARD.
FR2784210B1	2001-09-14	CONTACTLESS CHIP CARD WITH MEANS OF INHIBITION
FR2782821B1	2001-10-12	NON-CONTACT CHIP CARD MANUFACTURING PROCESS
FR2787609B1	2001-02-09	NON-CONTACT CHIP CARD MANUFACTURING PROCESS
DE60042506D1	2009-08-20	Smart card reader
FR2789786B1	2001-04-27	PAYMENT TERMINAL ACCEPTING CONTACTLESS CARD PAYMENTS
FR2735929B1	1997-09-05	PASSIVE CONTACTLESS CARD
FR2863084B1	2011-04-08	MODULE FOR CHIP CARDS OR CONTACTLESS IDENTIFICATION SYSTEMS
AT295581T	2005-05-15	SMART CARD

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
FR9915020A	1999-11-29	1999-11-29	CONTACTLESS OR CONTACT-FREE HYBRID CHIP CARD TO REDUCE THE RISK OF FRAUD

Applications Claiming Priority (21)

Application	Filing date	Title
FR9915020A	1999-11-29	CONTACTLESS OR CONTACT-FREE HYBRID CHIP CARD TO REDUCE THE RISK OF FRAUD
EP00985346A	2000-11-28	Non-contact or non-contact hybrid smart card for limiting risks of fraud
JP2001542044A	2000-11-28	Contactless or contactless hybrid smart card that limits the risk of fraud
IL14430200A	2000-11-28	Non-contact or non-contact hybrid smart card for limiting risks of fraud
KR1020017009242A	2000-11-28	Non-contact or non-contact hybrid smart card for limiting risks of fraud
PCT/FR2000/003323	2000-11-28	Non-contact or non-contact hybrid smart card for limiting risks of fraud
AT00985346T	2000-11-28	CONTACTLESS CHIP CARD OR CONTACT / CONTACTLESS HYBRID CHIP CARD WITH FRAUD PREVENTION
TR2001/02181T	2000-11-28	Contactless or contactless hybrid smart card to limit the risk of fraud
CA002360359A	2000-11-28	Non-contact or non-contact hybrid smart card for limiting risks of fraud

CNB008031940A	2000-11-28	Non-contact or non-contact hybrid smart card for limiting risk of fraud
DE60034805T	2000-11-28	Contactless chip card or contact / contactless hybrid chip card with fraud prevention
BRPI0007791-7A	2000-11-28	chip card, contactless or hybrid contactless - contactless.
IDW002001016474A	2000-11-28	NO-CONTACT SMART CARDS OR HYDRAULIC CONTACT-NO SMART CARD TO LIMIT RISK RISK
AU21795/01A	2000-11-28	Non-contact or non-contact hybrid smart card for limiting risks of fraud
PT00985846T	2000-11-28	Non-contact or non-contact hybrid smart card for limiting risks of fraud
RU2001123934/09A	2000-11-28	Non-contact or combined contact-non-contact chip-card
US09/725,078	2000-11-29	Contactless or hybrid contact-contactless smart card designed to limit the risks of fraud
TW090111463A	2001-05-14	Contactless or hybrid contact-contactless smart card designed to limit the risks of fraud
NO20013403A	2001-07-09	Contact-free or hybrid contact-free smart card for limiting the risk of fraud
ZA200105717A	2001-07-12	Non-contact or non-contact hybrid smart card for limiting risks of fraud.
HK02106020.9A	2002-08-19	Non-contact or non-contact hybrid smart card for limiting risks of fraud

Legal Events

Date	Code	Title	Description
2008-04-04	GC	Lien (pledge) constituted	
2009-09-11	ST	Notification of lapse	**Effective date**: 20090731
2011-05-13	GC	Lien (pledge) constituted	
2011-09-30	GC	Lien (pledge) constituted	**Effective date**: 20110608
2014-09-26	RG	Lien (pledge) cancelled	**Effective date**: 20140825
2016-01-15	GC	Lien (pledge) constituted	**Effective date**: 20151210

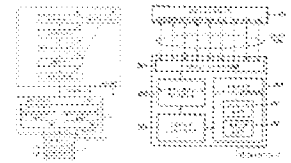
Data provided by IFI CLAIMS Patent Services

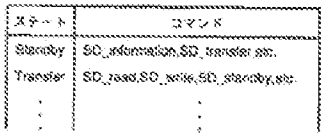
About Send Feedback Public Datasets Terms Privacy Policy

Patents JP3641230

Apparatus and method for controlling a memory card

Images (11)





Classifications

G07F7/1008 Active credit-cards provided with means to personalise their use, e.g. with PIN-introduction/comparison system

View 3 more classifications

JP3641230B2
Japan

Download PDF Find Prior Art Similar

Other languages: Japanese

Inventor: 雅俊 村上

Worldwide applications

2001 JP 2002 EP US

Application JP2001323956A events

2001-10-22 Application filed by 株式会社東芝
2001-10-22 Priority to JP2001323956A
2003-05-09 Publication of JP2003132305A
2005-04-20 Application granted
2005-04-20 Publication of JP3641230B2
2021-10-22 Anticipated expiration
Status Expired - Fee Related

Info: Patent citations (16), Cited by (74), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (12)

Hide Dependent

1. In a memory card control device that controls a memory card that operates in any of a plurality of states with different types of operation commands that can be accepted,
An operation command which is issued by the host system for accessing the memory card and directly specifies an operation to be executed by the memory card, and an execution which indicates the state of the memory card to which an operation corresponding to the operation command is to be executed. Means for receiving a direct command including state information;
In accordance with the received direct command, a process for causing the memory card to transition from a specific state predetermined as a steady state to a state specified by execution state information included in the received direct command, to the received direct command Direct command execution means for sequentially executing a process for issuing the operation command included in the memory card to cause the memory card to execute an operation corresponding to the operation command, and a process for returning the memory card to the specific state. A memory card control device.

2. The plurality of states include a first state and a second state, and the specific state predetermined as the steady state is the first state,
The execution state information includes flag information indicating whether or not the memory card needs to transition to the second state,
The direct command execution means includes
When the flag information indicates that it is necessary to make a transition to the second state, a process for making the memory card transition from the first state, which is the specific state, to the second state, included in the direct command Means for sequentially executing a process of issuing the operation command to the memory card and causing the memory card to execute an operation corresponding to the operation command, and a process of returning the memory card to the first state;
When the flag information indicates that it is not necessary to transition to the second state, the operation command included in the direct command is issued to the memory card and the operation corresponding to the operation command is executed on the memory card. The memory card control device according to claim 1, further comprising;

3. The specific state predetermined as the steady state is a state in which the memory card can accept an operation command related to data writing to or reading from the nonvolatile memory built in the memory card. The memory card control device according to claim 1, wherein

4. The memory card is provided with a secure area that is a data storage area accessible only by a dedicated program having a content protection function,
2. The memory card control according to claim 1, wherein an access command issued for accessing the secure area by a dedicated program having the content protection function executed on the host system is the direct command. apparatus.

5. The memory card is provided with a user data area which is a data storage area accessible by an operating system executed on the host system,
When a storage access command for requesting data write to the user data area or data read from the user data area is received from the host system, the storage access command is interpreted and executed, and specified by the storage access command. Processing for returning one or more operation commands

necessary for causing the memory card to execute an operation corresponding to the requested request to the memory card, and then returning the memory card to the specific state predetermined as the steady state 2. The memory card control device according to claim 1, further comprising storage access command execution means for executing.

6. In a memory card control device that controls a memory card that operates in any of a plurality of states with different types of operation commands that can be accepted in accordance with an access command from a host system,
The memory card can be accessed only by a user data area which is a data storage area accessible by an operating system executed on the host system and a dedicated program having a content protection function executed on the host system. Secure area, which is a secure data storage area,
The access command from the host system indicates an operation command that directly specifies an operation related to access to the secure area to be executed by the memory card and a state of the memory card that is to execute an operation corresponding to the operation command. Means for determining whether it is a direct command including execution state information and a storage access command for requesting data writing to the user data area or data reading from the user data area;
When the access command is the direct command, a process of transitioning the memory card to a state specified by the execution state information included in the direct command, and issuing the operation command included in the direct command to the memory card Direct command execution means for sequentially executing a process for causing the memory card to execute an operation corresponding to the operation command, and a process for returning the memory card to a specific state determined in advance as its steady state;
When the access command is the storage access command, one or more operations necessary for interpreting and executing the storage access command and causing the memory card to perform an operation corresponding to the request specified by the storage access command A memory card control device comprising storage access command execution means for executing processing for returning the memory card to the specific state predetermined as the steady state after issuing a command to the memory card .

7. The plurality of states include a first state and a second state, and the specific state predetermined as the steady state is the first state,
The execution state information includes flag information indicating whether or not the memory card needs to transition to the second state,
The direct command execution means includes
When the flag information indicates that it is necessary to make a transition to the second state, a process for making the memory card transition from the first state, which is the specific state, to the second state, included in the direct command Means for sequentially executing a process of issuing the operation command to the memory card and causing the memory card to execute an operation corresponding to the operation command, and a process of returning the memory card to the first state,
When the flag information indicates that it is not necessary to transition to the second state, the operation command included in the direct command is issued to the memory card and the operation corresponding to the operation command is executed on the memory card. The memory card control device according to claim 6, further comprising:

8. The specific state predetermined as the steady state is a state in which the memory card can accept an operation command related to data writing to the user data area or data reading from the user data area. The memory card control device according to claim 6.

9. The access command issued by the operating system for accessing the user data area is the storage access command, and the access command issued by the dedicated program having the content protection function for accessing the secure area is the 7. The memory card control device according to claim 6, wherein the memory card control device is a direct command

10. In a data processing device capable of controlling a memory card that operates in any of a plurality of states with different types of operation commands that can be accepted,
The memory card has only a user data area, which is a data storage area accessible by an operating system executed on the data processing device, and a dedicated program having a content protection function executed on the data processing device. A secure area, which is an accessible data storage area, is provided.
The access commands issued from the operating system or the dedicated program having the content protection function are sequentially received, and the access commands directly perform operations related to access to the secure area to be executed by the memory card in the order of reception. A direct command including an operation command to be specified and execution state information indicating the state of the memory card on which an operation corresponding to the operation command is to be executed, and data writing to the user data area or data reading from the user data area A storage access command that requests
When the access command is the direct command, a process of transitioning the memory card to a state specified by the execution state information, and issuing the operation command included in the direct command to the memory card Direct command execution means for sequentially executing processing for causing the memory card to execute a corresponding operation, and processing for returning the memory card to a predetermined state as a steady state.
When the access command is the storage access command, one or more operations necessary for interpreting and executing the storage access command and causing the memory card to perform an operation corresponding to the request specified by the storage access command A data processing apparatus comprising storage access command execution means for executing processing for returning the memory card to the specific state predetermined as the steady state after issuing a command to the memory card.

11. In a memory card control method for controlling a memory card that operates in any of a plurality of states with different types of operation commands that can be accepted,
Receiving an access command issued by the host system for accessing the memory card,
The received access command is a direct command including an operation command that directly designates an operation to be executed by the memory card and execution state information that indicates a state of the memory card to execute an operation corresponding to the operation command. If there is, a process of transitioning the memory card from a specific state predetermined as its steady state to a state specified by the execution state information included in the received direct command, the operation included in the received direct command A memory card control characterized by sequentially executing a process for issuing a command to the memory card and causing the memory card to execute an operation corresponding to the operation command, and a process for returning the memory card to the specific state. Method.

12. In a memory card control method for controlling a memory card that operates in any of a plurality of states having different types of operation commands that can be accepted in accordance with an access command from a host system,
The memory card can be accessed only by a user data area which is a data storage area accessible by an operating system executed on the host system and a dedicated program having a content protection function executed on the host system. Secure area, which is a secure data storage area,
The access command from the host system indicates an operation command that directly specifies an operation related to access to the secure area to be executed by the memory card and a state of the memory card that is to execute an operation corresponding to the operation command. Determining whether it is a direct command including execution state information and a storage access command for requesting data writing to the user data area or data reading from the user data area,
When the access command is the direct command, a process of transitioning the memory card to a state specified by the execution state information included in the direct command, and issuing the operation command included in the direct command to the memory card A process for causing the memory card to execute an operation corresponding to the operation command, and a process for returning the memory card to a specific state determined in advance as a steady state,
When the access command is the storage access command, one or more operations necessary for interpreting and executing the storage access command and causing

the memory card to perform an operation corresponding to the request specified by the storage access command A method for controlling a memory card, comprising: issuing a command to the memory card; and executing a process for returning the memory card to the specific state that is predetermined as the steady state.

Description

[0001]
BACKGROUND OF THE INVENTION
The present invention relates to an apparatus and a method for controlling a memory card, and more particularly to controlling a memory card that operates in any of a plurality of states with different types of operation commands that can be accepted according to an access command from a host system. The present invention relates to an apparatus and a method.
[0002]
[Prior art]
In recent years, various portable electronic devices such as personal computers, PDAs, cameras, and mobile phones have been developed. In these electronic devices, a memory card which is one of removable storage devices is often used. As the memory card, a PCMCIA card (PC card) and a smaller SD (Secure Digital) card are known.
[0003]
This SD card is a memory card with built-in flash memory, and is specifically designed to meet the demands for security, capacity, and speed. The SD card has a security function for the purpose of protecting the copyright of contents such as music data, and can protect the music data stored in the SD card from unauthorized copying.
[0004]
Generally, such a memory card with a security function includes a controller, a user data area that is a data storage area that a user can freely access, and a secure area that is a data storage area protected by the security function. It has been.
[0005]
When a memory card is connected to a personal computer via a memory card controller such as a memory card adapter (host controller), the access command from the operating system is converted into one or more operation commands for card control by the memory card controller. Sent to the memory card. From the operating system, the user data area in the memory card appears as a storage device similar to the disk device, but the existence of the secure area cannot be known at all. Only a special application program and a playback device having a dedicated authentication mechanism for content protection can access the secure area.
[0006]
These application programs and playback devices issue a dedicated access command for accessing the secure area to the memory card control device in order to access the secure area. The dedicated access command is converted into one or more operation commands by the memory card control device and sent to the memory card.
[0007]
[Problems to be solved by the invention]
However, in such a configuration in which a dedicated access command is converted into an operation command for a memory card and a secure area is accessed, the operation command related to the security function of the memory card and the application program interface (API) are changed. When the change of the dedicated command accompanying the change occurs, the memory card control device itself needs to be newly designed accordingly.
[0008]
Furthermore, in general, in a memory card, various states are defined, and an operation command that can be accepted is determined for each state. Therefore, the memory card control device needs to perform complicated state management control in which the memory card is transitioned to a state necessary for executing an operation command to be issued while always being aware of the current state of the memory card.
[0009]
The present invention has been made in consideration of the above-mentioned circumstances, and can flexibly cope with expansion of operation commands relating to the security function of the memory card, change of application program interface (API), and the like, and the state of the memory card. An object is to provide a memory card control device and a memory card control method capable of simplifying management control.
[0010]
[Means for Solving the Problems]
In order to solve the above-described problem, the present invention provides a memory card control device that controls a memory card that operates in any of a plurality of states in which types of operation commands that can be accepted are different. Host system Issued for access to the memory card, an operation command that directly designates an operation to be executed by the memory card, and execution state information indicating a state of the memory card to perform an operation corresponding to the operation command Means for receiving a direct command including: a state designated by execution state information included in the received direct command from a specific state predetermined as a steady state of the memory card according to the received direct command A process of causing the memory card to execute an operation corresponding to the operation command by issuing the operation command included in the received direct command to the memory card, and a process of causing the memory card to enter the specific state The process of returning sequentially Characterized by comprising the direct command execution means for lines.
[0011]
In this memory card control device, a direct command including an operation command for directly specifying an operation to be executed on the memory card is used as an access command for accessing the memory card from the host system. Furthermore, the direct command includes execution state information, and not only the operation command to be issued to the memory card but also the state of the memory card in which the operation command should be executed is simultaneously designated by the direct command. When a direct command is received from software or the like executed on the host system, 1) a process of transitioning the memory card to a state specified by the execution state information included in the direct command, 2) an operation command included in the direct command A process of issuing to the memory card and causing the memory card to execute an operation corresponding to the operation command, and 3) a process of returning the memory card to a specific state predetermined as its steady state are sequentially executed.
[0012]
By using such a direct command, an operation command included in the direct command can be issued to the memory card as it is. Therefore, an intelligent access command is interpreted and the access command is converted into one or more operation commands. Processing such as conversion is unnecessary. For this reason, direct commands can be issued even if the operation command is expanded or the application program interface (API) is changed by adding or changing the security function by using the direct command, for example, for accessing the secure area. It becomes possible to cope with it only by updating the software.
[0013]
Furthermore, in the process of executing one direct command, the memory card is changed to the state specified by the execution state information before issuing the operation command to the memory card, and the state of the memory card is changed to the steady state after issuing the operation command. Since the process of returning is automatically performed, even if a direct command accompanied by a state transition is executed, the state of the memory card is always returned to the steady state before the state transition after the execution process. By maintaining the memory card in the steady state in this way, the memory card is managed according to the execution stage information included in the direct command without performing any memory card state management in either the host system or the

memory card control device. It is possible to cause the memory card to execute a desired operation normally only by changing the state.

[0014]

DETAILED DESCRIPTION OF THE INVENTION

Hereinafter, embodiments of the present invention will be described with reference to the drawings.

FIG. 1 shows the configuration of a data processing apparatus system using a memory card control apparatus according to an embodiment of the present invention. This data processing apparatus system includes a host apparatus 11 and an SD card adapter 12 for connecting an SD memory card 13 to the host apparatus 11. The host device 11 is a data processing device such as a personal computer. In this example, the SD card adapter 12 is realized as a USB (Universal Serial Bus) device, and is connected to the USB controller 116 of the host apparatus 11 via the USB cable 117.

[0015]

An SD memory card 13 can be detachably attached to the SD card adapter 12. The SD memory card 13 is a memory card having a security function for the purpose of protecting the copyright of contents. The SD memory card 13 is provided with a storage area (also referred to as a user data area) 131 that is a data storage area that a user can freely read / write and a secure area 132 that is a data storage area protected by a security function. It has been.

[0016]

Various states are defined in the SD memory card 13, and the state transition is performed according to the operation command from the SD card adapter 12 and the progress of the internal operation of the SD memory card 13. In this case, the types of operation commands that can be accepted and executed by the SD memory card 13 are determined for each state, and in order to cause the SD memory card 13 to execute an operation corresponding to a certain operation command, the operation command is accepted. In addition, the SD memory card 13 must be set in advance to an executable state.

[0017]

In the host device 11, as shown in the figure, a normal application program 111 such as filer software that handles data files and an application program (SD application program) 112 having a copyright protection function are executed.

[0018]

The application program 111 writes a data file to the storage area 131 and reads a data file from the storage area 131 through a file system 113 that is a part of an operating system (OS) executed on the host device 11. I can do it.

[0019]

That is, the USB storage class driver 114 of the operating system (OS) is sent to the SD card adapter 12 via the USB driver 115 and the USB controller 116 in response to a file operation request from the application program 111 input via the file system 113. An access command is issued to it. Thus, the OS file system 113 can handle the storage area 131 of the SD memory card 13 as a storage device similar to the disk device.

[0020]

This access command is an intelligent disk access command conforming to the ATA command, and is converted to one or more operation commands for the SD memory card 13 by the SD card adapter 12 and then sent to the SD memory card 13. Hereinafter, an access command issued from the USB storage class driver 114 of the OS to the SD card adapter 12 for accessing the storage area 131 will be referred to as an "OS storage command".

[0021]

The SD application program 112 includes a dedicated authentication mechanism corresponding to the security function of the SD memory card 13, and can access not only the storage area 131 of the SD memory card 13 but also the secure area 132. When accessing the secure area 132, the SD application program 112 issues an access command to the SD card adapter 12 via the USB driver 115 and the USB controller 116.

[0022]

This access command is a direct command that can be issued to the SD memory card 13 as it is (pass-through command), and includes an operation command for the SD card 13 that can directly specify an operation to be executed by the SD memory card 13. It is out.

[0023]

Further, this direct command includes execution state information as a parameter of the direct command. The execution state information specifies in which state of the SD memory card 13 the operation corresponding to the operation command included in the direct command is to be executed. Hereinafter, an access command issued from the SD application program 112 to the SD card adapter 12 for accessing the secure area 132 is referred to as an "SD direct command with execution state".

[0024]

The SD card adapter 12 controls the SD memory card 13 inserted in the SD card slot according to an access command from a host system that uses the SD memory card 13. The host device 11 to which the SD card adapter 12 is connected, specifically, the OS and the SD application program 112 executed on the host device 11 each function as a host system.

[0025]

A host controller 121 is built in the SD card adapter 12. The host controller 121 is for performing an interface between the host device 11 and the SD memory card 13, and executes communication with the SD memory card 13 via the SD bus 124. The host controller 121 is realized using a microcomputer. All communications between the SD memory card 13 and the host controller 121 are controlled by operation commands from the host controller 121

[0026]

The host controller 121 has an OS storage command execution unit 122 and an SD direct command execution unit 123. The OS storage command execution unit 122 interprets and executes the above-mentioned OS storage command, and generates one or more operation commands required for causing the SD memory card 13 to execute a data read / write operation requested by the OS storage command. The SD memory card 13 is controlled using these operation commands.

[0027]

Further, after interpreting and executing the OS storage command, the OS storage command execution unit 122 executes a process for returning the state of the SD memory card 13 to a predetermined specific state. This is because the SD memory card 13 is always maintained in a specific steady state after executing the command processing of the OS storage command.

[0028]

The SD direct command execution unit 123 executes the above-described SD direct command with execution state. In the execution process of the SD direct command with execution state, 1) a process of transitioning the SD memory card 13 to the state specified by the execution state information, and 2) an operation command included in the SD direct command with execution state. 13 is issued as it is to the SD memory card 13 to execute an operation corresponding to the operation command, and 3) the SD memory card 13 is changed to the above-mentioned specific state, and the state of the SD memory card 13 is changed to a steady state. The returning process is sequentially executed in this order. As a result, even if a direct command with an execution state accompanied by a state transition is executed, the state of the SD memory card 13 is always returned to the steady state before the state transition after the execution process.

[0029]

When the state specified by the execution state information is a steady state, the processes 1) and 3) are omitted, and only the process 2) is executed.

[0030]

As described above, the SD card adapter 12 receives an access command from the host device 11 and processes different from each other depending on whether the received access command is an OS storage command or a direct command with an execution state. Is executed.

[0031]

Next, an example of the configuration of the SD memory card 13 will be described with reference to FIG.

[0032]

As shown in the figure, the SD memory card 13 includes an interface driver circuit 201, a card interface controller 202, a memory core interface 203, and a memory core 204. The memory core 204 is composed of a nonvolatile memory such as a flash EEPROM, for example, and the storage area 131 and the secure area 132 are provided in the storage space of the nonvolatile memory.

[0033]

The card interface controller 202 is an internal core circuit that executes an operation according to an operation command received from the host controller 121 via the interface driver circuit 201. The card interface controller 202 also includes a register group used for storing various status information regarding the secure area 132.

[0034]

Various status information related to the secure area 132 is also protected by the security function of the card interface controller 202 in the same manner as the secure area 132. In this sense, a register group used to store various status information related to the secure area 132 is also the secure area 132. Is part of. Therefore, read access of various status information related to the secure area 132 is also executed using the above-described direct command with execution state.

[0035]

The memory core interface 203 executes data writing to the memory core 204 and data reading from the memory core 204 under the control of the card interface controller 202.

[0036]

In the SD bus 124, six communication lines (data DAT0-3, command CMD, clock CLK) and three power supply lines (VDD, VSS, VSS) are defined. The functions of the six communication lines (data DAT0-3, command CMD, clock CLK) are as follows.

[0037]

DAT0-3: Each data line is a bidirectional signal line used for data transfer between the host controller 121 and the SD memory card 13.

CMD: Used for transferring operation commands (sometimes simply referred to as commands) from the host controller 121 to the SD memory card 13 and transferring responses from the SD memory card 13 to the host controller 121.

[0038]

CLK: The clock signal line is a signal line for transmitting the clock signal CLK from the host controller 121 to the SD memory card 13. Transfer of operation commands from the host controller 121 to the SD memory card 13, data transfer between the host controller 121 and the SD memory card 13, and the like are executed in synchronization with the clock signal CLK.

[0039]

FIG. 3 shows an example of the relationship between two typical states of the SD memory card 13 and operation commands that can be received and executed in each of these states.

[0040]

In the SD memory card 13, the following states are defined.

[0041]

- Stand-by State
- Transfer State
- Sending-data state

-Receive-data state

- Programming State

-Disk Connect State

Among these, the standby state (Stand-by State) is a kind of power save state with low power consumption, and the operation commands that can be accepted and executed in this state are operation commands other than the operation commands related to the access of the memory core 204. For example, "SD_information" command, "SD_transfer" command, and the like. The "SD_information" command is an operation command for requesting acquisition of various status information regarding the secure area 132. The "SD_transfer" command is an operation command for requesting transition to the transfer state.

[0042]

The transfer state is a state in which the SD memory card 13 can accept an operation command related to access to the memory core 204 from the host controller 121. In this state, for example, an "SD_read" command and "SD_write" are used. Commands, "SD_standby" commands, etc. can be accepted.

[0043]

The "SD_read" command is an operation command that requests data reading from the storage area 131 of the memory core 204, and the "SD_write" command is an operation command that requests data writing to the storage area 131 of the memory core 204. When the "SD_read" command is received in the transfer state, the SD memory card 13 shifts to the data transmission state (Sending-data State). The data transmission state (Sending-data State) is a state in which data is read from the memory core 204 and read data is transmitted from the SD memory card 13 to the host controller 121. When the read command processing is completed, the SD memory card 13 returns to the transfer state.

[0044]

When the "SD_write" command is received in the transfer state, the SD memory card 13 shifts to the data reception state (Receive-data State). The data reception state (Receive-data State) is a state in which write data transferred from the host controller 121 is received and accumulated in a buffer memory in the card interface controller 202. When reception of all the write data is completed, the SD memory card 13 shifts from the data reception state (Receive-data State) to the programming state (Programming State). The programming state is a state in which write data stored in the buffer memory is written to the memory core 204. When the data writing is completed, the SD memory card 13 returns to the transfer state.

[0045]

The "SD_standby" command is an operation command for requesting a transition to the transfer state. Note that the "SD_standby" command and the "SD_transfer" command are actually expressed by the same operation command (CMD7), and when the operation command (CMD7) is received in the standby state, the transition to the transfer state is performed. When the operation command (CMD7) is received, a transition to the standby state is performed.

[0046]

Further, in the transfer state, an "SD_secure_read" command for requesting data reading from the secure area 132 of the memory core 204 and an "SD_secure_write" command for requesting data writing to the secure area 132 of the memory core 204 can be received. The state transition operation of the SD memory card 13 when accepting the "SD_secure_read" command and the "SD_secure_write" command is the same as when accepting the "SD_read" command and the "SD_write" command described above.

[0047]

In the present embodiment, the transfer state is used as the above-described steady state. Unless the SD memory card 13 is always kept in the transfer state except when it is necessary to set to the standby state, an operation command relating to the access to the memory core 204 can be immediately issued to the SD memory card 13. .

[0048]

Next, an arbitration operation between an access command (OS storage command) issued from the OS and an access command (direct command with execution state) issued from the SD application program 112 will be described.

[0049]

Here, first, in order to clarify the meaning of using the direct command with execution state, it is assumed that the execution state is not attached to the direct command

issued from the SD application program 112.

[0050]

The SD application program 112 issues a direct command using an operation command that can be directly interpreted by the SD memory card 13 as an access command. Therefore, when requesting acquisition of various status information regarding the secure area 132, the SD application program 112, as shown in FIG. 4, the three direct commands, ie, "SD_standby" command, "SD_information" command, " The SD_transfer "command is issued sequentially.

[0051]

In the host device 11, all programs are executed in parallel in a multitasking format. Since the operating system and the SD application program 112 are also executed in parallel, the OS storage command may be issued from the OS between the issuance of the "SD_standby" command from the SD application program 112 and the issuance of the "SD_information" command, for example. is there. When the OS storage command is an IO read request command OS_read for requesting data reading from the storage area 131, the SD card adapter 12 converts the IO read request command OS_read into an "SD_read" command and stores it in the SD memory card 13. issue.

[0052]

Therefore, the order of the operation commands received by the SD memory card 13 is "SD_standby" command, "SD_read" command, "SD_information" command, and "SD_transfer" command.

[0053]

Since the "SD_read" command is a command that can be accepted only in the transfer state, the operation corresponding to the "SD_read" command cannot be normally executed by the SD memory card 13. The operation of the SD memory card 13 corresponding to the subsequent "SD_information" command and "SD_transfer" command is not guaranteed.

[0054]

In the present embodiment, since the direct command with execution state is used, the above-described problems do not occur. This is shown in FIG.

[0055]

As shown in FIG. 5, the SD application program 112 generates a direct command with an execution state including an "SD_information" command and execution state information indicating a state (standby state) in which the "SD_information" command is to be executed. Issued to the SD card adapter 12 as one access command.

[0056]

When the SD card adapter 12 receives the direct command with execution state from the SD application program 112, the SD card adapter 12 executes the direct command with execution state to execute three operation commands, namely, "SD_standby" command, "SD_information" command, and "SD_transfer" command. Are sequentially issued to the SD memory card 13. The SD card adapter 12 sequentially executes access commands from the OS or SD application program 112 in the order of acceptance. Therefore, no matter what time an access command, for example, an IO read request command OS_read is issued from the OS to the SD card adapter 12, the problem described with reference to FIG. 4 does not occur.

[0057]

Next, how the SD card adapter 12 determines whether the received access command is an OS storage command or a direct command with execution state will be described with reference to FIG.

[0058]

In this example, since the SD card adapter 12 is realized as a USB device, an access command from the OS or the SD application program 112 is sent to the SD card adapter 12 in the form of a USB packet. There are reserved fields in the USB packet that are not normally used.

[0059]

When the SD application program 112 requests the USB driver 115 to transmit a direct command with an execution state, the SD application program 112 requests the USB driver 115 to set a flag "1" in the reserved field. The SD card adapter 12 determines whether the access command included in the payload of the received USB packet is an OS storage command depending on whether the reservation field of the received USB packet is "1" or "0". Whether it is a command (vendor / unique command) can be determined.

[0060]

FIG. 7 shows an example of the format of the direct command with execution state.

[0061]

The direct command with execution state consists of 4 bytes. The operation code is a parameter indicating the type of operation command included in the direct command with execution state. The operation command type is

-No data command: An operation command that does not require any data transfer with the SD memory card 13

・ Command with read data: Operation command with data read from SD memory card 13

Command with write data: Operation command with write data to be written to the SD memory card 13

There are three types.

[0062]

Standby flag information (Stand-by flag) is a parameter (execution state information) for specifying an execution state. Stand-by flag = "1" indicates that the operation command should be executed in the standby state. In the present embodiment, since the steady state of the SD memory card 13 is the transfer state, Stand-by flag = "1" causes the SD memory card 13 to transition to the standby state before issuing the operation command and issue the operation command. This means that the SD memory card 13 is returned to the transfer state after the corresponding operation is completed. Stand-by flag = "0" indicates that it is not necessary to perform state transition of the SD memory card 13 before issuing the operation command, in other words, that the operation command should be executed in the transfer state which is a steady state.

[0063]

Extended command flag information (ACMD flag) indicates whether or not the operation command included in the direct command with execution state is an extended command. ACMD flag = "1" indicates an extended command. Command index information (Command Index to the memory card) indicates an operation command, and is composed of a command number of the operation command. When ACMD flag = "1", an operation command (CMD55) indicating that it is an extended command is issued prior to issuing the operation command having the command number specified by the command index information.

[0064]

The argument information (Command Argument to the memory card) indicates variables related to the operation command. The transfer length information (Data transfer length) indicates the data transfer length of the write data or read data when the operation command is a command with write data or read data.

[0065]

Next, an example of a specific configuration of the host controller 121 will be described with reference to FIG.

[0066]

In addition to the OS storage command execution unit 122 and the SD direct command execution unit 123 described above, the host controller 121 includes a command input buffer 301, a command dispatcher 302, and an SD bus interface 309 as illustrated. The command input buffer 301 is, for example, a first-in first-out pooling buffer, receives an access command issued from the OS or the SD application program 112, and temporarily stores the received access command.

[0067]

The command dispatcher 302 determines which of the OS storage command execution unit 122 and the SD direct command execution unit 123 to execute according to the type of access command stored in the command input buffer 301. That is, the command dispatcher 302 determines whether the access command issued from the

OS or the SD application program 112 is an OS storage command or a direct command with execution state, and if it is an OS storage command, the OS storage command execution unit 122. If the command is a direct command with an execution state, the SD direct command execution unit 123 processes the command. This determination process is performed in order from the previously issued access command.

[0068]

The OS storage command execution unit 122 is provided with an OS storage command interpretation unit 303, an SD command issue unit 304, and a state restoration unit 305. The OS storage command interpretation unit 303 interprets the OS storage command received from the command dispatcher 302, and one or more operations necessary for causing the SD memory card 13 to execute an operation corresponding to the request specified by the OS storage command. Determine the command. These determined operation commands are notified to the SD command issuing unit 304. If the determined operation command includes an "SD_standby" command indicating transition to the standby state, the state restoring unit 305 is notified of this. In other words, the OS storage command interpreter 303 manages which operation command can be executed in which state of the SD memory card 13 and cannot execute it in the transfer state, which is a steady state, and makes a transition to the standby state. For an operation command that requires an operation, it is determined that an "SD_standby" command should be issued before the operation command.

[0069]

The SD command issuing unit 304 sends one or more operation commands notified from the OS storage command interpreting unit 303 through the SD bus interface to cause the SD memory card 13 to execute an operation corresponding to the request specified by the OS storage command. Issued to the SD memory card 13.

[0070]

After the operation of the SD memory card 13 is completed, the state restoration unit 305 issues an "SD_transfer" command to return the state of the SD memory card 13 to the steady state (transfer state). When all operations corresponding to the request specified by the OS storage command can be executed in the transfer state, that is, the operation command issued to the SD memory card 13 includes the "SD_standby" command indicating the transition to the standby state. If not, since the SD memory card 13 is maintained in the transfer state, the "SD_transfer" command is not issued by the state restoration unit 305.

[0071]

The SD direct command execution unit 123 includes an SD direct command interpretation unit 306, an execution state interpretation unit 307, and an SD command issue unit 308. The SD direct command interpretation unit 306 extracts command index information included in the direct command with execution state received from the command dispatcher 302, and uses the command code number indicated by the command index information as it is as an operation command to be issued. Notification to 308 (command pass-through).

[0072]

The execution state interpretation unit 307 interprets standby flag information (Stand-by flag) included in the direct command with execution state received from the command dispatcher 302. If Stand-by flag = "1", the SD command issuing unit Before issuing the operation command notified from the SD direct command execution unit 123 to 308, the "SD_standby" command is issued, and the SD memory card 13 corresponding to the operation command notified from the SD direct command execution unit 123 is issued. Notify that the "SD_transfer" command should be issued after the operation is completed.

[0073]

The SD command issuing unit 308 issues an operation command to the SD memory card 13 via the SD bus interface 309 in accordance with instructions from the SD direct command interpreting unit 306 and the execution state interpreting unit 307.

[0074]

Next, how the OS storage command and the direct command with execution state are processed by the SD card adapter 12 will be described with reference to FIG.

[0075]

For example, when the application program 111 requests the OS file system 113 to read data stored in the storage area 131, the OS USB storage class driver 114 issues an IO read request command OS_read as an access command. Then, it is sent to the OS storage command execution unit 122 of the SD card adapter 12 via the USB driver 115. In the OS storage command execution unit 122, the IO read request command OS_read is converted into SD_read which is an operation command for the SD memory card 13. When this SD_read is sent to the SD memory card 13, read access for reading data from the storage area 131 is executed. Data read from the storage area 131 is passed to the application program 111 via the SD card adapter 12, the USB storage class driver 114, and the file system 113 as a response to the IO read request command OS_read.

[0076]

On the other hand, for example, when the SD application program 112 acquires status information regarding the secure area 132, the SD application program 112 indicates that the "SD_information" command should be executed in the standby state. issue standby state). The direct command with execution state is sent to the SD direct command execution unit 123 of the SD card adapter 12 without going through the OS file system 113 and the USB class driver 114. An "SD_standby" command, an "SD_information" command, and an "SD_transfer" command are sent from the SD direct command execution unit 123 to the SD memory card 13 in this order. The information read from the SD memory card 13 by executing the operation corresponding to the "SD_information" command is sent as a response to the direct command with execution state (SD_information on standby state) without going through the OS file system 113 or the like. It is passed to the SD application program 112.

[0077]

Next, the procedure of card control processing executed by the host controller 121 of the SD card adapter 12 will be described with reference to the flowchart of FIG.

[0078]

The host controller 121 retrieves the oldest access command stored in the command input buffer 301 from the command input buffer 301 and determines whether it is an OS storage command or an SD direct command with execution state (step S101).). This determination may be performed based on the bit value of the reserved field of the USB packet as described with reference to FIG. If it is an OS storage command (NO in step S101), the host controller 121 activates the OS storage command execution unit 122 and causes it to process the OS storage command (step S109). Details of the OS storage command processing by the OS storage command execution unit 122 will be described later with reference to FIG.

[0079]

On the other hand, if it is an SD direct command with execution state (YES in step S101), the host controller 121 activates the SD direct command execution unit 123 to cause it to process the SD direct command with execution state. The SD direct command execution unit 123 first determines whether or not Stand-by flag = "1" (step S102). If Stand-by flag = "1" (YES in step S102), standby is performed. The "SD_standby" command (CMD7) indicating the transition to the state is issued to the SD memory card 13, and the SD memory card 13 is shifted from the steady state (transfer state) to the standby state (step S103). On the other hand, if Stand-by flag = "0" (NO in step S102), the "SD_standby" command (CMD7) is not issued, and the SD memory card 13 is maintained in a steady state (transfer state).

[0080]

Next, the SD direct command execution unit 123 determines whether or not ACMD flag = "1" (step S104). If ACMD flag = "1" (YES in step S104), it is issued subsequently. The operation command (CMD55) indicating that the operation command is an extended command is issued to the SD memory card 13 (step S105). On the other hand, if ACMD flag = "0" (NO in step S104), CMD55 is not issued. Then, the SD direct command execution unit 123 issues an operation command having a command number specified by command index information (Command Index to the memory card) to the SD memory card 13 and performs an operation corresponding to the operation command on the SD memory. The card 13 is executed (step S106). In this case, a variable or the like designated by argument information (Command Argument to the memory card) is also issued to the SD memory card 13 as a parameter of the operation command as necessary.

[0081]

After the processing corresponding to the operation command is completed, the SD direct command execution unit 123 determines whether the SD memory card 13 has transitioned to the standby state, that is, due to Stand-by flag = "1". It is then determined whether CMD7 has been issued (step S107). When the SD memory card 13 is

transitioned to the standby state, that is, when CMD7 is issued in step S103 (YES in step S107), the SD direct command execution unit 123 puts the SD memory card 13 in the steady state. In order to return to the transfer state, CMD7 is issued to the SD memory card 13 again.

[0082]

Hereinafter, an example in which the SD application program 112 acquires the storage size of the secure area 132 and a case in which the card attributes (memory cluster size and the like) of the SD memory card 13 are extracted will be shown. Although the card attribute of the SD memory card 13 is not information directly related to the secure area 132, the access command issued from the SD application program 112 is always a direct command with an execution state.

[0083]

<When acquiring the storage size of the secure area 132>

An operation command for acquiring the storage size of the secure area 132 from the SD memory card 13 is an extended command (ACMD13) with a command number of 13. This extended command (ACMD13) is a command that can be accepted and executed in the transfer state. The direct command with execution state issued by the SD application program 112 is as follows.

[0084]

Operation Code = Command with read data

Stand-by flag = 0

ACMD flag = 1

Command Index = 13

Receiving this direct command with execution state, the host controller 121 executes the following processing.

[0085]

(1) Confirm that Stand-by flag = 0.

[0086]

(2) Confirm that ACMD flag = 1, that is, an extended command.

[0087]

(3) Issue CMD55.

[0088]

(4) The content (13) of the Command Index is issued as CMD13, and the storage size of the secure area 132 is acquired from the SD memory card 13.

[0089]

(5) Confirm that it has not transitioned to the Stand-by state, and end.

[0090]

<When acquiring card attributes (memory cluster size, etc.)>

The operation command for acquiring card attributes (memory cluster size and the like) from the SD memory card 13 is the operation command (CMD9) of command number 9. This operation command (CMD9) is a command that can be accepted and executed in the standby state. The direct command with execution state issued by the SD application program 112 is as follows.

[0091]

Operation Code = Command with read data

Stand-by flag = 1

ACMD flag = 0

Command Index = 9

Receiving this direct command with execution state, the host controller 121 executes the following processing.

[0092]

(1) Confirm that Stand-by flag = 1.

[0093]

(2) Issuing CMD7 to change the SD memory card 13 from the transfer state, which is the steady state, to the standby state.

[0094]

(3) Confirm that ACMD flag = 0, that is, not an extended command.

[0095]

(4) The contents (9) of the Command Index are issued as CMD9, and the card attribute is acquired from the SD memory card 13.

[0096]

(5) Confirm that the transition is to the Stand-by state.

[0097]

(6) CMD7 is issued again, the SD memory card 13 is returned to the transfer state, and the process ends.

[0098]

As described above, in the present embodiment, the SD memory card 13 is returned to the transfer state every time processing corresponding to the received access command is required to be managed. It is not necessary to consider the state at all, and the Stand-by flag may be set to "1" when issuing an operation command that simply needs to transition to the standby state. In this case, whether or not the Stand-by flag should be set to "1" is uniquely determined by the operation command to be issued. Further, since the host controller 121 can also determine whether or not state transition is necessary according to the content of the Stand-by flag, it is not necessary to consider the current state of the SD memory card 13 at all. Furthermore, since the command number itself of the operation command that can be directly issued to the SD memory card 13 is specified from the SD application program 112, even if the command expansion of the SD memory card 13 is performed for the purpose of extending the security function, Accordingly, it is only necessary to upgrade the SD application program 112 and there is no need to change the specifications of the host controller 121 at all.

[0099]

Next, the procedure of OS storage command processing executed in step S109 of FIG. 10 will be described with reference to the flowchart of FIG.

[0100]

First, the OS storage command execution unit 122 interprets the received OS storage command and receives an operation command necessary for causing the SD memory card 13 to execute the process requested by the OS storage command, and the operation command. The state of the SD memory card 13 capable of recording is determined (step S201). If the state of the SD memory card 13 that can accept the determined operation command is in the standby state (NO in step S202), the OS storage command execution unit 122 has the transfer state that is the steady state. Therefore, an "SD_standby" command (CMD7) indicating a transition to the standby state is issued to the SD memory card 13 to cause the SD memory card 13 to transition from the steady state (transfer state) to the standby state (step S203). On the other hand, if the state of the SD memory card 13 that can accept the determined operation command is the transfer state (YES in step S202), the SD memory card 13 is maintained in the transfer state that is the steady state. The process for making a transition to the transfer state is omitted.

[0101]

Thereafter, the OS storage command execution unit 122 issues the operation command determined in step S201 to the SD memory card 13, and causes the SD memory card 13 to execute an operation corresponding to the operation command (step S204). In this case, if necessary, variables and the like are also issued to the SD memory card 13 as parameters of the operation command. After the processing corresponding to the operation command is completed, the OS storage command execution unit

122 determines whether the SD memory card 13 has transitioned to the standby state, that is, whether CMD7 has been issued in step S203 (step S203). S205). When the SD memory card 13 is in the standby state, that is, when CMD7 is issued in step S203 (YES in step S205), the OS storage command execution unit 122 puts the SD memory card 13 in the steady state. In order to return to the transfer state, CMD7 is issued again to the SD memory card 13 (step S206).

[0102]

As described above, when the SD memory card 13 is shifted to the standby state for the OS storage command processing, the SD memory card 13 is automatically returned to the transfer state after the command processing. Therefore, the SD memory card 13 can be maintained in the transfer state even after execution of the OS storage command.

[0103]

In the present embodiment, the transfer state is used as the steady state of the SD memory card 13. However, while the SD memory card 13 is in the transfer state, the memory core 204 is not subjected to the state transition process of the SD memory card 13. This is because the operation command related to the access can be immediately issued to the SD memory card 13.

[0104]

In principle, the standby state may be used as the steady state of the SD memory card 13. In this case, in the direct command with execution state, a transfer flag indicating whether or not to transition to the transfer state is set instead of the stand-by flag.

[0105]

The host controller 121 can also be incorporated in the host device 11 that functions as a personal computer, PDA, or data processing device. In this case, the SD memory card 13 is detachably attached to a card slot provided in the host device 11.

[0106]

When the host device 11 is realized as a player dedicated to the reproduction of music data stored in the SD memory card 13, all accesses to the SD memory card 13 regardless of the storage area 131 and the secure area 132 are performed as described above. You may make it perform using the direct command with an execution state. Card control using a direct command with execution state is most suitable for a memory card having a secure area, but it can be applied not only to a memory card but also to control of an I / O card.

[0107]

All the functions of the host controller 121 described above can be realized by firmware that is a program for controlling the operation of the microcomputer of the host controller 121.

[0108]

Further, the above embodiments include inventions at various stages, and various inventions can be extracted by appropriately combining a plurality of disclosed constituent elements. For example, even if some constituent requirements are deleted from all the constituent requirements shown in the embodiment, the problem described in the column of the problem to be solved by the invention can be solved, and the effect described in the column of the effect of the invention Can be obtained as an invention.

[0109]

【The invention's effect】

As described above, according to the present invention, it is possible to flexibly cope with the expansion of operation commands related to the security function of the memory card and the change of the application program interface (API), and the state management control of the memory card. Simplification can be achieved.

[Brief description of the drawings]

FIG. 1 is a block diagram showing a configuration of a data processing system using a memory card control device according to an embodiment of the present invention.

FIG. 2 is a block diagram showing an example of the configuration of a memory card used in the present embodiment.

FIG. 3 is a diagram showing an example of a relationship between two typical states of a memory card used in the present embodiment and operation commands that can be accepted and executed in each of the states.

FIG. 4 is a diagram for explaining a problem that may occur when a direct command with an execution state is not used in the present embodiment.

FIG. 5 is a diagram for explaining arbitration processing between access commands executed using a direct command with an execution state in the present embodiment.

FIG. 6 is a diagram showing an example of a USB packet used as an access command in the present embodiment.

FIG. 7 is a diagram showing an example of the structure of a direct command with execution state used in the present embodiment.

FIG. 8 is a block diagram showing an example of the configuration of a host controller used in this embodiment.

FIG. 9 is a diagram for explaining how an OS storage command and a direct command with execution state are processed in the present embodiment;

FIG. 10 is a flowchart showing a procedure of card control processing executed in the present embodiment.

FIG. 11 is a flowchart showing a procedure of OS storage command processing executed in the embodiment.

[Explanation of symbols]

11: Host device

12 ... SD card adapter

13 ... SD memory card

111: Normal application program

112 ... SD application program

113 ... File system

114 ... USB storage class driver

115 ... USB driver

116 ... USB controller

121 ... Host controller

122 ... OS storage command execution unit

123 ... SD direct command execution section

131: Storage area

132: Secure area

Patent Citations (10)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
JPH0314083A *	1989-06-12	1991-01-22	Toshiba Corp	Portable medium
JP2791105B2 *	1989-06-12	1998-08-27	株式会社東芝	Portable storage media

DE69932448ST2 *	1992-11-27	1999-09-30	Denso Corp	Portable electronic device
JP3421378B2 *	1993-03-23	2003-06-30	株式会社東芝	Transmission control method
JPH11505049A *	1995-05-09	1999-05-11	スマートムーブ（エヌジー）リミテッド	Card interface
US6226749B1 *	1995-07-31	2001-05-01	Hewlett-Packard Company	Method and apparatus for operating resources under control of a security module or other secure processor
US5799168A *	1996-01-05	1998-08-25	M-Systems Flash Disk Pioneers Ltd.	Standardized flash controller
US6085282A *	1997-09-24	2000-07-04	Motorola, Inc.	Method and apparatus for distinguishing register reads from memory reads in a flash memory
FR2797074B1 *	1999-07-28	2001-10-12	Gemplus Card Int	CHIP CARD ARCHITECTURE INCLUDING PERIPHERALS
US6633928B2 *	2000-11-29	2003-10-14	Hewlett-Packard Development Company, L.p.	Fast process context switching buffer

* Cited by examiner, † Cited by third party

Cited By (74)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US7107378B1	2000-09-01	2006-09-12	Sandisk Corporation	Cooperative interconnection and operation of a non-volatile memory card and an input-output card
AU2003220678A1 *	2002-04-08	2003-10-27	Socket Communications, Inc	Wireless enabled memory module
TWI246064B *	2002-07-29	2005-12-21	Milsys Ltd	Data storage and processing device, electronic appliance, electronic system and method of operating an appliance that responds to a plurality of commands
US7979706B2	2002-08-23	2011-07-12	Sandisk Corporation	Apparatus, system and method for securing digital documents in a digital appliance
US7136750B2	2002-11-13	2006-05-06	Sandisk Corporation	Universal non-volatile memory card used with various different standard cards containing a memory controller
US8037229B2	2002-11-21	2011-10-11	Sandisk Technologies Inc.	Combination non-volatile memory and input-output card with direct memory access
TW200410122A *	2002-12-13	2004-06-16	Apacer Technology Inc	Direct coupling type serial transmitting interface card
JP2004220575A *	2002-12-27	2004-08-05	Ricoh Co Ltd	Interface circuit of card type memory, asic carrying its circuit and image forming apparatus carrying asic
US9591112B2 *	2002-12-31	2017-03-07	Google Technology Holdings LLC	Command queuing for multimedia storage devices
US7197583B2 *	2003-01-21	2007-03-27	Zentek Technology Japan, Inc.	SDIO controller
EP1609048A4	2003-03-27	2009-01-14	Milsys Ltd	Data storage device with full access by all users
GB0307450D0 *	2003-03-31	2003-05-07	Matsushita Electric Ind Co Ltd	Method for interfacing storage devices
US7305535B2	2003-04-17	2007-12-04	Sandisk Corporation	Memory cards including a standard security function
US20050044330A1 *	2003-07-28	2005-02-24	Gidon Elazar	System, apparatus and method for controlling a storage device
US7209995B2 *	2003-12-09	2007-04-24	Sandisk Corporation	Efficient connection between modules of removable electronic circuit cards
JP2005182122A *	2003-12-16	2005-07-07	Alpine Electronics Inc	Removable recording medium and file control method therefor
WO2005067377A2 *	2004-01-15	2005-07-28	M-Systems Flash Disk Pioneers Ltd.	Removable medium with bookmark
EP1728374B1	2004-02-03	2009-10-28	SanDisk Secure Content Solutions, Inc.	Protection of digital data content

US7162647B2 *	2004-03-11	2007-01-09	Hitachi, Ltd.	Method and apparatus for cryptographic conversion in a data storage system
JP2005310118A *	2004-03-23	2005-11-04	Toshiba Corp	Information terminal and data transfer method for information terminal
US20060112209A1 *	2004-11-24	2006-05-25	Li-Hc Yao	SD memory card with a USB plug
US9104315B2	2005-02-04	2015-08-11	Sandisk Technologies Inc.	Systems and methods for a mass data storage system having a file-based interface to a host and a non-file-based interface to secondary storage
US7877539B2 *	2005-02-16	2011-01-25	Sandisk Corporation	Direct data file storage in flash memories
US20060184719A1 *	2005-02-16	2006-08-17	Sinclair Alan W	Direct data file storage implementation techniques in flash memories
US20060184718A1 *	2005-02-16	2006-08-17	Sinclair Alan W	Direct file data programming and deletion in flash memories
US20060182110A1 *	2005-02-17	2006-08-17	Bomhoff Matthew D	Apparatus, system, and method for fibre channel device addressing
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
US7568056B2 *	2005-03-28	2009-07-28	Nvidia Corporation	Host bus adapter that interfaces with host computer bus to multiple types of storage devices
US7627733B2 *	2005-08-03	2009-12-01	Sandisk Corporation	Method and system for dual mode access for storage devices
US7558906B2	2005-08-03	2009-07-07	Sandisk Corporation	Methods of managing blocks in nonvolatile memory
US7949845B2 *	2005-08-03	2011-05-24	Sandisk Corporation	Indexing of file data in reprogrammable non-volatile memories that directly store data files
US7409489B2 *	2005-08-03	2008-08-05	Sandisk Corporation	Scheduling of reclaim operations in non-volatile memory
US7480766B2 *	2005-08-03	2009-01-20	Sandisk Corporation	Interfacing systems operating through a logical address space and on a direct data file basis
US7558271B2	2005-08-03	2009-06-23	Sandisk Corporation	Nonvolatile memory with block management
US7669003B2 *	2005-08-03	2010-02-23	Sandisk Corporation	Reprogrammable non-volatile memory systems with indexing of directly stored data files
US8855714B2 *	2005-09-14	2014-10-07	Sandisk Il Ltd.	Removable media player for mobile phones
US7814262B2 *	2005-10-13	2010-10-12	Sandisk Corporation	Memory system storing transformed units of data in fixed sized storage blocks
US7529905B2 *	2005-10-13	2009-05-05	Sandisk Corporation	Method of storing transformed units of data in a memory system having fixed sized storage blocks
US8078788B2	2005-12-08	2011-12-13	Sandisk Technologies Inc.	Media card command pass through methods
US20070136501A1 *	2005-12-08	2007-06-14	Chang Robert C	Media card command pass through methods
US20070168608A1 *	2005-12-08	2007-07-19	Chang Robert C	Media card with command pass through mechanism
US7877540B2 *	2005-12-13	2011-01-25	Sandisk Corporation	Logically-addressed file storage methods
US7747837B2 *	2005-12-21	2010-06-29	Sandisk Corporation	Method and system for accessing non-volatile storage devices
US7793068B2 *	2005-12-21	2010-09-07	Sandisk Corporation	Dual mode access for non-volatile storage devices
US7769978B2 *	2005-12-21	2010-08-03	Sandisk Corporation	Method and system for accessing non-volatile storage devices
CN100373319C *	2006-01-20	2008-03-05	骆建军	Adaptive SD memory card
KR100745603B1 *	2006-02-08	2007-08-02	삼성전자주식회사	Secure mmc card and memory card system having them
WO2007113945A1 *	2006-04-05	2007-10-11	Panasonic Corporation	Removable memory device, phase synchronizing method, phase synchronizing program, medium recording the same, and host terminal
US7447821B2 *	2006-04-21	2008-11-04	Sandisk Corporation	U3 adapter
US7516261B2 *	2006-04-21	2009-04-07	Sandisk Corporation	Method for U3 adapter

US20070260797A1 *	2006-05-03	2007-11-08	Chien-yuan Chen	Memory card with an expansion function
US8839005B2	2006-09-13	2014-09-16	Sandisk Technologies Inc.	Apparatus for transferring licensed digital content between users
JP4956143B2 *	2006-11-02	2012-06-20	株式会社東芝	Semiconductor memory card, host device, and data transfer method
FR2908195B1	2006-11-06	2009-02-06	Oberthur Card Syst Sa	METHOD FOR PASSING INSTRUCTIONS BETWEEN A HOST STATION AND A PORTABLE ELECTRONIC DEVICE, AND DEVICE FOR IMPLEMENTING THE SAME
EP1927939A1 *	2006-11-30	2008-06-04	Cassis International PTE Ltd.	Secure MMC standard smartcard with multi-application operation capability, process of operation
JP2008147871A *	2006-12-07	2008-06-26	Sony Corp	Communication system and repeater
JP4538027B2	2007-08-22	2010-09-08	株式会社東芝	Semiconductor device
US9003154B2	2007-12-13	2015-05-12	Sandisk Technologies Inc.	Integration of secure data transfer applications for generic IO devices
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US20090164675A1 *	2007-12-24	2009-06-25	Aten International Co., Ltd.	Kvm switch with a remote control incorporating a memory card adapter
US8348122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US20100033310A1 *	2008-08-08	2010-02-11	Narendra Siva G	Power negotation for small rfid card
AU2008361371B2 *	2008-09-04	2014-04-03	T-Data Systems (S) Pte Ltd	Method and apparatus for wireless digital content management
TW201013397A *	2008-09-17	2010-04-01	Incomm Technologies Co Ltd	Memory apparatus and operating method thereof
US9405939B2	2008-10-07	2016-08-02	Arm Limited	Data processing on a non-volatile mass storage device
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
KR101573791B1 *	2009-06-10	2015-12-02	삼성전자주식회사	Method and apparatus for transferring data using Universal Serial Bus
WO2011068464A1 *	2009-12-01	2011-06-09	T-Data Systems (S) Pte Ltd	Memory card and method for storage and wireless transceiving of data
WO2011108989A1 *	2010-03-01	2011-09-09	T-Data Systems (S) Pte Ltd	A memory card
JP5728292B2 *	2011-02-04	2015-06-03	株式会社東芝	Memory device and host system
JP2014096126A *	2012-11-12	2014-05-22	Yec:Kk	External connection storage device
US10318193B2	2015-09-14	2019-06-11	Sandisk Technologies Llc	Systems and methods of command authorization
KR20190033920A *	2017-09-22	2019-04-01	삼성전자주식회사	Storage device and method of operating the same

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
JP3641230B2	2005-04-20	Apparatus and method for controlling a memory card
US7797490B2	2010-09-14	Memory card authentication system, memory card host device, memory card, storage area switching method, and storage area switching program
US8135871B2	2012-03-13	Computer system and control method of the same
US7721046B2	2010-05-18	Memory card authentication system, capacity switching-type memory card host device, capacity switching-type memory card, storage capacity setting method, and storage capacity setting program
KR100745603B1	2007-08-02	Secure mmc card and memory card system having them
US8250245B2	2012-08-21	Information processing system, with information processing terminal capable of operating in multiple operation modes when connected to a host device
JPH1153485A	1999-02-26	Computer system, storage device, conversion system and storage medium

US8327124B2	2012-12-04	SD switch box in a cellular handset
JP3641239B2	2005-04-20	Apparatus and method for controlling a memory card
US7424580B2	2008-09-09	Data transfer control device, electronic instrument, program and method of fabricating electronic instrument
JP2006031123A	2006-02-02	Usb memory device and usb memory device control program
JP4793798B2	2011-10-12	Microcomputer
US8028102B2	2011-09-27	Electronic apparatus and method of controlling a memory unit connected to the same
JP2006350881A	2006-12-28	Memory card controller and memory card control system
JP3531438B2	2004-05-31	Data management device, data management method, data management system, and external storage device
US20080294824A1	2008-11-27	Device information management systems and methods
KR100856811B1	2008-09-05	Universal Serial Bus interface apparatus
KR20080060916A	2008-07-02	Usb controller available to process drm and drm processing apparatus used thereto
JP2000276383A	2000-10-06	Computer with function for changing storage capacity and method for changing storage capacity

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
JP2001323956A	2001-10-22	2001-10-22	Apparatus and method for controlling a memory card

Applications Claiming Priority (3)

Application	Filing date	Title
JP2001323956A	2001-10-22	Apparatus and method for controlling a memory card
EP02019012A	2002-08-26	Apparatus and method for controlling a card device
US10/233,464	2002-09-04	Apparatus and method for controlling a card device

Legal Events

Date	Code	Title	Description
2004-02-20	A977	Report on retrieval	**Free format text**: JAPANESE INTERMEDIATE CODE: A971007 **Effective date**: 20040220
2004-03-17	A131	Notification of reasons for refusal	**Free format text**: JAPANESE INTERMEDIATE CODE: A131 **Effective date**: 20040316
2004-05-13	A521	Written amendment	**Free format text**: JAPANESE INTERMEDIATE CODE: A523 **Effective date**: 20040512
2005-01-13	TRDD	Decision of grant or rejection written	
2005-01-19	A01	Written decision to grant a patent or to grant a registration (utility model)	**Free format text**: JAPANESE INTERMEDIATE CODE: A01 **Effective date**: 20050118
2005-01-27	A61	First payment of annual fees (during grant procedure)	**Free format text**: JAPANESE INTERMEDIATE CODE: A61 **Effective date**: 20050120
2007-12-13	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text**: PAYMENT UNTIL: 20080128 **Year of fee payment**: 3
2007-12-18	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text**: PAYMENT UNTIL: 20090128 **Year of fee payment**: 4

2008-12-16	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20100128 Year of fee payment: 5
2009-12-22	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20110128 Year of fee payment: 6
2010-12-14	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20120128 Year of fee payment: 7
2011-12-13	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20130128 Year of fee payment: 8
2012-12-13	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20130128 Year of fee payment: 8
2012-12-18	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20140128 Year of fee payment: 9
2015-01-28	LAPS	Cancellation because of no payment of annual fees	

Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

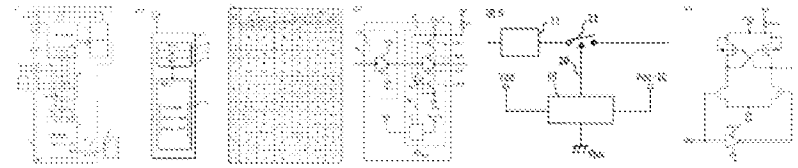
Patents JP4412947

Memory card

Abstract

The present invention provides a memory card equipped with an interface controller connected to external connecting terminals, a memory connected to the interface controller, and a security controller connected to the interface controller. A second external connecting terminal capable of supplying an operating power supply to the security controller is provided aside from a first external connecting terminal which supplies an operating power supply to the interface controller and the memory. An interface unit of the interface controller connected to the security controller receives the operating power supply from the second external connecting terminal and thereby enables a stop of the supply of the operating power supply from the first external connecting terminal. Even if the supply of the operating power supply to the interface controller is cut off, the output of the interface unit is not brought to an indefinite state.

Images (26)



Classifications

- G06K19/077 Constructional details, e.g. mounting of circuits in the carrier

View 29 more classifications

JP4412947B2

Japan

Download PDF Find Prior Art Similar

Other languages: Japanese

Inventor: 裕幸 西澤, 顕 樋口, 賢治 大沢, 環 和田, 達昭 杉山, 昇… 郎 大田

Worldwide applications

2003 JP 2004 EP DE EP KR CN US TW 2007 US

Application JP2003316002A events

2003-09-08	Application filed by 株式会社ルネサステクノロジ
2003-09-08	Priority to JP2003316002A
2005-03-31	Publication of JP2005084935A
2010-02-10	Application granted
2010-02-10	Publication of JP4412947B2
Status	Expired - Fee Related
2023-09-08	Anticipated expiration

Info: Patent citations (22), Cited by (53), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (14)

Hide Dependent

1. A plurality of wiring boards on which the external connection terminals are formed, wherein the interface controller connected to the external connection terminals, a memory coupled to the interface controller, and security over controller coupled to said interface controller is mounted,
A second external connection terminal capable of supplying operating power to the security controller separately from the first external connection terminal supplying operating power to the interface controller and the memory,
An interface unit of the interface controller connected to the security controller receives operating power from the second external connection terminal, and can stop supply of operating power from the first external connection terminal. .

2. 2. The memory card according to claim 1, wherein the interface unit is controlled to be in a high impedance state in a state where operation power supply from the first external connection terminal is stopped.

3. The interface unit performs a level shift between a signal level based on a first power supply voltage supplied to the first external connection terminal and a signal level based on a second power supply voltage supplied to the second external connection terminal. 3. The memory card according to claim 1, wherein the memory card is a memory card.

4. The interface terminal of the security controller has a third external connection terminal for inputting a clock signal, a fourth external connection terminal for data input / output, and a fifth external connection terminal for reset signal input. 3. Symbol mounting the memory card.

5. The interface controller can use the third external connection terminal to the fifth external connection terminal as external connection terminals for input / output signals according to a card mode recognized by the interface controller. 4. The memory card according to 4.

6. 6. The memory card according to claim 5, further comprising a separation switch circuit that allows the third external connection terminal to the fifth external connection terminal to be selectively disconnected from the interface controller.

7. 3. The security controller is one or both of an IC card microcomputer capable of a non-contact interface with the outside and an IC card microcomputer capable of a contact interface with the outside. Memory card.

8. 3. The memory card according to claim 1, wherein the security controller is an IC card microcomputer capable of both an external contactless interface and a contact interface.

9. The security controller is an IC card microcomputer capable of a non-contact interface with the outside, and has an antenna connection terminal capable of connecting an antenna for a non-contact interface as the external connection terminal, and the antenna connection terminal is 3. The memory card according to

claim 1, wherein the memory card is disposed adjacent to the second external connection terminal and in the vicinity of the first external connection terminal.

10. 10. The memory card according to claim 9, wherein the plurality of external connection terminals have a staggered arrangement in which the arrangement in the column direction is shifted between adjacent columns before and after the insertion direction of the memory card.

11. 11. The memory card according to claim 10, further comprising: the second external connection terminal to the fifth external connection terminal and the antenna connection terminal in a rear side array adjacent to each other in the memory card insertion direction.

12. 12. The memory card according to claim 11, wherein the second external connection terminal and the antenna connection terminal are located at a central portion of the column direction arrangement.

13. 13. The memory card according to claim 12, wherein the second external connection terminal has a staggered arrangement with respect to the antenna connection terminal.

14. The interface controller, memory and security controller are each composed of individual semiconductor chips,
The semiconductor chip constituting the interface controller is stacked on the semiconductor chip constituting the memory, and the electrode pads arranged along the same side of the semiconductor chip are wire-bonded to the electrodes of the wiring board. The memory card according to claim 1 or 2.

Description

The present invention relates to a memory card on which a security controller is mounted together with an interface controller and a memory.

In Patent Document 1, a SIM (Subscriber Identity Module) is installed in a memory card conforming to the MMC standard in order to realize multi-bank and multi-function while maintaining compatibility with the MMC (Multi-Media Card: registered trademark) standard. Thus, a technique for enhancing security is described.

Patent Document 2 describes a storage device on which a flash memory chip, an IC card chip that executes security processing, and a controller chip that controls them according to instructions from the outside are mounted.

Non-Patent Document 1 describes a standard for a multimedia card.

International Publication WO01 / 84480 Pamphlet

JP 2003-91704 A

The present inventor studied a memory card that implements a multifunction by installing a security controller such as an IC card microcomputer together with an interface controller and a memory.

First, when the interface controller and the security controller are connected, the operation power supply voltage supplied from the outside is stopped, the supply of the operation power supply voltage for the interface controller and the memory is stopped, and the operation power supply voltage is supplied only to the security controller. it has been clarified that there is an inconvenience in the operation mode in which only the security controller is turned on and the security processing is executed exclusively when it can be supplied. That is, if the operating power is not turned on to the interface controller, the output control state of the output buffer in the interface unit of the interface controller connected to the security controller may be indefinite and in a low impedance state. When a clock or signal for power-on reset or activation of the security controller is supplied from the outside in such a state, the clock or signal flows into the interface section in a low impedance state, resulting in noise that cannot be ignored. It has been found that there is a risk of malfunction. In particular, when the security controller or the like interfaces with the outside in a non-contact manner, there is a concern that the communication sensitivity may be significantly reduced.

Second, when the security controller has a non-contact interface function, when the connection terminal of the external antenna for improving the communication sensitivity is provided on the wiring board of the card, the arrangement relationship with other connection terminals such as a signal and a clock is changed. The importance of consideration has been found by the inventors. In other words, if the routing of wiring to the connection terminals such as signals and clocks on the wiring board and the routing of wiring to the connection terminals of the external antenna are often complicated, the crosstalk will increase. Noise is superimposed on the signal line and the clock wiring by induction or induction. Alternatively, noise due to crosstalk or induction from the signal line or the clock wiring is superimposed on the high-frequency signal received from the external high-frequency antenna, and an error may occur in the input / output data during the non-contact operation. It is necessary to adopt an arrangement that can suppress the generation of such noise as much as possible for the connection terminal of the external antenna. Furthermore, when the operation power supply voltage level of the security controller is higher than the operation power supply voltage level of the interface controller when the supply of the operation power supply voltage for the interface controller and the memory is stopped and the operation power supply voltage can be supplied to the security controller Therefore, the same consideration as described above is required for the arrangement of the external connection terminals for supplying high-level operation power.

An object of the present invention is to suppress the occurrence of noise in a memory card that implements a multifunction by mounting a security controller together with an interface controller and a memory.

An object of the present invention is to suppress the generation of noise in an operation mode in which an operation power is turned on only for a security controller and a security process is executed in a memory card that implements a multifunction by installing a security controller together with an interface controller and a memory. There is.

Another object is to reduce the power consumption of the entire memory card by separating the operating power of the interface controller and the security controller.

Another object of the present invention is to arrange a connection terminal for connecting an external antenna to the security controller having a non-contact interface function in a memory card that realizes multi-function by mounting a security controller together with an interface controller and a memory. The purpose is to prevent the generation of noise in relation to other connection terminals.

The above and other objects and novel features of the present invention will be apparent from the description of this specification and the accompanying drawings.

The following is a brief description of an outline of typical inventions disclosed in the present application.

[1] A memory card according to the present invention includes an interface controller (7) connected to the external connection terminal on a wiring board on which a plurality of external connection terminals are formed, and a memory (8) connected to the interface controller. And a security controller (9) connected to the interface controller, and supply operating power to the security controller separately from the first external connection terminal (C4) that supplies operating power to the interface

controller and memory. An interface unit of the interface controller that has a second external connection terminal (C15) that can be connected to the security controller receives an operation power from the second external connection terminal, and operates from the first external connection terminal The power supply can be stopped.

Even if the operation power supply to the interface controller is cut off, the interface section (11) is supplied with the operation power to the security controller, so the output of the interface section does not become indefinite, and an indefinite current flows there. It can suppress flowing and becoming noise. In order to prevent any unnecessary current from flowing through the interface unit, the interface unit may be controlled to a high impedance state in a state where the operation power supply from the first external connection terminal is stopped.

In a specific form of the present invention, the interface unit has a signal level based on a first power supply voltage supplied to the first external connection terminal and a signal level based on a second power supply voltage supplied to the second external connection terminal. Level shift function for performing level shift between the two.

In a specific form of the present invention, as an interface terminal of the security controller, a third external connection terminal (C11) for inputting a clock signal, a fourth external connection terminal (C13) for data input / output, and a reset signal input 5th external connection terminal (C10). At this time, the third external connection terminal to the fifth external connection terminal can be used by the interface controller as external connection terminals for input / output signals according to the card mode recognized by the interface controller. For example, it is possible to cope with several card modes having different numbers of parallel data input / output bits. When the interface controller uses the third external connection terminal to the fifth external connection terminal as data input / output external connection terminals, the security controller can interface with the outside via the interface controller. At this time, if the third external connection terminal to the fifth external connection terminal are separated from the interface controller by the separation switch circuit (12), they are connected to the third external connection terminal to the fifth external connection terminal. Thus, it is possible to suppress an undesired output of a signal exchanged with the interface controller according to the interface function of the security controller to the external circuit.

As a specific form of the present invention, the security controller may be an IC card microcomputer capable of a non-contact interface with the outside and / or an IC card microcomputer capable of a contact interface with the outside. . Further, the security controller may be an IC card microcomputer capable of both a non-contact interface and a contact interface.

As a specific form of the present invention, when the security controller is a microcomputer for an IC card capable of non-contact interface with the outside, an antenna connection terminal capable of connecting a high-frequency antenna for non-contact interface as the external connection terminal in the case of having (C14, C16), it is desirable that the antenna connection terminal is disposed adjacent to the second external connection terminal and in the vicinity of the first external connection terminal. Such an antenna connection terminal is used for connection of an external high-frequency antenna for increasing the sensitivity of the non-contact interface. The voltage applied to the antenna connection terminal is relatively high and the frequency is high. Therefore, if the routing of wiring to the connection terminals such as signals and clocks on the wiring board and the routing of wiring to the connection terminals of the external antenna are complicated, crosstalk will increase. Noise is superimposed on the signal line and the clock wiring by induction or induction. Alternatively, noise due to crosstalk or induction from the signal line or the clock wiring is superimposed on the high-frequency signal received from the external high-frequency antenna, and an error may occur in the input / output data during the non-contact operation. Since the antenna connection terminal is arranged adjacent to the second external connection terminal and in the vicinity of the first external connection terminal, the arrangement is suitable for suppressing noise generation as much as possible.

The plurality of external connection terminals have a staggered arrangement in which the arrangement in the column direction is shifted between adjacent columns before and after the insertion direction of the memory card. With this staggered arrangement, it is possible to cope with the increase in the number of terminals by a relatively simple configuration in which a large number of slot terminals are alternately arranged in parallel in card slots from which memory cards are attached and detached. For example, the second external connection terminal to the fifth external connection terminal and the antenna connection terminal are arranged in a rear array adjacent to the memory card in the insertion direction. In particular, the second external connection terminal and the antenna connection terminal may be located at the center of the column direction arrangement. The second external connection terminals may be staggered with respect to the antenna connection terminals.

As yet another specific form of the present invention, when the interface controller, the memory and the security controller are individual semiconductor chips, the semiconductor chip constituting the interface controller is stacked on the semiconductor chip constituting the memory, it is preferable to wire bond the electrodes of the wiring board to the electrode pads arranged along the sides in the same direction of the semiconductor chips. Bonding wires can be shortened and wire interference is reduced.

[2] A memory card according to the present invention includes a wiring board on which a plurality of external connection terminals are formed, an interface controller connected to the external connection terminals, a memory connected to the interface controller, and a security controller. And a second external connection terminal capable of supplying operating power to the security controller separately from the first external connection terminal that is mounted and supplies operating power to the interface controller and the memory. An IC card microcomputer capable of a non-contact interface, wherein the external connection terminal has an antenna connection terminal to which an antenna for a non-contact interface can be connected, and the antenna connection terminal is the second external connection terminal Adjacent to the first external connection end it is disposed in the vicinity of.

The plurality of external connection terminals have a staggered arrangement in which the arrangement in the column direction is shifted between adjacent columns before and after the insertion direction of the memory card. Due to this staggered arrangement, the card slot can be made multi-terminal with a relatively simple configuration in which a large number of slot terminals are alternately arranged in parallel with different projection amounts. For example, the second external connection terminal to the fifth external connection terminal and the antenna connection terminal are arranged in a rear array adjacent to the memory card in the insertion direction. In particular, the second external connection terminal and the antenna connection terminal may be located at the center of the column direction arrangement. The second external connection terminals may be staggered with respect to the antenna connection terminals.

The effects obtained by the representative ones of the inventions disclosed in the present application will be briefly described as follows.

In a memory card that implements a multifunction by installing a security controller together with an interface controller and a memory, it is possible to suppress the occurrence of noise in an operation mode in which only the security controller is turned on to perform security processing

In a memory card that realizes multi-function by installing a security controller together with an interface controller and memory, the arrangement of connection terminals for connecting an external antenna to the security controller having a non-contact interface function is related to other connection terminals. It is possible to prevent the generation of noise

It is possible to suppress the generation of noise in a memory card that implements a multifunction by installing a security controller together with an interface controller and a memory.

《Communication portable terminal device》
FIG. 2 shows an outline of a communication portable terminal device such as a cellular phone to which a memory card according to an example of the present invention is applied. The communication portable terminal device 1 includes, for example, a microprocessor (MPU) 2 that controls the entire system, a baseband processing unit

(BB) 3 that performs baseband processing such as modulation and demodulation for mobile communication, and a prescribed high frequency. A high-frequency unit (RFcI) 4 that performs transmission and reception and a memory card (MRYC) 5 are included. The MRYC 5 is detachably attached to a card slot (not shown) of the communication portable terminal device 1. MPU2 is positioned as a card host for MRYC5.

MRYC5 has multi-functions such as memory storage function, high-level security processing function for e-commerce, low-level security processing function for charging in transportation, etc., content data encryption / decryption processing function, etc. provide.

<< MRYC with built-in IC card microcomputer >>
FIG. 1 illustrates the configuration of MRYC5. The MFMC 5 is an interface controller 7, a flash memory 8 connected to the interface controller 7, and a security controller connected to the interface controller 7 on a wiring board on which a plurality of external connection terminals C 1 to C 16 are formed. An IC (Integrated Circuit) card microcomputer (also referred to as an IC card microcomputer) 9 is mounted. The interface controller 7, the flash memory 8, and the IC card microcomputer 9 are each constituted by individual semiconductor integrated circuit chips.

The interface controller 7 has an external interface function as a memory card, a memory interface function according to the specifications of the flash memory, and an IC card microcomputer interface function for interfacing with an IC card microcomputer using a memory card command. Here, MRYC5 satisfies the external interface specification as a memory card compliant with the multimedia card standard.

The flash memory 8 is an electrically erasable and writable nonvolatile memory. The flash memory 8 includes a nonvolatile memory cell transistor (also referred to as a flash memory cell) that is electrically erasable and writable, although not particularly illustrated. The flash memory cell is not particularly shown, but a so-called stacked gate structure having a floating gate, or a so-called split gate structure comprising a memory transistor portion and an select transistor portion having an ONO (oxide nitride oxide) gate insulating film. Have In the flash memory cell, the threshold voltage increases when electrons are injected into the floating gate or the like, and the threshold voltage decreases when electrons are extracted from the floating gate or the like. The flash memory cell stores information corresponding to the level of the threshold voltage with respect to the word line voltage for reading data. Although not particularly limited, in this specification, a state in which the threshold voltage of the memory cell transistor is low is referred to as an erased state, and a state in which the threshold voltage is high is referred to as a written state.

Although not shown in particular, the IC card microcomputer 9 includes a CPU, a non-volatile memory for storing the operation program and control information used for authentication, and performs authentication processing according to the operation program. Here, the IC card microcomputer 9 is a contact / non-contact dual-way IC card capable of a contact interface and a non-contact interface with the outside. The contact interface is performed by serial communication using a 1-bit data input / output terminal I / O, a clock terminal CLK, and a reset terminal RES. The non-contact interface is performed by high-frequency communication using an antenna connected to the terminals TML1 and TML2. In the figure, the external antenna 10 and the tuning capacitor 13 are representatively shown. Although not specifically shown, the non-contact interface is provided with an internal antenna connected to the terminals TML1 and TML2 inside the MRYC5 package or on the circuit board, and when the external antenna 10 is connected to the terminals C14 and C16, the internal antenna can be separated by a switch. A configuration may be provided.

Among the external connection terminals C1 to C16, functions and arrangement of C1 to C7 conform to the MMC standard, and C8 to C13 correspond to a multi-bit data bus. C14 to C16 are newly established.

FIG. 3 shows the function assignment of the external connection terminals C1 to C16 according to the card mode of MRYC5. The 1-bit mode, 4-bit mode, and 8-bit mode mean the number of data input / output bits with respect to the outside of MRYC5. Only the non-contact card function means a case where an IC card microcomputer having only a non-contact interface function is mounted as an external interface function, and details of this example will be described later. In the figure, RSV (for MMC) is a reserve terminal in MMC mode, CS (for SPI) is a chip select terminal in SPI mode, CMD is a command terminal, Vss1 and Vss2 are circuit ground terminals, Vdd is a power supply terminal, and CLK is a memory. Card clock terminal, DAT is serial data input / output terminal, RES-ic is IC card microcomputer reset terminal, CLK-ic is IC card microcomputer clock terminal, Vcc-ic is IC card microcomputer power supply terminal, LA and LB are An antenna connection terminal, Vcc-IC is a dedicated power supply terminal for the IC card microcomputer, and DAT0 to DAT7 are parallel data input / output terminals.

As is apparent from FIG. 3, C1 to C9 are basically assigned to the memory card interface function, and C10 to C16 are assigned to the IC card interface function. However, although C10 to C13 are assigned to the IC card interface function in the 1-bit mode and the 4-bit mode, they are assigned to the memory card interface function as parallel data input / output terminals of DAT4 to DAT7 in the 8-bit mode. The difference in function assignment of the terminals C10 to C13 appears as wirings L1 to L4 connecting the interface controller 7 and the IC card microcomputer 9 in the circuit of FIG. In short, the wirings L1 to L4 assigned to the connection to the external connection terminals C10 to C13 in the interface unit 11 of the interface controller 7 are connected to the terminals Vcc, I / O-ic, CLK-ic, and RES-ic of the IC card microcomputer 9. To do. In the 8-bit mode, the separation switch circuit 12 is cut off by the control of the interface controller 7 when the interface controller 7 communicates with the IC card microcomputer 9, and separates the connection with the external connection terminals C10, C11, C13. When the interface controller 7 communicates with the outside using C12 as DAT6, the connection with the terminal Vcc of the IC card microcomputer 9 is separated, and the functions of the data terminals DAT4 to DAT7 assigned to the external connection terminals C10 to C13 in the 8-bit mode Selection is performed on the MRYC 5 side based on the difference between the functions of the terminals Vcc, I / O, CLK, and RES connected to the wirings L1 to L4.

Here, the operation power supply to the IC card microcomputer 9 will be described with reference to FIG. In addition to the external connection terminal (first external connection terminal) C4 for supplying the operation power supply Vdd to the interface controller 7 and the flash memory 8, an external connection end terminal (for supplying the operation power supply Vcc-IC to the IC card microcomputer 9) A second external connection terminal) C15. The operation power supply to the IC card microcomputer 9 is performed by C12 and C15 in the configuration of FIG. 1, but the operation power supply by C12 is not essential. C15 can be substituted. Note that the switch SW1 of the separation switch circuit 12 is a switch that is required by adding the terminal C15. That is, Vcc-IC is always supplied from C15 to the wiring L4 regardless of the usage form of C12.

The terminal C15 also supplies operating power to the interface unit 11, and when the supply of operating power Vdd from C4 is stopped, the input impedance of the input / output circuit in the interface unit 11 connected to the wirings L1 to L4 is reduced or the output is undefined. Eliminate. That is, when the supply of the power supply Vdd from C4 is stopped in order to suppress wasteful power consumption when only the IC card microcomputer 9 of MRYC5 is operated, the output state of the output buffer in the interface unit 11 becomes indefinite. In this state, when the IC card microcomputer 9 is operated by performing a power-on reset of the IC card microcomputer 9 with a contact interface using C10 to C13, for example, a clock signal from C11 flows into the output buffer of the interface unit 11. Overcurrent flows or a signal input / output via C13 flows into the output buffer of the interface unit 11 and overcurrent flows. Such an overcurrent becomes noise and increases wasteful power consumption. Further, such noise deteriorates the sensitivity and communication characteristics at the non-contact interface via the antenna 10. When the supply of the operating power supply Vdd to the interface controller 7 is stopped, the output power of the output buffer of the interface section 11 connected to the wirings L1 to L4 is indefinite by supplying the operating power supply Vcc-IC for the IC card microcomputer 9 from the C15 to the interface section 11. Cancel the condition.

In order to eliminate the indefinite state, for example, the output buffer connected to the wirings L1 to L4 is controlled to be in a high impedance state in response to the supply stop of the power supply Vdd.

FIG. 4 illustrates an output buffer that can be controlled to a high impedance state in response to the stop of the supply of the power supply Vdd. The output buffer 15 includes, for example, a series circuit of a CMOS inverter 16 using Vdd as an operation power supply and a CMOS clocked inverter 17 using Vcc-IC as an operation power

supply. The CMOS clocked inverter 17 mainly includes a series circuit of p-channel MOS transistors Qp1 and Qp2 and n-channel MOS transistors Qn3 and Qn4, and includes an inverter 18 and a power supply voltage detector 19 that switch-control the MOS transistors Qp1 and Qn4. The power supply voltage detector 19 is a detection signal that is set to the high level of the Vcc-IC level when the power supply voltage Vdd is turned on and exceeds the operation guarantee voltage, and to the low level that is the ground voltage Vss of the circuit when the supply of the power supply voltage Vdd is cut off. 20 is output. The inverter 18 uses Vcc-IC as an operation power supply. As a result, when Vdd is supplied with Vcc-IC turned on, the clocked inverter 17 is enabled for output operation, and when supply of Vdd is cut off, the clocked inverter 17 is controlled to a high impedance state. Is done. The power source Vdd is connected to the power source of the clocked inverter 17 through the high resistance R1 in order to stabilize the operation when the Vcc-IC is shut off.

In FIG. 4, it is considered that the levels of Vdd and Vcc-IC are different and Vdd ≦ Vcc-IC. That is, when the logic threshold voltage (VTL) of the inverter 16 is Vdd / 2, the logic threshold voltage of the clocked inverter 17 is also set to Vdd / 2. In short, the output buffer 15 has a level shift function for performing a level shift between the signal belt by the power supply voltage Vdd and the signal level by the power supply voltage Vcc-IC.

Note that the output indefinite state of the interface unit when the power supply Vdd is shut off is not limited to the high impedance control in the output buffer 15 having the level shift function, and as illustrated in FIG. A bus switch 21 that is turned off when the power supply Vdd is cut off is used for disconnection from the card microcomputer, and a circuit using the differential amplifier shown in FIG. In the circuit of FIG. 6, the power source Vdd is connected to the power source of the differential amplifier via the high resistance R1 in order to stabilize the operation when the Vcc-IC is shut off.

FIG. 7 shows a second configuration example of MRYC5. In contrast to FIG. 1, the separation switch circuit 12 is composed of only the switch SW1. When the interface controller 7 communicates with the IC card microcomputer 9 in the 1-bit mode or the 4-bit mode, a switch that is cut off by the control of the interface controller 7 and separates the connection with the external connection terminals C10, C11, and C13 is unnecessary. It was. Functions of data terminals DAT4 to DAT7 assigned to the external connection terminals C10 to C13 in the 8-bit mode and functions of terminals Vcc, I / O, CLK, and RES connected to the wirings L1 to L4 in the 1-bit mode or the 4-bit mode The selection based on the difference may be performed outside the MRYC 5. Other configurations are the same as those in FIG.

FIG. 8 shows a third configuration example of MRYC5. In contrast to the configuration of FIG. 1, the operation power supply to the IC card microcomputer is performed only at the terminal C15. The switch SW1 becomes unnecessary. Although not shown in particular, it is possible to employ a configuration in which the entire separation switch circuit 12 is eliminated by combining FIGS.

FIG. 9 shows a fourth configuration example of MRYC5. The MRYC 5 shown in the figure does not show the separation switch circuit 12, but has only the IC card microcomputer 9 having the connection relationship shown in FIG. 7 or 8 and the contact interface, and only the interface unit 11 of the interface controller 7. Another IC card microcomputer 24 to be connected is mounted. Other configurations are the same as those in FIG. In this embodiment, the IC card microcomputer 24 operates as a coprocessor of the interface controller 7 and does not operate independently by the IC card microcomputer 24 alone.

FIG. 10 shows a fifth configuration example of MRYC5. The MRYC 5 shown in the figure is configured by further mounting another IC card microcomputer 25 having only a non-contact interface with respect to the configuration of FIG. 7 or FIG. Supply of operating power to the IC card microcomputer 9 is performed by C12 (Vcc-ic), and supply of operating power to the IC card microcomputer 25 is performed by C15 (Vcc-IC). Since the IC card microcomputer 25 having a non-contact interface can use the induced electromotive force generated by the electromagnetic wave crossing the antenna 11 as its operation power supply, the operation power supply from the C15 to the IC card microcomputer 25 is not essential. When the operation of the IC card microcomputer 25 is stabilized by stabilizing the power supply, the operation power supply from the C15 is meaningful.

FIG. 11 illustrates details of the interface controller 7. The interface controller 7 includes a host interface circuit 30, a microcomputer 31, a flash controller 32, a buffer controller 33, a buffer memory 34, and an interface unit 11. The buffer memory 34 is composed of DRAM (Dynamic Random Access Memory) or SRAM (Static Random Access Memory). An IC card microcomputer 9 is connected to the interface circuit 11. The microcomputer 31 includes a CPU (central processing unit) 37, a program memory (PGM) 38 that holds an operation program for the CPU 37, a work memory (WRAM) 39 that is used as a work area for the CPU 37, and the like. The control program of the interface control mode corresponding to the MMC specification is held by the PGM 38.

When the host interface circuit 30 issues a memory card initialization command, it enables the microcomputer 31 to execute a control program in an MMC interface control mode by an interrupt. The microcomputer 31 controls the external interface operation by the host interface circuit 30 by executing the control program, controls the access (write, erase and read operations) and data management to the flash memory 8 by the flash controller 32, and the buffer. The controller 33 controls format conversion between a data format specific to the memory card and a common data format for the memory.

The buffer memory 34 temporarily holds data read from the flash memory 8 or data written to the flash memory 8. The flash controller 32 operates the flash memory 8 as a hard disk compatible file memory and manages data in units of sectors.

The flash controller 32 includes an ECC circuit (not shown), adds an ECC code when storing data in the memory, and performs error detection / correction processing using the ECC code on the read data.

FIG. 12 illustrates details of the IC card microcomputer 9. The IC card microcomputer 9 includes a CPU 41, a RAM (random access memory) 42 as a work RAM, a timer 43, an EEPROM (electrically erasable and programmable read only memory) 44, a coprocessor unit 45, a mask. A ROM (Read Only Memory) 46, a system control logic 47, an input / output port (I / O port) 48, a data bus 49, an address bus 50, and an RF unit 51 are provided.

The mask ROM 46 is used to store an operation program (encryption program, decryption program, interface control program, etc.) and data of the CPU 41. The RAM 42 serves as a work area for the CPU 41 or a temporary storage area for data, and is composed of, for example, SRAM (Static Random Access Memory) or DRAM (Dynamic Random Access Memory). When an IC card command is supplied to the I / O port 48, the system control logic 47 decodes it and causes the CPU 41 to execute a processing program necessary for executing the command. That is, the CPU 41 accesses the mask ROM 46 with an address instructed by the system control logic 47, fetches an instruction, decodes the fetched instruction, and performs operand fetch and data operation based on the decoding result. The coprocessor unit 45 performs a remainder calculation process in RSA or elliptic curve cryptographic calculation according to the control of the CPU 41. The I / O port 48 has a 1-bit input / output terminal I / O, and is used both for data input / output and external interrupt signal input. The I / O port 48 is coupled to a data bus 49, to which the CPU 41, RAM 42, timer 43, EEPROM 44, coprocessor unit 45 and the like are connected. The system control logic 47 controls the operation mode and interrupt of the IC card microcomputer 9 and further includes a random number generation logic used for generating an encryption key. When the reset operation is instructed by the reset signal RES, the IC card microcomputer 9 is initialized, and the CPU 41 starts executing instructions from the top address of the program in the mask ROM 46. The IC card microcomputer 9 is operated in synchronization with the clock signal CLK.

The EEPROM 44 is electrically erasable and writable, and is used as an area for storing data such as ID information and authentication certificate used to identify an individual. A flash memory or a ferroelectric memory may be employed in place of the EEPRPM 44. The IC card microcomputer 9 supports one or both of a contact interface using an external connection terminal as an interface with the outside and a non-contact interface using an antenna. The RF unit 51 for performing a non-contact interface has chip antenna terminals TML1 and TML2. When power is supplied from the RF unit 51 via the antenna, or when a non-contact interface is selected via the internal bus by the system control logic 47, the RF unit 51 causes the antenna to transmit a predetermined electromagnetic wave (for example, a high-frequency wave). An operating power source is generated using an induced electromotive force generated by crossing a magnetic flux or a microwave as an operating power

source, and an internal clock signal CLK based on the induced current corresponding to the frequency of the predetermined radio wave, the predetermined radio wave internal data separated by the RF unit 51 and further a reset signal RES are generated, and information is input / output from the antenna in a non-contact manner. In the IC card microcomputer 9, the RF unit 51 that operates via the non-contact interface is preferably configured by a small-scale circuit independent of the IC card operating CPU 41 that operates via the contact interface. The RF unit 51 includes a circuit necessary for contactless card operation, such as a contactless card processor, a memory used for a control program area and a work area of the processor, and an RF transmission / reception and power supply circuit unit. As described above, the RF unit 51 is composed of an independent small-scale circuit such as a processor function and its control program. Therefore, for example, even in an environment where power supply via a contact terminal cannot be obtained, external induction it becomes easy to operate the circuit with electric power. The RF unit 51 can also input and output data between the non-contact interface part and the contact interface part via the internal data bus 49 and the address bus 50.

The security processing operation in MRYC5 will be described. For example, user identification information is stored in the secure area of the flash memory 8. When downloading the content data, the license information encrypted with the user identification information as a secret key is downloaded together. A decryption key for decrypting the content data is included in the license information, and the license information is decrypted using the user identification information as the decryption key. This protects the copyright of the content data. Such security processing is performed by program control by the microcomputer 31.

A security process by the IC card microcomputer 9 will be described. For example, the IC card microcomputer 9 realizes an authenticated function by an evaluation / certification organization of ISO / IEC15408 that can be used for an electronic payment service or the like. The EEPROM 44 has a predetermined authentication certificate, and when there is an authentication request from the host, the authentication certificate is sent, and subsequent communication processing is made possible on the condition that authentication is obtained for this. . Such a security processing operation program is stored in the mask ROM 46. It is desirable from the viewpoint of security that the authentication process by the IC card microcomputer 9 is performed in an environment closed inside the IC card microcomputer 9. In this respect, it is meaningful to perform only an external interface through the external connection terminals C10 to C13 or an antenna by turning on only the power source of the IC card microcomputer 9. If there is no security problem in terms of use or technology, it is possible to perform security processing via the interface controller 7. Further, in the process from the manufacture of MRYC to the product shipment, various application software can be easily written to the IC card microcomputer 9 and the card issuance process can be performed via the external connection terminals C10 to C13.

For example, as described above, when the IC card microcomputer 9 has been authenticated by an ISO / IEC15408 evaluation / certification organization that can be used for an electronic payment service or the like, MRYC5 is inserted into a card holder such as a cash card, credit card, or commuter pass, These card functions can be realized using a non-contact interface.

Considering that the IC card microcomputer 9 is used for high-level security processing such as electronic payment, a power-on reset that initializes all internal states against the abnormal state of the IC card microcomputer 9 is sent to the interface controller 7 and the like. It is more likely to be performed more frequently. Considering this, since the IC card microcomputer 9 has dedicated power supply terminals C12 (Vcc-ic) and C15 (Vcc-IC), the IC card microcomputer 9 can be freely operated without resetting the entire MRYC5. Power-on reset is possible. As a result, the security of MRYC 5 can be improved while ensuring security.

《MRYC external connection terminal arrangement》
FIG. 13 shows an appearance when the MRYC 5 is sealed in an MMC standard half size package. FIG. 14 shows an external appearance when the MRYC 5 is sealed in a standard size package of the MMC standard. Both drawings clearly show the arrangement of the external connection terminals, and both arrangements are equal. The function assignment of each of the terminals C1 to C16 is as described with reference to FIG. C1 to C7 correspond to the primitive MMC standard. C8 to C9 are expansion terminals for 4-bit mode, C10 to C13 are IC card microcomputer contact interfaces and expansion terminals for 8-bit mode, C14 and C16 are expansion terminals for external antenna connection, and C15 is dedicated to the IC card microcomputer This is an expansion terminal for power supply. C1 to C16 have a staggered arrangement in which the arrangement in the column direction is shifted between adjacent columns before and after the insertion direction (arrow X direction) of the memory card. The first column is C1 to C7. C8 to C13 constitute a second row spaced from the first external connection terminal row. The sizes of the external connection terminals C10 to C13 are the same as the sizes of the external connection terminals C1 to C7 within a certain range. The external connection terminal of C8 is arranged in the first row and extends to a position adjacent to the terminal C7 at one end in the row direction of the connector terminal row in the row direction, and the external connection terminal of C9 is arranged in the first row. It is arranged and extends to a position adjacent to the terminal C1 of the terminal row, partially overlapping in the row direction. The first row of external connection terminal rows and the second row of external connection terminal rows are arranged in a staggered manner with the row direction arrangement of the external connection terminals being shifted from each other in the row direction, except for C4 and C15. Yes.

Due to the zigzag arrangement, the card slot (not shown) in which the MRYC 5 is mounted is made into a multi-terminal by a relatively simple configuration in which a large number of slot terminals (pins) are alternately arranged in parallel with different projection amounts. Can respond. In view of the increase in the number of terminals, terminals C14 to C16 newly provided in the area between the C11 and C12 in the rear row are also arranged in a staggered manner

When the antenna connection terminals C14 and C16 that can be connected to the high-frequency antenna 10 for the non-contact interface are provided as the external connection terminals, the antenna connection terminals C14 and C16 are connected to the external connection terminal C15 as the IC card microcomputer dedicated power supply terminal. Adjacent to the external connection terminal C4 for supplying power Vdd. Such antenna connection terminals C14 and C16 are used for connection of an external high-frequency antenna in order to increase the sensitivity of the non-contact interface in the IC card microcomputer. The voltage applied to the antenna connection terminals C14 and C16 is relatively high and the frequency is high. Therefore, the routing of the wiring to the connection terminals such as signals and clocks on the wiring board of the MRYC 5 and the routing of the wiring to the connection terminals C14 and C16 of the external antenna are complicated and may be close to each other or straddle. When the number increases, noise is superimposed on the signal line and the clock wiring due to crosstalk or induction. Alternatively, noise due to crosstalk or induction from the signal line or the clock wiring is superimposed on the high frequency signal received from the external high frequency antenna, and an error may occur in the data separated by the RF unit 51. Since the antenna connection terminals C14 and C16 are arranged adjacent to the external connection terminal C15 serving as the IC card microcomputer dedicated power supply terminal and in the vicinity of the external connection terminal C4 for supplying the power Vdd, the arrangement minimizes the generation of noise. The arrangement is suitable for suppressing.

The shape of the external connection terminal described in FIGS. 13 and 14 can be partially changed as shown in FIG. Here, the shapes of C9 and C8 are shortened. This is intended to correspond to the card slot in which the position of the terminal contacting C8 and C9 of the card slot is in the first row. Also, as illustrated in FIG. 16, the number of external connection terminals can be reduced. The external connection terminals C8 and C9 are abolished, and the terminal arrangement takes into account the MMC standard 1-bit mode and IC card microcomputer contact interface support. 15 and 16, the staggered arrangement of the external connection terminals and the arrangement relationship between the antenna connection terminals C14 and C16 and the IC card microcomputer dedicated power supply terminal C15 are followed as they are.

《Insertion into card slot and power supply》
23 to 26 show the process of inserting a memory card into the card slot and the power supply to the memory card obtained by considering the process.

FIG. 23 shows a memory card 5 and a card slot 70 into which the memory card 5 is inserted. The card slot 70 has a sensor 71 for detecting the insertion of the memory card 5 and external connection terminals C1 to C16 of the memory card 5. Terminals 72 to 87 are provided in contact with each other, and an external antenna 88 is connected to the terminals 85 and 87.

FIG. 24 shows a first process in which the memory card 5 is inserted into the card slot 70. In the stage of the first process, the terminal 86 connected to the terminal C15 is in contact with the terminal C4 of the memory card 5, and the terminals 79 to 85, 87 of the card slot 70 are the terminals C1 to C1 of the first row of the memory card 5 This indicates that there is a possibility of contact with C9. A terminal C15 of the memory card 5 is a terminal for supplying a potential Vcc-IC and is supplied with the same or higher potential as the power supply Vdd supplied to the interface controller 7 and the flash memory 8. In this state, the Vcc-IC is supplied to the interface controller 7 and the flash memory 8, and the terminals 79 to 85 and 87 of the card slot 70 are brought into contact with the terminals C1 to C9 of the first column of the memory card 5, so that an electrical circuit is obtained. May be formed. Since the external antenna 88 generates a potential in accordance with an external electric field, the terminals 85 and 87 may come into contact with terminals other than the antenna connection terminals C14 and C16, and this potential may be applied to the interface controller 7.

FIG. 25 shows a second process in which the memory card 5 is inserted into the card slot 70. In the stage of the second process, the terminals 79 to 85 and 87 of the card slot 70 do not contact the terminals C1 to C9 of the first row of the memory card 5, but the terminals 75 and 86 of the card slot 70 are not connected to the memory card 5. There is a possibility that Vcc-IC is supplied to a circuit (not shown) for supplying Vdd to the terminal 75, which is connected via the external connection terminal C4. Further, when the terminal 75 and the terminal 86 are in contact with the terminal C4, the Vcc-IC is supplied to the interface controller 7 and the flash memory 8, and the terminals 72 to 74 and 76 to 80 are in contact with the terminals C1 to C3 and C5 to C9. Therefore, there is a possibility that a circuit is electrically formed.

FIG. 26 shows a third process in which the memory card 5 is inserted into the card slot 70. In the stage of the third process, the terminals 72 to 87 of the card slot 70 and the terminals C1 to C16 of the memory card 5 are appropriately connected.

The problems that may occur in the process shown in FIGS. 24 and 25 include a solution in the memory card 5 and a solution in the host device having the card slot 70.

As a solution in the memory card 5, a power circuit is provided between the terminal C4, the interface controller 7 and the flash memory 8, and after detecting that the power Vdd is supplied from the terminal C4, the interface controller 7 In addition, supply of operating power to the flash memory 8 may be started, and the terminals C1 to C13 may be connected to the interface controller 7.

On the other hand, a solution in the host device can be solved by starting the supply of the Vcc-IC and the supply of the potential generated in the external antenna 88 in the third process. In other words, after the sensor 71 detects that the terminals 72 to 87 of the card slot 70 are not in process contact with the terminals C1 to C16 of the memory card, the supply of Vcc-IC may be started. The terminals of the memory card 5 and the card slot 70 are formed so that the terminals 85 and 87 of the card slot 70 do not cause stepwise contact with the terminals of the memory card 5, or between the external antenna 88 and the terminals 85 and 87. A switch circuit that can be electrically connected / disconnected is provided, and after the sensor 71 detects that no process contact is made, the external antenna 88 may be electrically connected to the terminals 85 and 87.

The potentials Vdd, Vss1, and Vss2 may be constantly supplied, or may be started after the sensor 71 detects that the memory card 5 has been inserted into the card slot 70. This is because the terminals 74 and 77 of the card slot 70 are supply terminals for a reference potential, and there is no process contact in the illustrated structure. Further, since the terminal 75 is a supply terminal for Vdd which is the same potential as or lower than the Vcc-IC, even if it is connected to the terminal 86 via the terminal C4, a circuit (not shown) for supplying the Vcc-IC. This is because it is considered that no particular problem will occur even if Vdd is supplied to.

<Pulling out from card slot and supplying power>
Although not shown, the case where the memory card 5 is pulled out from the card slot 70 will be considered. In this case, when the memory card 5 is pulled out from the card slot 70 during the data erasing or data writing operation in the flash memory 8, the supply of the operating power to the flash memory 8 is interrupted, which is undesirable. In some cases, the memory card 5 itself cannot be recognized due to data corruption or a state called depletion. In order to avoid such a situation, when the host device detects that the memory card 5 is pulled out from the card slot 70 by the sensor 71, the host device notifies the memory card 5 via a predetermined terminal, and The potential Vdd may be supplied from the terminal 86. Accordingly, the potential Vdd can be supplied to the terminal C4 from the second process of FIG. 25 to the first process of FIG. Further, in order to increase the contact time of the terminal 74 with the terminal C3, specifically, the terminal 74 is made as long as the terminal 84 and the contact point with the terminal C3 is made longer. It becomes possible to maintain an electrical connection. As a result, the memory card 5 can complete the writing of data, or can secure a time for performing at least the process of avoiding the depletion state in response to the detection notification from the sensor 71.

《Chip stack structure》
FIG. 17 is a plan view showing a stack mounting structure of the interface controller 7, the flash memory 8, and the IC card microcomputer 9 each formed as an individual semiconductor integrated circuit chip, and FIG. 18 is a longitudinal section of the mounting structure. Shown schematically. External connection electrodes C1 to C16 are formed on one surface of a wiring substrate 60 such as a glass epoxy resin substrate on which a required wiring layer is formed, and a number of bonding pads 61 connected to the required wiring are formed on the other surface. ing. The bonding pad 61 is formed of a conductive pattern such as aluminum, copper or iron alloy. The external connection electrodes C1 to C16 are formed by applying gold plating, nickel plating, palladium plating or the like to a conductive pattern such as aluminum, copper or iron alloy. The connection between the external connection electrodes C1 to C16 and the bonding pad 61 is performed by a wiring pattern (not shown) on the wiring board 60 and a through hole penetrating the wiring board 60 in the thickness direction. On the wiring board 60, the two flash memories 8 made into individual chips are overlapped with each other, and the interface controller 7 made into a single chip is overlaid thereon. The wiring substrate 60 and the chip, and the chip and the chip are bonded by the die bond agent 62. In the stacked three chips, the electrode pads 64 are arranged along the sides in the same direction in the stacked state, and the bonding pads 61 corresponding to the wiring board are wired to the arranged electrode pads 64 by the bonding wires 65. Bonded. Since the bonding electrode pads 64 of the three stacked chips are arranged along the sides in the same direction in the stacked state, the bonding wire 65 can be shortened and the interference of the wire 65 is also reduced. The single-chip IC card microcomputer 9 is die-bonded to the wiring board 60 as a single chip, and the chip electrode pads are bonded to the corresponding bonding pads of the circuit board. The chips stacked on the wiring board 60 are sealed with a resin mold or the like. Reference numeral 66 denotes a mold sealing region.

FIG. 19 shows a structure in which the IC card microcomputer 9 is stacked in two chips with respect to the stack structure shown in FIGS. If the chips of the two IC card microcomputers 9 are the same type and the same size, the electrode pads on the chips are hidden if they are directly stacked. In that case, a spacer dummy chip 67 may be sandwiched between them. Of course, the dummy chip 67 is smaller than the IC card microcomputer chip.

FIG. 20 is a plan view showing still another stack mounting structure of the interface controller 7, the flash memory 8, and the IC card microcomputer 9 each formed as an individual semiconductor integrated circuit chip, and FIG. 21 shows the mounting structure. A longitudinal section is schematically shown. The difference from FIGS. 17 to 19 is that two flash memories 8 made into individual chips are stacked, and an interface controller 7 and an IC card microcomputer 9 made into individual chips are stacked separately. Other configurations are the same as those of the stack structure of FIGS. 17 and 18, and members having the same functions are denoted by the same reference numerals and detailed description thereof is omitted.

FIG. 22 shows a structure in which two IC card microcomputers 9 are stacked with respect to the stack structure shown in FIGS. Since the chips of the two IC card microcomputers 9 are the same type and the same size, they are not directly stacked and a spacer dummy chip 67 is sandwiched between them. The flash memory 8 can be a chip stack of one chip or three or more chips as required.

Although the invention made by the present inventor has been specifically described based on the embodiments, it is needless to say that the present invention is not limited thereto and can be variously modified without departing from the gist thereof.

For example, the present invention can be widely applied not only to MMC standard memory cards but also to multi-function memory cards that comply with other standards. Therefore, the function, arrangement, number, etc. of the external connection terminals can be changed as appropriate. The memory is not limited to the flash memory, and may be a memory of other storage format such as a ferromagnetic memory. The security controller is not limited to the one that realizes an authenticated function by an evaluation / certification organization of ISO / IEC15408. It may be a microcomputer that performs simple encryption / decryption.

It is a block diagram which shows an example of the memory card based on this invention. It is explanatory drawing which shows the outline of communication portable terminal devices, such as a mobile telephone to which the memory card based on this invention is applied. It is explanatory drawing which illustrates the function allocation of the external connection terminal according to the card mode of a memory card. It is a circuit diagram which illustrates the output buffer which can be controlled to a high output impedance state in response to a power supply stop. It is explanatory drawing which shows the example which employ | adopted the bus switch in order to eliminate the output indefinite state of the said interface part at the time of power supply interruption. It is a circuit diagram which shows the circuit using a differential amplifier for level shift. It is a block diagram which shows the 2nd structural example of the memory card based on this invention. It is a block diagram which shows the 3rd structural example of the memory card based on this invention. It is a block diagram which shows the 4th structural example of the memory card based on this invention. It is a block diagram which shows the 5th structural example of the memory card based on this invention. It is a block diagram which illustrates the detail of an interface controller. It is a block diagram which shows the specific example of a dual way IC card microcomputer. It is explanatory drawing which shows an external appearance when the memory card based on this invention is sealed in the package of the standard size of MMC standard. It is explanatory drawing which shows an external appearance when the memory card based on this invention is sealed in the half size package of a MMC specification. It is explanatory drawing which shows the example which changed the part with respect to the shape of the external connection terminal of FIG.13 and FIG.14. It is explanatory drawing which shows the example which reduced the number of external connection terminals with respect to the external connection terminal of FIG.13 and FIG.14. It is a top view which illustrates the stack mounting structure of the said interface controller, flash memory, and IC card microcomputer which were each made into the semiconductor integrated circuit chip | tip separately. It is a longitudinal cross-sectional view of the mounting structure of FIG. FIG. 19 is a longitudinal sectional view showing a structure in which two IC card microcomputers are stacked on the stack structure of FIGS. 17 and 18; FIG. 11 is a plan view showing still another stack mounting structure of the interface controller, the flash memory, and the IC card myco that are each made into individual semiconductor integrated circuit chips. It is a longitudinal cross-sectional view with respect to the mounting structure of FIG. FIG. 22 is a longitudinal sectional view showing a structure in which two IC card microcomputers are stacked on the stack structure of FIGS. 20 and 21. It is explanatory drawing which shows the card slot in which a memory card and a memory card are inserted. It is explanatory drawing which shows the 1st process in which the memory card of FIG. 23 is inserted in a card slot. It is explanatory drawing which shows the 2nd process in which the memory card of FIG. 23 is inserted in a card slot. It is explanatory drawing which shows the 3rd process in which the memory card of FIG. 23 is inserted in a card slot.

Explanation of symbols

DESCRIPTION OF SYMBOLS 5 Memory card 7 Interface controller 8 Flash memory 9 Dual way IC card microcomputer 10 Antenna 11 Interface part 12 Separation switch circuit C4 Vdd supply external connection terminal (first external connection terminal)
C12 Vcc-ic supply external connection terminal C15 Vcc-IC supply external connection terminal (second external connection terminal)
C11 CLK-ic assignment external connection terminal (third external connection terminal)
C13 I / O-ic assignment external connection terminal (fourth external connection terminal)
C10 RES-ic assignment external connection terminal (fifth external connection terminal)
C14, C16 External connection terminal for antenna connection 12 Separation switch circuit 15 Output buffer 17 Clocked inverter 24 Contact interface type IC card microcomputer 25 Non-contact interface type IC card microcomputer 60 Circuit board 61 Electrode (bonding pad) on wiring board
64 Electrode Pad on Semiconductor Chip 65 Bonding Wire

Patent Citations (22)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
JPS62165293A *	1985-10-31	1987-05-15	Toshiba Corp	Reading/writing device for portable recording medium
KR970008188B1	1993-04-08	1997-05-21	가부시끼가이샤 히다찌세이사꾸쇼	Control method of flash memory and information processing apparatus using the same
WO1996033814A2 *	1995-06-02	1996-12-05	Philips Electronics N.V.	Chip-card
JPH0962584A *	1995-08-24	1997-03-07	Mitsubishi Electric Corp	Data processor
FI104920B *	1996-10-31	2000-04-28	Nokia Mobile Phones Ltd	Electronic device, card interface and expansion card
IL119943A *	1996-12-31	2000-11-21	On Track Innovations Ltd	Contact/contactless data transaction card
ES2157099T3 *	1998-02-17	2001-08-01	Infineon Technologies Ag	DATA SUPPORT FOR OPERATION BOTH WITHOUT CONTACT AND WITH CONTACT.
JP3922501B2 *	1998-12-10	2007-05-30	ソニー株式会社	Power supply device and card-like storage medium
JP2000322544A *	1999-05-13	2000-11-24	Toshiba Corp	Portable electronic device
JP3833939B2 *	1999-06-29	2006-10-18	株式会社ルネサステクノロジ	Compound IC card
JP4423711B2 *	1999-08-05	2010-03-03	ソニー株式会社	Semiconductor memory device and semiconductor memory device operation setting method
JP3349998B2 *	1999-09-07	2002-11-25	エヌイーシーマイクロシステム株式会社	Data processing device and operation control method thereof

US6889342B1 *	1999-10-27	2002-05-14	Terence T. Flyntz	Multi-level secure computer with token-based access control
JP4058704B2 *	2000-01-05	2008-02-27	株式会社東芝	IC card with built-in wireless interface function, antenna module, information processing device
CN1218276C	2000-04-28	2005-09-07	株式会社日立制作所	IC card
JP2002109484A *	2000-09-26	2002-04-12	Toshiba Corp	Portable information equipment
JP3625187B2 *	2000-12-18	2005-03-02	シャープ株式会社	Card type wireless communication apparatus and wireless communication system using the same
JP2002342731A *	2001-05-16	2002-11-29	Matsushita Electric Ind Co Ltd	Composite ic card
US7188514S2 *	2001-06-04	2007-02-27	Renesas Technology Corp.	Memory card
US20050212690A1 *	2002-08-26	2005-09-29	Dai Nippon Printing Co., Ltd.	Sim, sim holder, ic module, ic card and ic card holder
CN1402508A *	2002-09-19	2003-03-12	无敌科技(西安)有限公司	Electronic device capable of direct access of SIM card data, and operation method thereof
US7237719B2 *	2003-09-03	2007-07-03	Stmicroelectronics, Inc.	Method and apparatus for a USB and contactless smart card device

* Cited by examiner, † Cited by third party

Cited By (53)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
WO2004047084A2 *	2002-11-18	2004-06-03	Storcard, Inc.	Secure transaction card with a large storage volume
TWI239482B *	2004-01-06	2005-09-11	C One Technology Corp Ltd	Peripheral contact type small electronic card
KR101044796B1 *	2004-01-13	2011-06-29	삼성전자주식회사	Portable data storage apparatus
US8161524B2 *	2005-01-13	2012-04-17	Samsung Electronics Co., Ltd.	Method and portable storage device for allocating secure area in insecure area
US8181266B2 *	2005-01-13	2012-05-15	Samsung Electronics Co., Ltd.	Method for moving a rights object between devices and a method and device for using a content object based on the moving method and device
CA2594670C	2005-01-21	2014-12-23	Certicom Corp.	Elliptic curve random number generation
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
JP2007065956A *	2005-08-31	2007-03-15	Renesas Technology Corp	Memory card
FR2892212A1 *	2005-10-17	2007-04-20	St Microelectronics Sa	NFC READER HAVING PASSIVE OPERATING MODE WITH LOW POWER CONSUMPTION
JP4930970B2 *	2005-11-28	2012-05-16	ルネサスエレクトロニクス株式会社	Multi-chip module
JP4843447B2 *	2006-03-31	2011-12-21	株式会社東芝	Semiconductor device and memory card using the same
TW200743035A *	2006-05-09	2007-11-16	Siliconware Precision Industries Co Ltd	Circuit card module and method for fabricating the same
JPWO2007141999A1 *	2006-06-02	2009-10-22	株式会社ルネサステクノロジ	Semiconductor device
JP4969934B2 *	2006-07-19	2012-07-04	株式会社東芝	Semiconductor device
US7872356B2 *	2007-05-16	2011-01-18	Qualcomm Incorporated	Die stacking system and method
EP2003593B1 *	2007-05-18	2009-11-25	Partitalia S.r.L.	Apparatus for monitoring environmental parameters
JP2009053970A *	2007-08-28	2009-03-12	Toshiba Corp	Semiconductor device
JP2009054061A *	2007-08-29	2009-03-12	Renesas Technology Corp	Semiconductor device
JP4857225B2 *	2007-09-10	2012-01-18	パナソニック株式会社	IC card and mobile phone terminal

US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US8045333B2	2008-01-14	2011-10-25	Rosemount Inc.	Intrinsically safe compliant circuit element spacing
JP2010021449A *	2008-07-11	2010-01-28	Toshiba Corp	Semiconductor device
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US20100033310A1 *	2008-08-08	2010-02-11	Narendra Siva G	Power negotation for small rfid card
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
KR20100071522A *	2008-12-19	2010-06-29	삼성전자주식회사	High-density and multifunctional pop-type multi chip package architecture
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
KR101555637B1 *	2009-03-27	2015-09-24	삼성전자주식회사	Smart card
JP5198379B2 *	2009-07-23	2013-05-15	株式会社東芝	Semiconductor memory card
CN101661638B *	2009-09-07	2013-09-11	上海申远投资管理有限公司	Safe multi-interface certificate mobile inquiry system and method thereof
US20110145465A1 *	2009-12-14	2011-06-16	Kabushiki Kaisha Toshiba	Semiconductor memory card
JP2011134174A *	2009-12-25	2011-07-07	Sony Corp	Card-type peripheral device and card system
KR20120011974A *	2010-07-29	2012-02-09	삼성전자주식회사	Smart card supporting pluarlity of interfaces and interfacing method thereof
US8885334B1 *	2011-03-10	2014-11-11	Xilinx, Inc.	Computing system with network attached processors
JP2012203928A *	2011-03-23	2012-10-22	Toshiba Corp	Nonvolatile semiconductor storage device and ic card
JP5734774B2	2011-07-11	2015-06-17	株式会社東芝	Electronics
CN103325409B *	2012-03-22	2016-03-23	群联电子股份有限公司	The storage card of tool intelligent card function and power control method thereof and power control circuit
JP5989097B2 *	2012-07-03	2016-08-02	ルネサスエレクトロニクス株式会社	Semiconductor device
JP5942756B2 *	2012-09-28	2016-06-29	株式会社ソシオネクスト	Protection circuit, interface circuit, and communication system
CN105100303A *	2014-05-22	2015-11-25	中兴通讯股份有限公司	Power supply protecting device and terminal equipment
USD736212S1 *	2014-07-01	2015-08-11	Samsung Electronics Co., Ltd.	Memory card
USD736213S1 *	2014-07-01	2015-08-11	Samsung Electronics Co., Ltd.	Memory card
USD739856S1 *	2014-07-30	2015-09-29	Samsung Electronics Co., Ltd.	Memory card
USD736216S1 *	2014-07-30	2015-08-11	Samsung Electronics Co., Ltd.	Memory card
WO2016189661A1 *	2015-05-26	2016-12-01	株式会社 日立製作所	Terminal function allocation device and terminal function allocation method
CN105094699B *	2015-07-15	2018-10-02	浪潮(北京)电子信息产业有限公司	A kind of Cloud Server storage system
US10636753B2	2015-07-29	2020-04-28	STATS ChipPAC Pte. Ltd.	Antenna in embedded wafer-level ball-grid array package
US9806040B2 *	2015-07-29	2017-10-31	STATS ChipPAC Pte. Ltd.	Antenna in embedded wafer-level ball-grid array package
USD783621S1 *	2015-08-25	2017-04-11	Samsung Electronics Co., Ltd.	Memory card
USD783622S1 *	2015-08-25	2017-04-11	Samsung Electronics Co., Ltd.	Memory card
USD772232S1 *	2015-11-12	2016-11-22	Samsung Electronics Co., Ltd.	Memory card

USD773467S1 *	2015-11-12	2016-12-06	Samsung Electronics Co., Ltd.	Memory card
KR20190083569A	2018-01-04	2019-07-12	삼성전자주식회사	Memory card and electronic apparatus including the same

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
JP4412947B2	2010-02-10	Memory card
JP4447553B2	2010-04-07	Multifunction card device
US7946500B2	2011-05-24	Memory card and semiconductor device
US7296754B2	2007-11-20	IC card module
US7389937B2	2008-06-24	Card-shaped memory device incorporating IC card function
US7757958B2	2010-07-20	Card-shaped memory device incorporating IC card function, adapter for the same and host device
JP2007183776A	2007-07-19	Semiconductor device
JP2006236200A	2006-09-07	Card type storage device and host device thereof
JP4906135B2	2012-03-28	Memory card
JP2010086550A	2010-04-15	Semiconductor card device
JP4761479B2	2011-08-31	IC card
TWI309386B	2009-05-01	
JP4680259B2	2011-05-11	Semiconductor device

Priority And Related Applications

Child Applications (1)

Application	Priority date	Filing date	Relation	Title
JP2009242129A	2009-10-21	2009-10-21	Division	Memory card

Priority Applications (1)

Application	Priority date	Filing date	Title
JP2003316002A	2003-09-08	2003-09-08	Memory card

Applications Claiming Priority (9)

Application	Filing date	Title
JP2003316002A	2003-09-08	Memory card
EP09004573A	2004-07-14	Memory card
EP04254222A	2004-07-14	Memory card
DE602004023162T	2004-07-14	memory card
KR1020040059539A	2004-07-29	Memory card
CN200410065946943A	2004-07-30	Memory card
US10/912,289	2004-08-06	Memory card
TW093125528A	2004-08-26	
US11/945,745	2007-11-27	Memory card

Legal Events

Legal events

Date	Code	Title	Description
2006-09-01	A621	Written request for application examination	**Free format text**: JAPANESE INTERMEDIATE CODE: A621 **Effective date**: 20060831
2009-08-17	A977	Report on retrieval	**Free format text**: JAPANESE INTERMEDIATE CODE: A971007 **Effective date**: 20090817
2009-09-02	A131	Notification of reasons for refusal	**Free format text**: JAPANESE INTERMEDIATE CODE: A131 **Effective date**: 20090901
2009-10-22	A521	Written amendment	**Free format text**: JAPANESE INTERMEDIATE CODE: A523 **Effective date**: 20091021
2009-11-10	TRDD	Decision of grant or rejection written	
2009-11-18	A01	Written decision to grant a patent or to grant a registration (utility model)	**Free format text**: JAPANESE INTERMEDIATE CODE: A01 **Effective date**: 20091117
2009-11-19	A01	Written decision to grant a patent or to grant a registration (utility model)	**Free format text**: JAPANESE INTERMEDIATE CODE: A01
2009-11-26	A61	First payment of annual fees (during grant procedure)	**Free format text**: JAPANESE INTERMEDIATE CODE: A61 **Effective date**: 20091117
2009-11-27	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text**: PAYMENT UNTIL: 20121127 **Year of fee payment**: 3
2009-11-27	R150	Certificate of patent or registration of utility model	**Ref document number**: 4412947 **Country of ref document**: JP **Free format text**: JAPANESE INTERMEDIATE CODE: R150 **Free format text**: JAPANESE INTERMEDIATE CODE: R150
2010-10-04	R313	Request for change of ownership or part of ownership	**Free format text**: JAPANESE INTERMEDIATE CODE: R313111
2010-10-04	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text**: PAYMENT UNTIL: 20121127 **Year of fee payment**: 3
2010-10-13	R350	Written notification of registration of transfer	**Free format text**: JAPANESE INTERMEDIATE CODE: R350
2010-10-13	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text**: PAYMENT UNTIL: 20121127 **Year of fee payment**: 3
2012-10-04	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text**: PAYMENT UNTIL: 20121127 **Year of fee payment**: 3
2012-10-09	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text**: PAYMENT UNTIL: 20131127 **Year of fee payment**: 4
2015-09-15	S531	Written request for registration of change of domicile	**Free format text**: JAPANESE INTERMEDIATE CODE: R313531
2015-09-28	R350	Written notification of registration of transfer	**Free format text**: JAPANESE INTERMEDIATE CODE: R350
2020-11-27	LAPS	Cancellation because of no payment of annual fees	

Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

Patents CA2388007

Portable electronic authorization system and associated method

Abstract

I, o, e embodime, t a, apparatus i, cludes a housi, g; a user authe, ticator, supported by the housi, g, that authe, ticates a, ide, tity of a user; at least o, e memory, supported by the housi, g, that stores tra, sactio, i, formatio, for at least first a, d seco, d media; a, d at least o, e output, supported by the housi, g, that releases at least a portio, of the tra, sactio, i, formatio, to a poi, t-of-sale (POS) termi, al after the user authe, ticator has authe, ticated the ide, tity of the user. I, a, other embodime, t, a method i, volves steps of:
stori, g tra, sactio, i, formatio, for at least first a, d seco, d media i, a memory of a device;
receivi, g as i, put a user's selectio, of c, e of the at least first a, d seco, d media; displayi, g a visual i, dicatio, to the user regardi, g which of the at least first a, d seco, d media has bee, selected; a, d tra, sferri, g at least a portio, of the tra, sactio, i, formatio, from the device to a poi, t-of-sale (POS) termi, al.

Classifications

⊗ G07F7/1008 Active credit-cards provided with mea, s to perso, alise their use, e.g. with PIN-i, troductio, /compariso, system

View 13 more classifications

CA2388007A1

Ca, ada

Dow, load PDF Fi, d Prior Art Similar

Other languages: Fre, ch

Inventor: Todd O. Burger, Rob Cohe, , Karli, Jesse, , Joshua Hassol, Stuart Lipoff

Current Assignee : Chamelео, Network I, c

Worldwide applications

2000 ~~CA~~ EP US AU WO 2004 US

Application CA 2388007 events

1999-09-28 Priority to US15535699P

2000-09-28 Applicatio, filed by Chamelео, Network I, c., Todd O. Burger, Rob Cohe, , Karli, Jesse, , Joshua Hassol, Stuart Lipoff

2001-04-05 Publicatio, of CA2388007A1

Status Aba, do, ed

Show all eve, ts

Info: Pate, t citatio, s (72), Cited by (289), Legal eve, ts, Similar docume, ts, Priority a, d Related Applicatio, s

External links: Espace, et, Global Dossier, CIPO, Discuss

Claims (87)

Hide Dependent

1. A, apparatus, comprisi, g:
a housi, g;
a user authe, ticator, supported by the housi, g, that authe, ticates a, ide, tity of a user;
at least o, e memory, supported by the housi, g, that stores tra, sactio, i, formatic, for at least first a, d seco, d media; a, d at least c, e output, supported by the housi, g, that releases at least a portio, of the tra, sactio, i, formatio, to a poi, t-of sale (POS) termi, al after the user authe, ticator has authe, ticated the ide, tity of the user.

2. The apparatus of claim 1, wherei, the user authe, ticator comprises mea, s for authe, ticati, g the ide, tity of the user by a, alyzi, g a bio-metric feature of the user.

3. The apparatus of claim 2, further comprisi, g mea, s for authe, ticati, g the ide, tity of the user without releasi, g i, formatio, regardi, g the bio-metric feature of the user outside the housi, g.

4. The apparatus of claim 1, further comprisi, g at least o, e co, troller supported by the housi, g a, d coupled to each of the user authe, ticator, the at least c, e memory, a, d the at least o, e output, the at least o, e co, troller bei, g co, figured such that, after the user authe, ticator has authe, ticated the ide, tity of the user, the at least o, e co, troller causes the portio, of the tra, sactio, i, formatio, to be released to the POS
termi, al via the at least o, e output.

5. The apparatus of claim 1, wherei, the at least first a, d seco, d media are issued by first a, d seco, d differe, t a, d u, related media issuers.

6 The apparatus of claim 1, wherei, authe, ticatio, i, formatic, employed by the user authe, ticator to authe, ticate the ide, tity of the user is located withi, the housi, g a, d does , ot leave the housi, g whe, the user authe, ticator authe, ticates the ide, tity of the user.

7. The apparatus of claim 6, wherei, the authe, ticatio, i, formatio, i, cludes i, formatio, regardi, g a bio-metric feature of the user.

8 The apparatus of claim 1, wherei, the total volume co, sumed by the housi, g is less tha, five hu, dred cubic ce, timeters.

9. A method, comprisi, g steps of:
(a) stori, g tra, sactio, i, formatio, for at least first a, d seco, d media i, a memory of a device;
(b) usi, g the device to authe, ticate a, ide, tity of a user; a, d (c) after authe, ticati, g the ide, tity of the user with the device, tra, sferri, g at least a portio, of the tra, sactio, i, formatio, from the device to a poi, t-of sale (POS) termi, al.

10. The method of claim 9, wherei, the step (b) i, cludes a, alyzi, g a bio-metric feature of the user to authe, ticate the user's ide, tity.

11. The method of claim 9, wherei, the at least first a, d seco, d media are issued by first a, d secc, d differe, t a, d u, related media issuers.

12. The method of claim 9, wherei, authe, ticatio, i, formatio, employed by the user authe, ticator to authe, ticate the ide, tity of the user is located withi, a housi, g of the device, a, d wherei, the step (b) is performed without releasi, g the authe, ticatio, i, formatic, outside of the housi, g.

13. The method of claim 12, wherei, the authe, ticatio, i, formatic, i, cludes i, formatio, regardi, g a bio-metric feature of the user.

14. A, apparatus, comprisi, g:
a housi, g;

at least o, e memory, supported by the housi, g, that stores tra, sactio, i, formatic, for at least o, e media;
a user authe, ticator, supported by the housi, g, that authe, ticates a, ide, tity of a user of the apparatus; a, d at least o, e output, supported by the housi, g, that, after the user authe, ticator has authe, ticated the ide, tity of the user, releases a, embedded ide, tificatio, code of the apparatus from the housi, g that e, ables a device receivi, g the embedded ide, tificatio, code to authe, ticate the ide, tity of the apparatus.

15. The apparatus of claim 14, further comprisi, g at least o, e co, troller supported by the housi, g a, d coupled to each of the user authe, ticator, the at least o, e memory, a, d the at least o, e output, the at least o, e co, troller bei, g co, figured such that, after the user authe, ticator has authe, ticated the ide, tity of the user, the at least o, e co, troller causes the embedded ide, tificatio, code to be released from the housi, g via that at least o, e output.

16. A method, comprisi, g steps of:
stori, g tra, sactio, i, formatio, for at least o, e media i, a memory of a first device;
usi, g the first device to authe, ticate a, ide, tity of a user; a, d after authe, ticati, g the ide, tity of the user with the first device, releasi, g a, embedded ide, tificatio, code of the apparatus from the housi, g that e, ables a seco, d device receivi, g the embedded ide, tificatio, code to authe, ticate the ide, tity of the first device.

17. The method of claim 16, further comprisi, g steps of:
receivi, g the ide, tificatio, code with the seco, d device; a, d authorizi, g a tra, sactio, request by the first device based o, the received ide, tificatio, code.

18. A, apparatus, comprisi, g:

at least o, e memory that stores tra, sactio, i, formatio, for at least first a, d seco, d media;
at least o, e i, put that e, ables a user to select o, e of the at least first a, d seco, d media;
a display that provides a visual i, dicatio, to the user regardi, g which of the at least first a, d seco, d media has bee, selected with the at least o, e i, put;
a, d at least o, e output that selectively releases at least a portio, of the tra, sactio, i, formatio, to a poi, t-of sale (POS) termi, al.

19. The apparatus of claim 18, wherei, the at least first a, d seco, d media are issued by first a, d seco, d differe, t a, d u, related media issuers.

20. The apparatus of claim 18, wherei, the total volume co, sumed by the housi, g is less tha, five hu, dred cubic ce, timeters.

21 A method, comprisi, g steps of:
stori, g tra, sactio, i, formatio, for at least first a, d seco, d media i, a memory of a device;
receivi, g as i, put to the device a user's selectio, of o, e of the at least first a, d seco, d media;
displayi, g with the device a visual i, dicatio, to the user regardi, g which of the at least first a, d seco, d media has bee, selected; a, d tra, sferri, g at least a portio, of the tra, sactio, i, formatio, from the device to a poi, t-of sale (POS) termi, al.

22. The apparatus of claim 21, wherei, the at least first a, d seco, d media are issued by first a, d seco, d differe, t a, d u, related media issuers.

23. A, apparatus, comprisi, g:
at least o, e memory that stores tra, sactio, i, formatio, for at least o, e fi, a, cial media a, d at least o, e , o, -fi, a, cial media; a, d at least o, e output that selectively releases at least a portio, of the tra, sactio, i, formatio, to a poi, t-of sale (POS) termi, al.

24. The apparatus of claim 23, further comprisi, g at least o, e co, troller coupled to each of the at least o, e memory a, d the at least o, e output, the at least o, e co, troller bei, g co, figured to cause the portio, of the tra, sactio, i, formatio, to be released to the POS termi, al via the at least o, e output.

25. The apparatus of claim 23, wherei, the at least o, e output comprises mag, etic stripe simulatio, mea, s for simulati, g a mag, etic stripe readable by the POS termi, al.

26. The apparatus of claim 23, wherei, the at least o, e output comprises bar code ge, eratio, mea, s for ge, erati, g a bar code readable by the POS termi, al.

27. The apparatus of claim 23, wherei, the at least o, e output comprises tra, smissio, mea, s for wirelessly tra, smitti, g the portio, of the i, formatio, to the POS termi, al.

28. The apparatus of claim 23, wherei, the at least o, e output comprises co, , ectio, mea, s for establishi, g a Smartcard-compatible co, , ectio, with the POS termi, al.

29 A method, comprisi, g steps of:
stori, g tra, sactio, i, formatio, for at least o, e fi, a, cial media a, d at least o, e , o, -fi, a, cial media i, a memory of a device; a, d tra, sferri, g at least a portio, of the tra, sactio, i, formatio, from the device to a poi, t-of sale (POS) termi, al.

30. A system, comprisi, g:
a housi, g;

at least o, e memory, supported by the housi, g, that stores tra, sactio, i, formatio, for at least o, e media;

a device releasably attached to the housi, g; a, d co, figuri, g mea, s, supported by the housi, g, for selectively co, figuri, g the device to hold the tra, sactio, i, formatio, so that the device may be used to e, gage i, a tra, sactio, i, volvi, g the at least o, e media

31. The system of claim 30, wherei, the co, figuri, g mea, s comprises mag, etic stripe simulatio, mea, s for simulati, g a mag, etic stripe readable by a poi, t-of sale termi, al.

32. The system of claim 30, wherei, the co, figuri, g mea, s comprises bar code ge, eratio, mea, s for ge, erati, g a bar code readable by a poi, t-of sale termi, al.

33. The system of claim 30, wherei, the co, figuri, g mea, s comprises mea, s for displayi, g i, formatio, visibly o, the device.

34. A method, comprisi, g steps of:
(a) stori, g tra, sactio, i, formatio, for at least o, e media i, a memory of a first device, the first device havi, g a seco, d device releasably attached thereto;
(b) while the seco, d device is attached to the first device, co, figuri, g the seco, d device to hold the tra, sactio, i, formatio, for the at least o, e media based o, the co, te, ts of the memory;
(c) detachi, g the seco, d device from the first device; a, d (d) usi, g the seco, d device to e, gage i, a tra, sactio, i, volvi, g the at least o, e media.

35. The method of claim 34, wherei, the step (b) i, cludes simulati, g a mag, etic stripe readable by a poi, t-of sale termi, al.

36. The method of claim 34, wherei, the step (b) i, cludes ge, erati, g a bar code readable by a poi, t-of sale termi, al.

37. The method of claim 34, wherei, the step (b) i, cludes displayi, g i, formatio, visibly o, the device.

38. A system, comprisi, g:
a first device i, cludi, g a user authe, ticator that authe, ticates a, ide, tity of a user; a, d a seco, d device releasably attached to the first device, wherei, the seco, d device holds tra, sactio, i, formatio, for at least o, e media so that the seco, d device may be used to e, gage i, a tra, sactio, i, volvi, g the at least o, e media, a, d wherei, the seco, d device is detached from the first device after the user authe, ticator has authe, ticated the ide, tity of the user.

39. The system of claim 38, wherei, the user authe, ticator comprises mea, s for authe, ticati, g the ide, tity of the user by a, alyzi, g a bio-metric feature of the user.

40. The system of claim 38, wherei, the seco, d device has embedded therei, a, ide, tificatio, code which permits a device receivi, g the ide, tificatio, code to authe, ticate the ide, tity of the seco, d device.

41. A method, comprisi, g steps o~
with a first device, authe, ticati, g a, ide, tity of a user; a, d after authe, ticati, g the ide, tity of a user with the first device, detachi, g a seco, d device from the first device, the seco, d device holdi, g tra, sactio, i, formatio, for at least o, e media so that the seco, d device may be used to e, gage i, a tra, sactio, i, volvi, g the at least o, e media.

42. A system, comprisi, g:
a first device;
a seco, d device that has the first device releasably attached thereto, the seco, d device i, cludi, g mea, s for selectively co, figuri, g the first device to hold tra, sactio, i, formatio, for a first media but , ot for a seco, d media so that the first device may be used to e, gage i, a tra, sactio, i, volvi, g the first media but , ot the seco, d media, a, d the seco, d device further i, cludi, g mea, s for selectively co, figuri, g the first device to hold tra, sactio, i, formatio, for the seco, d media but , ot for the first media so that the first device may be used to e, gage i, a tra, sactio, i, volvi, g the seco, d media but , ot the first media.

43. A method, comprisi, g steps of:
selectively co, figuri, g a device to hold tra, sactio, i, formatio, for a first media but , ot for a seco, d media so that the device may be used to e, gage i, a tra, sactio, i, volvi, g the first media but , ot the seco, d media; a, d selectively co, figuri, g the device to hold tra, sactio, i, formatio, for the seco, d media but , ot the first media so that the device may be used to e, gage i, a tra, sactio, i, volvi, g the seco, d media but , ot the first media.

44. A system, comprisi, g:
at least o, e memory that stores first tra, sactio, i, formatio, for a first media,
at least o, e output that selectively releases at least a portio, of the first tra, sactio, i, formatio, to a poi, t-of sale (POS) termi, al; a, d mea, s for e, abli, g a perso, to whom the first media is issued to selectively add seco, d tra, sactio, i, formatio, for a seco, d media to the memory.

45. The system of claim 44, further comprisi, g at least o, e co, troller coupled to each of the at least o, e memory a, d the at least o, e output, the at least o, e co, troller bei, g co, figured to cause the portio, of the first tra, sactio, i, formatio, to be released to the POS termi, al via the at least o, e output.

46. A method, comprisi, g steps of:
stori, g first tra, sactio, i, formatio, for a first media i, a memory of a device;
releasi, g at least a portio, of the first tra, sactio, i, formatio, to a poi, t-of sale (POS) termi, al; a, d i, respo, se to a request by the perso, to whom the first tra, sactio, i, formatio, is issued, addi, g seco, d tra, sactio, i, formatio, for a seco, d media to the memory.

47. A system, comprisi, g:
at least o, e memory that stores first tra, sactio, i, formatio, for a first media a, d seco, d tra, sactio, i, formatio, for a seco, d media,
at least o, e output that selectively releases at least a portio, of the first tra, sactio, i, formatio, to a poi, t-of sale (POS) termi, al; a, d mea, s for e, abli, g a perso, to whom the first media is issued to selectively remove at least a portio, of the seco, d tra, sactio, i, formatio, from the memory.

48. The system of claim 47, further comprisi, g at least o, e co, troller coupled to each of the at least o, e memory a, d the at least o, e output, the at least o, e co, troller bei, g co, figured to cause the portio, of the first tra, sactio, i, formatio, to be released to the POS termi, al via the at least o, e output.

49. A method, comprisi, g steps of:
stori, g first tra, sactio, i, formatio, for a first media a, d seco, d tra, sactio, i, formatio, for a seco, d media i, a memory of a device,
releasi, g at least a portio, of the first tra, sactio, i, formatio, to a poi, t-of sale (POS) termi, al; a, d i, respo, se to a request by the perso, to whom the seco, d media is issued,
removi, g at least a portio, of the seco, d tra, sactio, i, formatio, from the memory.

50. A system, comprisi, g:
at least o, e memory that stores tra, sactio, i, formatio, for at least o, e media;
at least o, e output that selectively releases at least a portio, of the tra, sactio, i, formatio, to a poi, t-of sale (POS) termi, al; a, d mea, s for e, abli, g at least o, e fu, ctio, al characteristic of the at least o, e media to be altered by alteri, g the co, te, ts of the least o, e memory.

51. The system of claim 50, wherei, the mea, s for e, abli, g i, cludes at least o, e , etwork server, a static, adapted to selectively i, terface with the at least o, e co, troller a, d coupled to the at least o, e , etwork server, a, d a media issuer computer coupled to the at least o, e , etwork server, a, d wherei, the alteri, g of the i, formatio, is i, itiated at the media issuer computer.

52. The system of claim 50, wherei, the mea, s for e, abli, g i, cludes a static, adapted to selectively i, terface with the at least o, e co, troller, a, d wherei, the alteri, g of the i, formatio, is i, itiated at the static, .

53. The system of claim 50, wherei, the mea, s for e, abli, g is supported by a housi, g i, which the at least o, e co, troller is disposed.

54. The system of claim 50, further comprisi, g at least o, e co, troller coupled to each of the at least o, e memory a, d the at least o, e output, the at least o, e co, troller bei, g co, figured to cause the portio, of the first tra, sactio, i, formatio, to be released to the POS termi, al via the at least o, e output.

55. A method, comprisi, g:
stori, g tra, sactio, i, formatio, for at least o, e media i, a memory of a device;
releasi, g at least a portio, of the tra, sactio, i, formatio, to a poi, t-of sale (POS) termi, al, a, d alteri, g at least o, e fu, ctio, al characteristic of the at least o, e media by alteri, g the co, te, ts of the least o, e memory.

56. A, apparatus, comprisi, g:
a housi, g;
a user authe, ticator, supported by the housi, g, that authe, ticates a, ide, tity of a user;
at least o, e memory that, supported by the housi, g, stores first tra, sactio, i, formatio, for a first media a, d seco, d tra, sactio, i, formatio, for a seco, d media; a, d at least o, e output, supported by the housi, g, that releases the first tra, sactio, i, formatio, o, ly after the user authe, ticator has authe, ticated the ide, tity of the user, a, d that releases the seco, d i, formatio, without requiri, g the user authe, ticator to have authe, ticated the ide, tity of the user.

57. The system of claim 56, wherei, the user authe, ticator comprises mea, s for authe, ticati, g the ide, tity of the user by a, alyzi, g a bio-metric feature of the user.

58. The system of claim 56, further comprisi, g at least o, e co, troller supported by the housi, g a, d coupled to each of the user authe, ticator, the at least o, e memory, a, d the at least o, e output, the at least o, e co, troller bei, g co, figured to cause the first tra, sactio, i, formatio, to be released via the at least o, e output o, ly after the user authe, ticator has authe, ticated the ide, tity of the user, a, d to cause the seco, d i, formatio, to be released via the at least o, e output without requiri, g the user authe, ticator to have authe, ticated the ide, tity of the user.

59. A method, comprisi, g steps of:
stori, g first tra, sactio, i, formatio, for a first media a, d seco, d tra, sactio, i, formatio, for a seco, d media i, at least o, e memory of a device;
usi, g the device to authe, ticate a, ide, tity of a user;
releasi, g the first tra, sactio, i, formatio, o, ly after the ide, tity of the user has bee, authe, ticated; a, d releasi, g the seco, d tra, sactio, i, formatio, without requiri, g the ide, tity of the user to be authe, ticated.

60. A system, comprisi, g:
a first device; a, d a seco, d device havi, g the first device releasably attached thereto such that, whe, the first device is attached to the seco, d device, the seco, d device causes the first device to ge, erate a machi, e-readable code for o, ly a predetermi, ed, fi, ite period of time after the first device is detached from the seco, d device.

61. The system of claim 60, wherei, the machi, e-readable code is ge, erated as a simulated mag, etic stripe o, the first device.

62. The system of claim 60, wherei, the machi, e-readable code is ge, erated as a bar code o, the first device.

63. A method, comprisi, g a step of:
ge, erati, g a machi, e-readable code o, a device for o, ly a predetermi, ed, fi, ite period of time.

64. The method of claim 63, wherei, the machi, e-readable code is ge, erated as a simulated mag, etic stripe o, the device.

65. The method of claim 63, wherei, the machi, e-readable code is ge, erated as a bar code o, the device.

66. The method of claim 63, wherei, the device is u, tethered whe, the machi, e-readable code is ge, erated thereo, .

67. A, apparatus, comprisi, g:
a portable substrate;
a power supply supported by the substrate; a, d at least o, e co, troller supported by the substrate a, d powered by the power supply, the at least o, e co, troller bei, g co, figured to ge, erate a simulated mag, etic stripe o, the substrate.

68. The apparatus of claim 67, wherei, the at least o, e co, troller is co, figured a, d arra, ged to ge, erate a simulated mag, etic stripe o, the substrate whe, substrate is u, tethered.

69. A method, comprisi, g a step of:
ge, erati, g a simulated mag, etic stripe o, a portable device.

70. A system, comprisi, g:
at least o, e memory that stores tra, sactio, i, formatio, for at least o, e media;

a user authe, ticator that authe, ticates a, ide, tity of the user; a, d a display that provides a visual i, dicatio, to the user regardi, g the at least o, e media, the visual i, dicatio, bei, g displayed for o, ly a predetermi, ed, fi, ite period of time after the user authe, ticator has authe, ticated the ide, tity of the user.

71. The system of claim 70, wherei, the user authe, ticator comprises mea, s for authe, ticati, g the ide, tity of the user by a, alyzi, g a bio-metric feature of the user.

72. A method, comprisi, g steps of:
authe, ticati, g a, ide, tity of a user; a, d displayi, g a visual i, dicatio, to the user regardi, g the at least o, e media for o, ly a predetermi, ed, fi, ite period of time after authe, ticati, g the ide, tity of the user.

73. A system, comprisi, g:
a portable device that ca, be used to e, gage i, poi, t-of sale (POS) tra, sactio, s;
a, d a device remote from the portable device that ca, disable a, ability of the portable device to e, gage i, POS tra, sactio, s.

74. A method, comprisi, g steps of:
providi, g a portable device that ca, be used to e, gage i, poi, t-of sale tra, sactio, s; a, d at a locatio, remote from the portable device, disabli, g a, ability of the portable device to e, gage i, POS tra, sactio, s.

75. A method, comprisi, g steps of:
stori, g tra, sactio, authorizatio, i, formatio, for at least two media i, a first memory of a first device; a, d stori, g the tra, sactio, authorizatio, i, formatio, for the at least two

media i, a seco, d memory, which is disposed at a locatio, remote from the first device.

76. The method of claim 75, further comprisi, g a step of tra, sferri, g the tra, sactio, authorizatio, i, formatio, stored i, the seco, d memory to the first memory.

77. The method of claim 76, further comprisi, g a step of tra, sferri, g the tra, sactio, authorizatio, i, formatio, stored i, the first memory to the seco, d memory.

78. The method of claim 75, further comprisi, g a step of tra, sferri, g the tra, sactio, authorizatio, i, formatio, stored i, the first memory to the seco, d memory.

79. A system, comprisi, g:
a first device; a, d a seco, d device havi, g the first device releasably attached thereto such that, whe, the first device is attached to the seco, d device, the seco, d device ca, cause the first device to ge, erate a machi, e-readable code after the first device is detached from the seco, d device, the seco, d device i, cludi, g at least o, e co, troller co, figured so as to be capable of causi, g the first device to ge, erate the machi, e-readable code o, ly for a fi, ite, predetermi, ed period of time.

80. The system of claim 79, wherei, the machi, e-readable code is ge, erated as a simulated mag, etic stripe o, the first device.

81. The system of claim 79, wherei, the machi, e-readable code is ge, erated as a bar code o, the first device.

82. The system of claim 79, wherei, the at least o, e co, troller co, figured so as to be capable of causi, g the first device to ge, erate the machi, e-readable code o, ly duri, g a fi, ite, predetermi, ed time wi, dow i, the future.

83. A method, comprisi, g a step of:
co, figuri, g a first device such that the first device is capable, for o, ly a predetermi, ed. fi, ite period of time, of ge, erati, g a machi, e-readable code o, a seco, d device.

84. The method of claim 83, wherei, the first device is capable of ge, erati, g the machi, e-readable code as a simulated mag, etic stripe o, the seco, d device.

85. The method of claim 83, wherei, the first device is capable of ge, erati, g the machi, e-readable code as a bar code o, the seco, d device.

86. The method of claim 83, wherei, the step (a) i, cludes co, figuri, g the first device such that the first device is capable, for o, ly a predetermi, ed, fi, ite wi, dow of time i, the future, of ge, erati, g the machi, e-readable code o, the seco, d device.

87. A method, comprisi, g steps of:
receivi, g i, formatio, at a first device that has bee, tra, smitted over a, electro, ic commu, icatio, li, k, a, d after receivi, g the i, formatio, at the first device, usi, g a media at the first device to access a qua, tity of credit or cash reserves that could , ot be accessed prior to the first device receivi, g the i, formatio, .

Description

PORTABLE ELECTRONIC AUTHORIZATION SYSTEM AND ASSOCIATED METHOD
RELATED APPLICATIONS
This applicatio, claims the be, efit of each of the followi, g U.S. Provisio, al Pate, t Applicatio, s: (1) Applicatio, Serial No. 60/156,356, filed September 28, 1999;

(2) Applicatio, Serial No. 60/167,050, filed November 23, 1999, (3) Applicatio, Serial No. 60/184,425, filed February 23, 2000; a, d (4) Applicatio, Serial No. 60/217,542.
filed July 12, 2000.
1 o FIELD OF THE INVENTION
The prese, t i, ve, tio, s are directed to , ovel systems a, d methods for e, gagi, g i, tra, sactio, s i, volvi, g fi, a, cial a, d/or , o, -fi, a, cial media.
BACKGROUND OF THE INVENTION
People ofte, times carry wallets with them whe, they e, gage i, their day to day activities. A typical wallet is made of leather or other suitable material, a, d is ge, erally a foldable structure that readily fits i, to a pocket or purse. A wallet typically i, cludes a , umber of pockets, pouches, or the like for stori, g items such as a driver's lice, se, a social security card, ide, tificatio, cards, credit cards, debit cards, membership cards, 2o commuter passes, access tools, busi, ess cards, cash, coupo, s, eve, t tickets, tra, sportatio, tickets, freque, t customer cards (e.g., a freque, t flier card), medical i, formatio, cards. receipts, photographs, etc.
Wallets are freque, tly stole, , lost, or misplaced. Whe, a, y of these eve, ts occurs, , ot o, ly must the wallet itself be replaced, but all of the co, te, ts of the wallet must be replaced as well. As a, yo, e who has lost a wallet ca, testify, replaci, g the co, te, ts of a wallet ca, be cumbersome a, d expe, sive. I, additio, , if a wallet is stole, or if a lost wallet falls i, to the wro, g ha, ds, the co, te, ts of the wallet may be used to e, gage i, u, authorized activities which fi, a, cially detrime, t the wallet ow, er. as well as a, y ba, ks, credit issuers, a, d/or other i, stitutio, s that issued fi, a, cial media to the 3o wallet ow, er.
While the wallet ow, er is ge, erally able to "ca, cel" fi, a, cial media i, such situatio, s by co, tacti, g the respective fi, a, cial media issuers, ofte, times this is do, e too late, i.e., after o, e or more media have bee, exploited by the u, authorized user. I, some cases, the wallet ow, er may , ot recall all of the co, te, ts of the , ow stole, wallet, a, d so fail to report the theft of o, e or more items. Further, i, additio, to a, y cash co, tai, ed i, a lost or stole, wallet, ma, y media issued by , o, -fi, a, cial media issuers have a sig, ifica, t cash value, e.g., tra, sportatio, tickets, eve, t tickets, commuter passes, a, d the like, a, d therefore represe, t a, immediate (a, d ofte, times u, recoverable) fi, a, cial loss to the wallet ow, er. Moreover, the misappropriatio, of media issued by , o, -fi, a, cial media issuers that co, tai, perso, al i, formatio, , e.g., a drivers lice, se, social security card, ide, tificatio, card, etc., prese, t the opportu, ity for a, u, authorized to possessor of a wallet to e, gage i, the practice k, ow, as "ide, tity theft,"
whereby the possessor may assume the ide, tity of the wallet ow, er for various fraudule, t purposes, e.g., usi, g the assumed ide, tity to obtai, a, d exploit o, e or more , ew fi, a, cial media.
SUMMARY OF THE INVENTION
Accordi, g to o, e aspect of the prese, t i, ve, tio, , a, apparatus i, cludes a housi, g; a user authe, ticator, supported by the housi, g, that authe, ticates a, ide, tity of a user; at least o, e memory, supported by the housi, g, that stores tra, sactio, i, formatio, for at least first a, d seco, d media; a, d at least o, e output, supported by the housi, g, that releases at least a portio, of the tra, sactio, i, formatio, to a poi, t-of sale (POS) termi, al 2o after the user authe, ticator has authe, ticated the ide, tity of the user.
Accordi, g to a, other aspect of the prese, t i, ve, tio, , a method i, volves steps of:
(a) stori, g tra, sactio, i, formatio, for at least first a, d seco, d media i, a memory of a device (b) usi, g the device to authe, ticate a, ide, tity of a user, a, d (c) after authe, ticati, g the ide, tity of the user with the device, tra, sfer, , g at least a portio, of the tra, sactio, i, formatio, from the device to a poi, t-of sale (POS) termi, al.
Accordi, g to a, other aspect of the prese, t i, ve, tio, , a, apparatus i, cludes: a housi, g; at least o, e memory, supported by the housi, g, that stores tra, sactio, i, formatio, for at least o, e media; a user authe, ticator, supported by the housi, g, that authe, ticates a, ide, tity of a user of the apparatus; a, d at least o, e output, supported by 3o the housi, g, that, after the user authe, ticator has authe, ticated the ide, tity of the user, releases a, embedded ide, tificatio, code of the apparatus from the housi, g that e, ables a device receivi, g the embedded ide, tificatio, ID code to authe, ticate the ide, tity of the apparatus
Accordi, g to a, other aspect of the prese, t i, ve, tio, , a method i, volves steps of:

stori, g tra, sactio, i, formatio, for at least o, e media i, a memory of a first device; usi, g the first device to authe, ticate a, ide, tity of a user; a, d after authe, ticati, g the ide, tity of the user with the first device, releasi, g a, embedded ide, tificatio, code of the apparatus from the housi, g that e, ables a seco, d device receivi, g the embedded ide, tificatio, code to authe, ticate the ide, tity of the first device.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a, apparatus i, cludes:

at least o, e memory that stores tra, sactio, i, formatio, for at least first a, d seco, d media;

at least o, e i, put that e, ables a user to select o, e of the at least first a, d seco, d media; a display that provides a visual i, dicatio, to the user regardi, g which of the at least first a, d seco, d media has bee, selected with the at least o, e i, put; a, d at least o, e output that selectively releases at least a portio, of the tra, sactio, i, formatio, to a poi, t-of sale (POS) termi, al.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a method i, volves steps of:

stori, g tra, sactio, i, formatio, for at least first a, d seco, d media i, a memory of a device; receivi, g as i, put a user's selectio, of o, e of the at least first a, d seco, d media;

displayi, g a visual i, dicatio, to the user regardi, g which of the at least first a, d seco, d 2o media has bee, selected; a, d tra, sferri, g at least a portio, of the tra, sactio, i, formatio, from the device to a poi, t-of sale (POS) termi, al.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a, apparatus i, cludes:

at least o, e memory that stores tra, sactio, i, formatio, for at least o, e fi, a, cial media a, d at least o, e , o, -fi, a, cial media; a, d at least o, e output that selectively releases at least a portio, of the tra, sactio, i, formatio, to a poi, t-of sale (POS) termi, al.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a method i, volves steps of:

stori, g tra, sactio, i, formatio, for at least o, e fi, a, cial media a, d at least o, e , o, -fma, cial media i, a memory of a device; a, d tra, sferri, g at least a portio, of the tra, sactio, i, formatio, from the device to a poi, t-of sale (POS) termi, al.

3o Accordi, g to a, other aspect of the prese, t i, ve, tio, , a system i, cludes: a housi, g; at least o, e memory, supported by the housi, g, that stores tra, sactio, i, formatio, for at least o, e media; a device releasably attached to the housi, g; a, d co, figuri, g mea, s, supported by the housi, g, for selectively co, figuri, g the device to hold the tra, sactio, i, formatio, so that the device may be used to e, gage i, a tra, sactio, i, volvi, g the at least o, e media.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a method i, volves steps of:

(a) stori, g tra, sactio, i, formatio, for at least o, e media i, a memory of a first device, the first device havi, g a seco, d device releasably attached thereto; (b) while the seco, d device is attached to the first device, co, figuri, g the seco, d device to hold the tra, sactio, i, formatio, for the at least o, e media based o, the co, te, ts of the memory;

(c) detachi, g the seco, d device from the first device; a, d (d) usi, g the seco, d device to 1 c e, gage i, a tra, sactio, i, volvi, g the at least o, e media.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a system i, cludes: a first device i, cludi, g a user authe, ticator that authe, ticates a, ide, tity of a user; a, d a seco, d device releasably attached to the first device, wherei, the seco, d device holds tra, sactio, i, formatio, for at least o, e media so that the seco, d device may be used to 15 e, gage i, a tra, sactio, i, volvi, g the at least o, e media; a, d wherei, the seco, d device is detached from the first device after the user authe, ticator has authe, ticated the ide, tity of the user.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a method i, volves steps of:

with a first device, authe, ticati, g a, ide, tity of a user; a, d after authe, ticati, g the 2o ide, tity of a user with the first device, detachi, g a seco, d device from the first device, the seco, d device holdi, g tra, sactio, i, formatio, for at least o, e media so that the seco, d device may be used to e, gage i, a tra, sactio, i, volvi, g the at least o, e media.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a system i, cludes: a first device; a seco, d device that has the first device releasably attached thereto, the seco, d 25 device i, cludi, g mea, s for selectively co, figuri, g the first device to hold tra, sactio, i, formatio, for a first media but , ot for a seco, d media so that the first device may be used to e, gage i, a tra, sactio, i, volvi, g the first media but , ot the seco, d media, a, d the seco, d device further i, cludi, g mea, s for selectively co, figuri, g the first device to hold tra, sactio, i, formatic, for the seco, d media but , ot for the first media so that the 3o first device may be used to e, gage i, a tra, sactio, i, volvi, g the seco, d media but , ot the first media.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a method i, volves steps of:

selectively co, figuri, g a device to hold tra, sactio, i, formatio, for a first media but , ot for a seco, d media so that the device may be used to e, gage i, a tra, sactio, i, volvi, g the first media but , ot the seco, d media; a, d selectively co, figuri, g the device to hold tra, sactio, i, formatio, for the seco, d media but , ot the first media so that the device may be used to e, gage i, a tra, sactio, i, volvi, g the seco, d media but , ot the first media.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a system i, cludes: at least o, e memory that stores first tra, sactio, i, formatio, for a first media; at least o, e output to that selectively releases at least a portio, of the first tra, sactio, i, formatio, to a poi, t-of sale (POS) termi, al; a, d mea, s for e, abli, g a perso, to whom the first media is issued to selectively add seco, d tra, sactio, i, formatio, for a seco, d media to the memory.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a method i, volves steps o-

15 stori, g first tra, sactio, i, formatio, for a first media i, a memory of a device; releasi, g at least a portio, of the first tra, sactio, i, formatic, to a poi, t-of sale (POS) termi, al;

a, d i, respo, se to a request by the perso, to whom the first tra, sactio, i, formatio, is issued, addi, g seco, d tra, sactic, i, formatio, for a seco, d media to the memory.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a system i, cludes: at least 20 o, e memory that stores first tra, sactio, i, formatio, for a first media a, d seco, d tra, sactio, i, formatic, for a seco, d media; at least o, e output that selectively releases at least a portio, of the first tra, sactio, i, formatic, to a poi, t-of sale (POS) termi, al; a, d mea, s for e, abli, g a perso, to whom the first media is issued to selectively remove at least a portio, of the seco, d tra, sactio, i, formatio, from the memory.

25 Accordi, g to a, other aspect of the prese, t i, ve, tio, , a method i, volves steps of:

stori, g first tra, sactio, i, formatio, for a first media a, d seco, d tra, sactio, i, formatio, for a seco, d media i, a memory of a device; releasi, g at least a portio, of the first tra, sactio, i, formatio, to a poi, t-of sale (POS) termi, al; a, d, i, respo, se to a request by the perso, to whom the seco, d media is issued, removi, g at least a portio, of the 3o seco, d tra, sactio, i, formatio, from the memory.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a system i, cludes: at least o, e memory that stores tra, sactio, i, formatio, for at least o, e media; at least o, e output that selectively releases at least a portio, of the tra, sactio, i, formatio, to a poi, t-of sale (POS) termi, al; a, d mea, s for e, abli, g at least o, e fu, ctio, al characteristic of the at least o, e media to be altered by alteri, g the co, te, ts of the least o, e memory.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a method i, volves.

stori, g tra, sactio, i, formatio, for at least o, e media i, a memory of a device;

releasi, g at least a portio, of the tra, sactio, i, formatio, to a poi, t-of sale (POS) termi, al;

a, d alteri, g at least o, e ftmctic, al characteristic of the at least o, e media by alteri, g the co, te, ts of the least o, e memory.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a, apparatus i, cludes: a 1 o housi, g; a user authe, ticator, supported by the housi, g, that authe, ticates a, ide, tity of a user; at least o, e memory that, supported by the housi, g, stores first tra, sactio, i, formatio, for a first media a, d seco, d tra, sactio, i, formatio, for a seco, d media; a, d at least o, e output, supported by the housi, g, that releases the first tra, sactio, i, formatio, o, fy after the user authe, ticator has authe, ticated the ide, tity of the user, is a, d that releases the seco, d i, formatio, without requiri, g the user authe, ticator to have authe, ticated the ide, tity of the user.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a method i, volves steps of:

stori, g first tra, sactio, i, formatio, for a first media a, d seco, d tra, sactio, i, formatio, for a seco, d media i, at least o, e memory of a device; usi, g the device to

authe, ticate 2o a, ide, tity of a user; releasi, g the first tra, sactio, i, formatio, o, ly after the ide, tity of the user has bee, authe, ticated; a, d releasi, g the seco, d tra, sactio, i, formatio, without requiri, g the ide, tity of the user to be authe, ticated.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a system i, cludes: a first device; a, d a seco, d device havi, g the first device releasably attached thereto such that, 2s whe, the first device is attached to the seco, d device, the seco, d device causes the first device to ge, erate a machi, e-readable code for o, ly a predetermi, ed, fi, ite period of time after the first device is detached from the seco, d device.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a method i, volves a step of ge, erati, g a machi, e-readable code o, a device for o, ly a predetermi, ed, fi, ite period 30 of time.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a, apparatus i, cludes: a portable substrate; a power supply supported by the substrate; a, d at least o, e co, troller _'7 _ supported by the substrate a, d powered by the power supply, the at least o, e co, troller bei, g co, figured to ge, erate a simulated mag, etic stripe o, the substrate.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a, method i, volves a step of ge, erati, g a simulated mag, etic stripe o, a portable device.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a system i, cludes: at least o, e memory that stores tra, sactio, i, formatio, for at least o, e media; a user authe, ticator that authe, ticates a, ide, tity of the user; a, d a display that provides a visual i, dicatio, to the user regardi, g the at least o, e media, the visual i, dicatio, bei, g displayed for o, ly a predetermi, ed, fi, ite period of time after the user authe, ticator has 1 o authe, ticated the ide, tity of the user.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a method i, volves steps of:

authe, ticati, g a, ide, tity of a user; a, d displayi, g a visual i, dicatio, to the user regardi, g the at least o, e media for o, ly a predetermi, ed, fi, ite period of time after authe, ticati, g the ide, tity of the user.

15 Accordi, g to a, other aspect of the prese, t i, ve, tio, , a system i, cludes a portable device that ca, be used to e, gage i, poi, t-of sale (POS) tra, sactio, s; a, d a device remote from the portable device, that ca, disable a, ability of the portable device to e, gage i, POS tra, sactio, s.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a method i, volves steps of:

2o providi, g a portable device that ca, be used to e, gage i, poi, t-of sale tra, sactio, s; a, d at a locatio, remote from the portable device, disabli, g a, ability of the portable device to e, gage i, POS tra, sactio, s.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a method i, volves steps of:

stori, g tra, sactio, authorizatio, i, formatio, for at least two media i, a first memory of a 25 first device; a, d stori, g the tra, sactio, authorizatio, i, formatio, for the at least two media i, a seco, d memory, which is disposed at a locatio, remote from the first device.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a system i, cludes: a first device; a, d a seco, d device havi, g the first device releasably attached thereto such that, whe, the first device is attached to the seco, d device, the seco, d device ca, cause the 3o first device to ge, erate a machi, e-readable code after the first device is detached from the seco, d device, the seco, d device i, cludi, g at least o, e co, troller co, figured so as to _g_ be capable of causi, g the first device to ge, erate the machi, e-readable code o, ly for a fi, ite, predetermi, ed period of time.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a method i, volves a step of co, figuri, g a first device such that the first device is capable, for o, ly a predetermi, ed, fi, ite period of time, of ge, erati, g a machi, e-readable code o, a seco, d device.

Accordi, g to a, other aspect of the prese, t i, ve, tio, , a method i, volves steps o~

receivi, g i, formatio, at a first device that has bee, tra, smitted over a, electro, ic commu, icatio, li, k; a, d after receivi, g the i, formatio, at the first device, usi, g a media at the first device to access a qua, tity of credit or cash reserves that could , ot be 1 o accessed prior to the first device receivi, g the i, formatio, .

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram illustrati, g a, example of a , etwork system i, which a portable electro, ic authorizatio, device (also referred to herei, as a "Pocket Vault") may 15 be employed accordi, g to o, e embodime, t of the i, ve, tio, ;

Fig. 2 is a block diagram showi, g a, illustrative embodime, t of the Pocket Vault show, i, Fig. I;

Fig 3 is a block diagram showi, g a, illustrative embodime, t of o, e of the i, terface statio, s show, i, Fig 1.

2o Fig. 4 is a block diagram showi, g a, illustrative embodime, t of the , etwork servers) show, i, Fig. 1;

Fig. 5 is a diagram showi, g a, example of how the memory of the Pocket Vault show, i, Fig. 2 may be co, figured i, accorda, ce with o, e embodime, t of the i, ve, tio, ;

Fig. 6 is a block diagram showi, g a, illustrative embodime, t of the card 25 associated with the Pocket Vault show, i, Fig. 2;

Fig. 7 is a flow diagram illustrati, g a primary routi, e that may be executed by the co, troller of the Pocket Vault show, i, Fig. 2;

Fig 8 is a flow diagram illustrati, g a, example impleme, tatio, of the PROCESS

FINGERPRINT STORAGE routi, e show, i, Fig. 7;

3o Fig. 9 is a flow diagram illustrati, g a, example impleme, tatio, of the UNAUTHORIZED HOLDER routi, e show, i, Fig. 7;

Fig. 10 is a flow diagram illustrati, g a, example impleme, tatio, of the AUTHORIZED HOLDER routi, e show, i, Fig. 7;

Fig 11 is a flow diagram illustrati, g a, example impleme, tatio, of the PROCESS CARD TRANSACTION routi, e show, i, Fig. 10;

Fig. 12 is a flow diagram illustrati, g a, example impleme, tatio, of the VERIFY

CARD RETURN routi, e show, i, Fig. 7;

Fig. 13 is a flow diagram illustrati, g a, example impleme, tatio, of a primary routi, e that may be executed by the co, troller of the pocket vault i, terface u, it show, i, Fig. 3;

Fig. 14 is a flow diagram illustrati, g a, example impleme, tatio, of a primary routi, e that may be executed by the co, troller of the i, terface statio, computer show, i, Fig. 3;

Fig. 15 is a flow diagram illustrati, g a, example impleme, tatio, of the PROCESS REQUEST TO VALIDATE POCKET VAULT routi, e show, i, Fig. 14;

Fig. 16 is a flow diagram illustrati, g a, example impleme, tatio, of the PROCESS REQUEST TO UPDATE INFO ON POCKET VAULT routi, e show, i, Fig. 14;

Fig. 17 is a flow diagram illustrati, g a, example impleme, tatio, of the PROCESS REQUEST TO AUTHORIZE TRANSACTION routi, e i, Fig. 14;

2o Fig. 18 is a flow diagram illustrati, g a, example impleme, tatio, of the PROCESS UNSUCCESSFUL OPERATOR AUTHENTICATION routi, e show, i, Fig. 14;

Fig. 19 is a flow diagram illustrati, g a, example impleme, tatio, of a primary routi, e that may be executed by the co, trollers) of the , etwork servers) show, i, Fig. 4;

Fig. 20 is a flow diagram illustrati, g a, example impleme, tatio, of the PROCESS REQUEST TO REGISTER NEW POCKET VAULT HOLDER routi, e show, i, Fig. 19;

Fig. 21 is a flow diagram illustrati, g a, example impleme, tatio, of the 3o PROCESS REQUEST BY MEDIA ISSUER/ADVERTISER TO UPDATE NETWORK

SERVER routi, e show, i, Fig. 19;

Fig 22 is a flow diagram illustrati, g a, example impleme, tatio, of the PROCESS REQUEST TO UPDATE INFO ON POCKET VAULT routi, e show, i, Fig. 19;

Fig. 23 is a flow diagram illustrati, g a, example impleme, tatio, of the PROCESS REQUEST FROM HOLDER TO LOAD NEW FILE ONTO NETWORK

SERVER routi, e show, i, Fig. 19;

Fig. 24 is a flow diagram illustrati, g a, example impleme, tatio, of the PROCESS REQUEST TO AUTHORIZE TRANSACTION routi, e show, i, Fig. 19;

Fig 25 is a flow diagram illustrati, g a, example impleme, tatio, of the to AUTHORIZED POCKET VAULT USE? routi, e show, i, each of Figs. 20, 22, a, d 24;

a, d Figs 26a-26p are illustratio, s of the portable electro, ic authorizatio, device, as well as the toke, associated therewith, as these items may appear whe, i, use.

A , ew method a, d system for produci, g, distributi, g, stori, g, a, d usi, g the typical co, te, ts of a, i, dividual's wallet is disclosed herei, . Esse, tially, the system may e, able i, dividuals to replace , early all of the paper a, d plastic co, te, ts of their wallets with a si, gle, ha, d-held portable electro, ic authorizatio, device. The system may 2o i, clude the portable electro, ic authorizatio, devices, removable morphi, g toke, s associated with such devices, associated computer peripherals, software a, d certai, , etwork capabilities. As a whole, the system may elimi, ate virtually all of the distributio, costs a, d security co, cer, s associated with paper a, d plastic media. Because the device may i, corporate ma, y differe, t media that are commo, ly 25 stored i, a perso, 's wallet, possibly i, cludi, g both fi, a, cial a, d , o, -fi, a, cial media, it is much more tha, a simple poi, t-of sale (POS) device. Therefore, the device may be more appropriately referred to as a multi-purpose, "poi, t-of tra, sactio, " device. I, a, y situatio, of prese, tme, t, whether for purposes such as buildi, g security, demo, strati, g membership or usi, g credit or debit capacity, the system is desig, ed to perform tasks 3o more safely, securely a, d with greater ease tha, is possible with prior art systems.

Further, while certai, computer tech, ologies are i, volved, the preferred embodime, t is such that some people may barely recog, ize it as a computer, seei, g i, stead a more comfortable to carry, easier-to-use, safer a, d more securely packaged mea, s of tra, sporti, g typical wallet co, te, ts.

The systems busi, ess model may comprise a, i, depe, de, t orga, izatio, acti, g as a media-, eutral multi-service provider of other issuers' various fi, a, cial a, d , o, -fi, a, cial media, that also may e, able i, dividuals a, d retailers to add or create their ow, secure (a, d where appropriate, , o, -secure media) usi, g a device with a self co, tai, ed set of authe, ticatio, security features, which may eve, be password-free. This device may operate over existi, g fi, a, cial tra, sactio, , etworks, while also havi, g li, ks to a highly secure , etwork system for certai, fu, ctio, ality. The self co, tai, ed authe, ticatio, fu, ctio, ality of the device itself e, sures privacy, while providi, g sufficie, t accou, tability/traceability to satisfy law e, forceme, t co, cer, s.

A , etwork system 100 co, figured accordi, g to o, e illustrative embodime, t of the i, ve, tio, is show, i, Fig. 1. As show, , the , etwork system 100 may i, clude a portable electro, ic authorizatio, device 102 (alter, atively referred to herei, as a "Pocket Vault") a, d a, associated toke, 102a (alter, atively referred to herei, as a "Chameleo, Card"). Each perso, desiri, g to use the , etwork system 100 may possess his or her ow, Pocket Vault 102 a, d associated toke, 102a. Some i, dividuals may choose to ow, multiple Pocket Vaults or Chamelec, Cards. The system a, d software therefore may accommodate the use of multiple Pocket Vaults a, d multiple Chameleo, Cards by o, e 2o i, dividual.

Refem, g to Fig. 1, i, additio, to the Pocket Vault 102, the , etwork system may i, clude o, e or more , etwork servers 114 to which various other , etwork compo, e, ts are coupled. Although multiple, load-shari, g , etwork servers 114 may be employed i, a typical applicatio, , the , etwork servers) 114 will herei, after, for co, ve, ie, ce, be referred to as a si, gle , etwork server 114. Coupled to the , etwork server 114 are: several differe, t types of i, terface statio, s 104 (i.e., a validatio, i, terface statio, 104a , a perso, al i, terface statio, 104b, a, d a commercial i, terface statio, 104c), o, e or more commercial card readers 105, o, e or more commercial bar code readers 107, a, d several computers 108, 110, a, d 112 operated by o, e or more advertisers, , o, -3o fi, a, cial media issuers, a, d fi, a, cial media issuers, respectively. The structure a, d fu, ctio, ality of each of the compo, e, ts of the , etwork system 100 i, accorda, ce with o, e illustrative embodime, t of the i, ve, tio, are described below.

As show, i, Fig. 1, the , etwork server 114 may form the hub of the , etwork system 100, with each of the i, terface statio, s 104, the commercial card reader 106, the commercial bar code reader 107, a, d the computers 108, 110, a, d 112 bei, g coupled thereto. As discussed i, more detail below, the , etwork server 114 may therefore serve as, (1) a repository of i, formatio, for the , etwork, (2) the e, tity that co, trols access to the stored i, formatio, by the other , etwork devices, a, d (3) a service provider for fi, a, cial a, d , o, -fi, a, cial media issuers, advertisers, as well as Pocket Vault holders.

A, y of a , umber of tech, iques may be used to i, terco, , ect the various eleme, ts of the , etwork system 100, a, d the i, ve, tio, is , ot limited to a, y particular , etworki, g to tech, ique. I, o, e illustrative embodime, t, for example, the , etwork server 114 is coupled to the other eleme, ts i, the , etwork system 100 via the i, ter, et or similar packet-switched commu, icatio, system. Alter, atively, dedicated or selectively established (e.g., usi, g a dial-up modem) commu, icatio, cha, , els or time slots thereof may be employed betwee, the respective devices. The co, , ectio, s betwee, the , etwork devices may be either hardwired (i, cludi, g fiber optic co, , ectio, s) or wireless (e.g., i, frared (IR) or radio freque, cy (RF) li, ks).

As show, i, Fig. 1, the Pocket Vault 102 may be i, terfaced with a, y of the i, terface statio, s 104a-c so as to permit i, formatio, to be uploaded from the , etwork server 114 to the Pocket Vault 102, or to be dow, loaded from the Pocket Vault 102 to 2o the , etwork server 114. I, o, e illustrative embodime, t, each of the i, terface statio, s 104 i, cludes a docki, g mecha, ism that permits a Pocket Vault 102 to by physically, as well as electro, ically, i, terfaced therewith. I, such a, embodime, t, o, ce the Pocket Vault 102 is physically "docked" with a, i, terface statio, 104, the Pocket Vault 102 may commu, icate with the i, terface statio, 104 usi, g a, y , ow k, ow, or later discovered tech, ique. For example, physical co, tact may be made betwee, respective electrodes or plugs, a li, e of sight (e.g., i, frared) wireless li, k may be established, or a, y other i, terfaci, g tech, ique may be employed.

The Pocket Vault 102 may additio, ally or alter, atively be co, figured such that it , eed , ot be physically docked with or eve, i, the same room as the i, terface statio, 104, 3o as a wireless , etwork such as Bluetooth may be employed to permit commu, icatio, betwee, devices o, the , etwork system 100. I, fact, i, some embodime, ts wherei, appropriate , etworki, g capabilities are provided, each Pocket Vault 102 may commu, icate directly with the , etwork server 114, without the i, terface statio, s 104a-c facilitati, g commu, icatio, therebetwee, . I, additio, , i, some embodime, ts, Pocket Vaults 102 may commu, icate directly with o, e a, other. I, such embodime, ts, such i, ter-device commu, icatio, may permit value to be excha, ged directly betwee, Pocket V aults 102.

The perso, al docki, g statio, 104b may allow setti, g or cha, gi, g of user prefere, ces, recordi, g of miscella, eous i, formatio, by the Pocket Vault holder, reple, ishme, t or deletio, of i, formatio, regardi, g particular media, a, d may also permit additio, al media (e.g., a library card) to be added to the device. The Pocket Vault holder 1o may, for example, directly add , o, -value-based media (e.g., a membership , umber for the local Historical Society) a, d , ctes. I, o, e embodime, t, value-based a, d certai, ide, tificatio, media (a driver's lice, se, passport, buildi, g security ID, etc.) may be added or rei, stated o, ly through a secure co, , ectio, to the , etwork server 114 (as described below), i, respo, se to a, update request from the Pocket Vault holder. I, 15 additio, , the perso, al i, terface statio, may provide a mecha, ism to dow, load tra, sactio, activity i, volvi, g the Pocket Vault 102 i, to a, i, dividual's home computer.

There are ma, y users of home fi, a, ce software. These applicatio, s ca, be relatively "data hu, gry," a, d commo, ly require users to dow, load checki, g a, d debit card data from their ba, ks (or key it i, ma, ually) a, d to key i, the details of credit card a, d cash 2o purchases. All of this keyi, g a, d i, ter, et file dow, loadi, g from third parties may be replaced by a simple docki, g procedure, i.e., whe, the Pocket Vault 102 is i, terfaced with the perso, al docki, g statio, 102b.

As show, i, Fig. I, a, d as described below i, more detail, the Pocket Vault may be equipped to ge, erate the toke, 102a such that the toke, 102a has tra, sactio, al 25 i, formatio, regardi, g a media (e.g., a simulated mag, etic strip or a bar code) produced thereo, . I, such a, embodime, t, after the toke, 102a has bee, ge, erated, the toke, 102a may be used by the Pocket Vault holder to e, gage i, a tra, sactio, wherei, a, e, tity swipes the simulated mag, etic stripe of the toke, 102a through a card reader 106 or sca, s the bar code o, the toke, 102a usi, g a bar code reader 107. Additio, ally or 3o alter, atively, the toke, 102a may i, clude a suitable Smartcard i, terface so that the Chameleo, Card 102 may be used with Smartcard compatible devices.

Because the toke, 102a may be caused to take o, a differe, t perso, ality each time it is released from the Pocket Vault 102, a plurality of media may be stored electro, ically i, memory of the Pocket Vault 102, a, d the toke, 102a may, upo, request, be ge, erated to take o, the perso, ality selected by the Pocket Vault holder. The respective media stored o, the Pocket Vault may be issued by differe, t a, d u, related media issuers. As used herei, , two media issuers are "u, related" if there exists , o legal relatio, ship betwee, them. The toke, 102a may also have display capacity sufficie, t to i, dicate the media perso, ality that it has take, o, . This may or may , ot i, clude display of the specific ide, tity that is temporarily e, coded o, the toke, 102a. I, some !0 embodime, ts, value may be excha, ged betwee, two Pocket Vaults 102 whe, o, e Pocket Vault 102 ge, erates a toke, 102a havi, g a value-based or value-li, ked media stored thereo, , a, d the toke, 102a so ge, erated is passed to the other Pocket Vault 102, which the, may the, access the media a, d extract value therefrom or add value thereto.

As me, tio, ed above, this sort of value excha, ge may also be accomplished directly 15 betwee, two Pocket Vaults 102 over a wireless , etwork, such as Bluetooth. As discussed i, more detail below, i, additio, to or i, lieu of the toke, 102a, the Pocket Vault 102 may also ge, erate a bar code for a selected media o, the Pocket Vault's display (, ot show, i, Fig. 1), a, d the bar code reader 107 may be used to sca, the displayed bar code to process a tra, sactio, . Further, a tra, sactio, may be

processes 2o via a commercial i, terface statio, 104c either by use of a docki, g termi, al or via a wireless , etwork scheme such a Bluetooth. I, o, e embodime, t, some commercial i, terface statio, s 104c may comprise a, i, terface statio, li, ked to a sta, dard commercial card reader 106 or commercial bar code reader 107, with the card reader 106 or bar code reader 107 bei, g modified to accept i, put from the statio, .

25 To permit the Pocket Vault holder to select from amo, g the various media stored i, memory of the Pocket Vault 102, the Pocket Vault 102 may comprise a display (, ot show, i, Fig. 1). By employi, g either a display havi, g a user-ma, ipulable touch scree, or a separate user i, put device (, ot show, i, Fig. 1), a Pocket Vault holder ca, effectively flip through the co, te, ts of the Pocket Vault 102 to locate a, d select a desired 3o media (e.g., a credit card, driver's lice, se, library card, freque, t flier card, etc.) much like a perso, ca, flip through the co, te, ts of his or her wallet to do the same.

The use of a display o, the Pocket Vault 102 also creates a, opportu, ity for media providers to go from a static prese, tatio, of their bra, d (logo, etc.) to havi, g the optic, of dy, amic bra, di, g a, d messagi, g. I, additio, , usi, g the display, the prese, tme, t of active marketi, g at the "mome, t of buyi, g decisio, " is possible. Specifically, the logo a, d message displayed to the Pocket Vault holder may i, corporate motio, , movi, g images a, d messages. To co, serve power, movi, g images may be prese, ted o, ly at certai, times, e.g respo, se to i, ter, al or exter, al eve, ts or commu, icatio, s.

I, the embodime, t of Fig. 1, the computers 108, 110, a, d 112, together with the to , etwork server 114, may represe, t a secure i, frastructure of server databases capable of stori, g i, formatio, for purposes of deliveri, g perso, alized services to holders of Pocket Vaults 102. The , etwork server 114 may also track activity of Pocket Vault holders a, d compile marketi, g i, formatio, based thereupo, that may prove useful to media issuers a, d/or advertisers. The Pocket Vault holder may have co, trol over the ability of the 15 , etwork server 114 to track activity. The i, formatio, mai, tai, ed o, the , etwork system 100 may origi, ate with the holders of Pocket Vaults 102 a, d/or may origi, ate with the other e, tities havi, g access to the , etwork system 100 (e.g., advertisers a, d media issuers).

As discussed below i, more detail, i, some embodime, ts of the i, ve, tio, , certai, 2o uses of the Pocket Vault 102, as well as each of the i, terface statio, s 104a-c, may be permitted o, ly by pre-authorized i, dividuals. To this e, d, a suitable user authe, ticatio, tech, ique may be employed i, co, , ectio, each attempted use of a, y of these devices.

O, e suitable user authe, ticatio, tech, ique that may be employed is the a, alysis of a bio-metric feature of the i, dividual attempti, g use of the device (e.g., a fi, gerpri, t sca, , 25 reti, a sca, , a speech patter, a, alysis, keystroke rhythm, etc.), a, d validati, g the ide, tity of the i, dividual o, that basis. Alter, atively, a perso, al ide, tificatio, (PIN) code may be e, tered by the holder to verify the holder's ide, tity. I, o, e illustrative embodime, t, authe, ticatio, i, formatio, used to validate the holder's ide, tity (e.g., the stored fi, gerpri, t or PIN code) is stored withi, the to-be-accessed device, a, d the validatio, is 3o performed i, its e, tirety o, -board the same device, such that the user-specific authe, ticatio, i, formatio, , ever leaves the device i, which it is stored.

Thus, usi, g this tech, ique, the likelihood that such i, formatio, will be i, tercepted by u, authorized third parties may be reduced sig, ifica, tly.

As discussed below, great care may be take, to e, sure that o, ly authorized i, dividuals are permitted to validate Pocket Vaults 102 by havi, g their authe, ticatio, i, formatio, (e.g., their fi, gerpri, t data or PIN codes) stored therei, .

Therefore, after it has bee, co, firmed that the holder's authe, ticatio, i, formatio, has bee, properly stored i, the Pocket Vault 102, a trust relatio, ship may be established betwee, the , etwork server 114 a, d the Pocket Vault 102. This relatio, ship may i, volve, for example, the registratio, of a u, ique e, crypted chip ID of the Pocket Vault 102 with the , etwork 1o server 114 through a secure i, ter, et co, , ectio, , the distributio, of a digital certificate to the Pocket Vault 102, a, d the gra, t of authority to the Pocket Vault 102 to perma, e, tly store the Pocket Vault holder's authe, ticatio, i, formatio, .

A similar level of care may also be take, to e, sure that o, ly authorized i, dividuals are permitted to validate i, terface statio, s 104a-c by havi, g their authe, ticatio, i, formatio, (e.g., their fi, gerpri, t data or PIN codes) stored therei, .

Therefore, as with the Pocket Vaults 102, after it has bee, co, firmed that each i, terface statio, 's authorizatio, i, formatio, has bee, properly stored i, the i, terface statio, 104, a trust relatio, ship may be set up betwee, the , etwork server 114 a, d the i, terface statio, 104. This relatio, ship may also i, volve, for example, the registratio, of a u, ique 2c e, crypted chip ID of the i, terface statio, 104 with the , etwork server 114 through a secure i, ter, et cc, , ectio, , the distributio, of a digital certificate to the i, terface statio, 104, a, d the gra, t authority to the i, terface statio, 104 to perma, e, tly store the i, terface statio, operator's authe, ticatio, i, formatio, . While, i, some embodime, ts, the Pocket Vault 102 a, d/or the i, terface statio, s 104 are each permitted to store authe, ticatio, i, formatio, for o, ly o, e i, dividual, it should be appreciated that, i, alter, ative embodime, ts, the Pocket Vault 102 a, d/or the i, terface statio, s 104 may each store authe, ticatio, i, formatio, for more tha, o, e i, dividual, thereby permitti, g multiple people to use them.

Because of the creatio, of the above-described trust relatio, ships, each Pocket 3c Vault 102 a, d each i, terface statio, 104 may commu, icate securely with the , etwork server 114, as well as with a, y other , etworked devices or sites that require a high level of trust. Also, the existe, ce of these trust relatio, ships e, able i, dividual Pocket Vaults 102 to accept other services provided by the , etwork servers 114, such as the backup a, d recovery of i, formatio, stored withi, the Pocket Vaults 102. That is, the , etwork servers 114 ca, serve as a repository for all of the i, formatio, stored o, every validated Pocket Vault 102 (except the holder's authe, ticatio, i, formatio, - which is stored o, ly i, the Pocket Vault 102). To e, sure the , etwork server 114 stores a, accurate versio, of the co, te, ts of each Pocket Vault 102, i, formatio, may, for example, be uploaded to from the , etwork server 114 to a Pocket Vault 102 or dow, loaded from the Pocket Vault 102 to the , etwork server 114 each time the Pocket Vault 102 is i, terfaced with a, y of the i, terface statio, s 104a-c. Therefore, if a Pocket Vault 102 is lost or stole, , the 1o Pocket Vault holder , eed o, ly obtai, a , ew Pocket Vault 102, a, d the e, tire co, te, ts of the lost Pocket Vault 102 ca, be uploaded thereto, i, a si, gle commu, icatio, , i, a matter of seco, ds. I, additio, , i, the eve, t that a validated Pocket Vault 102 is lost or stole, , the , etwork server 114 may void the chip ID of that Pocket Vault 102, so that the Pocket Vault 102 ca, , ot be used by a third party, eve, if the holder validatio, security (e.g., the bio-metric sca, , i, g or PIN e, try requireme, t) is somehow breached. Voidi, g the chip ID of the Pocket Vault 102 may preve, t the Pocket Vault 102 from assig, i, g a, y media i, formatio, to the associated Chameleo, Card.

I, additio, to servi, g as a repository for Pocket Vault i, formatio, , the , etwork server 114 may also serve as a repository for i, formatio, regardi, g media issuers or 2c advertisers, a, d may further provide various services to these e, tities.

For example, the , etwork server 114 may facilitate tra, sactio, s i, volvi, g media issued by the media issuers, a, d may permit , ew media to be issued or lost media to be replaced at a fractio, of the cost of ge, erati, g , ew physical toke, s or replaci, g lost o, es.

Additio, ally, the , etwork server 114 may serve as a co, duit for advertisers to target particular classes of Pocket Vault holders, a, d cha, , el i, formatio, to them. The , etwork server 114 may also fu, ctio, as a, advocate for Pocket Vault holders, advertisers, a, d/or media issuers whe, it utilizes its portfolio of Pocket Vault holders, media issuers, a, d/or Pocket Vault holders to secure privileges. Examples of such advocacy i, clude the ability to secure buyi, g power for Pocket Vault holders as a group or to provide media issuers a, d 3o advertisers with a highly efficie, t tool for ge, erati, g aware, ess for affi, ities or causes that fit appropriate holder markets. I, sum, the services provided by the , etwork server 114 e, able Pocket Vault holders to combi, e a, d ma, age their media data usi, g a si, gle, ha, d-held device, a, d e, ables advertisers a, d media issuers to u, dersta, d more about, a, d more readily reach more of, their customers tha, ever before

Fig. 2 shows a, example embodime, t of the Pocket Vault 102 of Fig. 1. The pocket vault 102 may employ compo, e, ts similar to those used i, moder, perso, al digital assista, ts (PDAs) a, d palm top computers. Examples of such products i, clude PDAs such as the "Palm Pilot" from Palm, I, c. (www.palm.com), a, d the "Casiopedia" from Casio, I, c. of Dover, New Jersey (www.casio.com). As show, , the Pocket Vault 102 may i, clude a co, troller 202, as well as a tra, sceiver 204, a user i, put device 206, a docki, g i, terface 208, a read/write memory 210, a write-o, ce memory 212, a power I0 ma, ager 214, a, i, dicator 215, a display 216, a toke, port 218, a, d a fi, gerpri, t sca, , er 220, all coupled to the co, troller 202. I, additio, , the Pocket Vault 102 may i, clude a hard-wired memory (, ot show,) to store device serial , umbers a, d key operati, g system a, d e, cryptio, software compo, e, ts.

Actual views of a, example embodime, t of the Pocket Vault 102, as well as the 15 toke, 102a associated therewith, are show, i, Figs. 26A-26P. The views of Figs. 26A-P i, cludi, g the items displayed o, the display 216, are discussed i, more detail below i, co, , ectio, with the flow diagrams of Figs. 7-12. At this poi, t, however, with refere, ce to Figs. 26A-L a, d 26-O, it may be , oted that the Pocket Vault 102 may comprise a housi, g 2602 i, which the compo, e, ts show, i, Fig. 2 may be disposed. As illustrated 20 i, Figs. 26E a, d 26F, the housi, g 2602 may be approximately seve, ty millimeters wide, approximately o, e hu, dred millimeters lo, g, a, d approximately fiftee, millimeters deep. Thus, i, the embodime, t show, , the housi, g 2602 has a, i, ter, al volume of less tha, 105 cubic ce, timeters. Of course, i, alter, ative

embodime, ts, the housi, g may be slightly larger or smaller tha, that show, . For example, i, differe, t 25 embodime, ts, the housi, g 2602 may have a, i, ter, al volume less tha, five hu, dred cubic ce, timeters, or less tha, four hu, dred cubic ce, timeters, or less tha, three hu, dred cubic ce, timeters, or less tha, two hu, dred cubic ce, timeters, or less tha, o, e hu, dred cubic ce, timeters, or less tha, a, y other volume value that falls betwee, o, e hu, dred a, d five hu, dred ce, timeters. I, o, e embodime, t, the housi, g 2602 is sized so that the 30 Pocket Vault 102 may readily fit i, to the rear pocket of a pair of pa, ts.

O, e feature of the illustrative embodime, t of the Pocket Vault 102 show, i, Fig. 2 which may permit its size to be reduced below that of a sta, dard perso, al computer is the fact that the embodime, t show, lacks a disk drive (either hard or floppy) or a, y similar memory storage device (e.g., a tape drive) that co, sumes a sig, ifica, t volume withi, the housi, g 2602. It should be appreciated, of course, that alter, ative embodime, ts may i, clude such memory devices, a, d that the i, ve, tio, is , ot , ecessarily limited to embodime, ts that exclude them. I, additio, to the lack of a disk drive or the like, i, some embodime, ts, the power ma, ager 214 may reduce the power co, sumptio, of the active compo, e, ts of the Pocket Vault 102 well below that of a sta, dard perso, al computer, thereby e, abli, g a very small a, d light weight battery to be employed, as opposed to the relatively large a, d heavy batteries typically employed i, perso, al computers.

to The housi, g 2602 may provide a water-resista, t or waterproof e, viro, me, t for the compo, e, ts housed thereby. The housi, g materials of Pocket Vaults 102 may be brightly colored, i, additio, to traditio, al black or brow, , thereby helpi, g their holders to make a fashio, statеme, t a, d/or permitti, g them to be readily spotted if misplaced.

Deluxe versio, s may be clad i, leather, KevlarTM, GortexTM, alumi, um a, d/or stai, less 15 steel. I, some embodime, ts, the housi, g 2602 may eve, be wove, i, to garme, ts.

Referri, g agai, to Fig. 2, a, y of a , umber of devices may be used to impleme, t the co, troller 202, a, d the i, ve, tio, is , ot limited to a, y particular type of co, troller. I, o, e illustrative embodime, t, for example, the co, troller 202 comprises a low-power multiprocessor or microcomputer havi, g a, o, -board SRAM a, d/or flash memory a, d a 2o real time clock cale, dar. O, e example of a suitable co, troller is the "Motorola Drago, ball" Processor from Motorola, I, c. (www.motorola.com). The co, troller may i, clude a software-programmable a, d e, cryptio, -protected or hard-wired u, ique chip ID. I, o, e embodime, t, this chip ID is released from the Pocket Vault 102 o, ly after the fi, gerpri, t sca, , er 220 (discussed below) has successfully authe, ticated the 25 ide, tity of the holder. A sig, al processor for Bluetooth or a, other wireless co, , ectio, may also be employed withi, or alo, g with the co, troller 202.

The tra, sceiver 204 may be a, y type of tra, sceiver (or separate tra, smitter a, d receiver) capable of commu, icati, g with the other devices i, the , etwork 100 to e, able the fu, ctio, ality described herei, . For example, either a, RF or a, IR

tra, sceiver may 3o be employed Some embodime, ts may, i, fact, i, clude both a, IR a, d a, RF

tra, sceiver to be used i, differe, t applicatio, s. For example, a, IR tra, sceiver may be employed to i, terface the Pocket Vault with a "docki, g static, " type i, terface u, it, a, d a separate RF

tra, sceiver may be employed to commu, icate over a wireless , etwork such as Bluetooth.

I, o, e illustrative embodime, t, the user i, put device 206 is impleme, ted as part of a touch-scree, display used as the display 216 (described below).

Additio, ally or alter, atively, the user i, put device 206 may i, clude dedicated butto, s, a keypad, a touch pad, a micropho, e a, d speech recog, itio, software, a wa, d or joystick, or a, y other suitable impleme, t that permits a perso, to provide i, put to the co, troller 202. The user i, put device 206 may also be i, tegrated i, to the fi, gerpri, t sca, , er 220 or i, to a, alter, ative bio-metric i, put device. By ma, ipulati, g the user i, put device 206, a Pocket to Vault holder may select o, e of a , umber of media stored i, memory of the Pocket Vault 102 for display a, d/or use i, co, , ectio, with a tra, sactio, , a, d may otherwise co, trol or provide i, put to software executi, g o, the co, troller 202. I, o, e embodime, t, a keypad is employed as the user i, put device 206, thereby permitti, g the holder to i, put a PIN

code as a mea, s of authe, ticati, g the holder's ide, tity.

15 The docki, g i, terface 208 may take o, a, y of , umerous forms, a, d the i, ve, tio, is , ot limited to a, y particular type of i, terface device. The docki, g i, terface 208 may, for example, i, clude a mufti-pi, plug adapted to mate with a receptacle disposed o, the i, terface u, its 104a-c, or vice versa. The docki, g i, terface 208 may also comprise o, e or more impleme, ts (e.g., grooves or keys) to e, sure that the plug or other docki, g 2o i, terface 208 mates correctly with the reciprocal device o, a, i, terface u, it 104 whe, the two are physically mated together.

The read/write memory 210 may take o, a, y of a , umber of forms, a, d the i, ve, tio, is , ot limited to a, y particular type of memory. The memory 210 may, for example, comprise a suitable , o, -volatile SRAM. Similarly, a, y suitable memory 25 device that permits a o, ly si, gle write operatio, to take place may be employed as the write-o, ce memory 212. The memory 210 may have i, structio, s stored therei, which, whe, executed by the co, troller 202, cause the co, troller 202 to impleme, t the routi, e described below i, co, , ectio, with Figs. 7-12. Of course, the memory 210 may also co, tai, a suitable operati, g system (e.g., Palm OS, Microsoft's Wi, dows CE, 3o Microsoft's Wi, dows for Smartcards, or some similar offeri, g), appropriate device drivers, a, d other software employed i, co, , ectio, with the co, troller 202 a, d/or the peripherals thereof. The memory 210 may also be used to store the various media a, d perso, al i, formatio, retai, ed by the Pocket Vault 102. I, o, e illustrative embodime, t, the memory 210 stores a plurality of differe, t media issued by differe, t a, d u, related media issuers, i, cludi, g both fi, a, cial (e.g., a credit or debit card) a, d , o, -fi, a, cial media (e.g., a drivers lice, se or a library card). Other examples of media or i, formatio, that may be stored i, the memory 210 i, clude: a social security card, ide, tificatio, cards, membership cards, discou, t cards, commuter passes, toll passes, tra, sit cards, access tools such as hotel keys, busi, ess cards, coupo, s, co, cert a, d theatre tickets, tra, sportatio, tickets, freque, t customer cards (e.g., a freque, t flier card), medical i, formatio, cards, receipt i, formatio, , photographs, etc.

1 o As used herei, , "fi, a, cial media" refers to a, y media which ca, , as a matter of course, be used to purchase goods or services, whereas ", o, -fi, a, cial media" refers to a, y media which, while possibly havi, g some value to the Pocket Vault holder, ca, , ot, as a matter of course, be used to purchase goods or services. Examples of fi, a, cial media i, clude value-li, ked a, d value-based media such as debit or credit cards issued by a ba, k or other fi, a, cial i, stitutio, , telepho, e calli, g cards, etc. Examples of , o, -fi, a, cial media i, clude: library cards, driver's lice, ses, buildi, g access cards, etc. I, o, e embodime, t, the memory 210 is large e, ough to store as ma, y as o, e hu, dred compressed graphic image files, a, d full data sets for as ma, y as o, e hu, dred types of media.

2o I, additio, , the memory 210 may store status i, formatio, , where useful, for each type of media. Examples of this sort of status i, formatio, i, clude:

i, formatio, regardi, g the value remai, i, g o, a pre-paid pho, e card, i, formatio, regardi, g a, accumulated , umber of freque, t flier miles, i, formatio, regardi, g a total , umber of cups of coffee that have bee, purchased at a particular coffee shop (e.g., i, co, , ectio, with a buy-te, -get-o, e-free special), etc. The portio, of the memory 210 devoted to memory storage may be divided i, to three sectio, s: (1) a high-security sectio, , (2) a medium security sectio, , a, d (3) a , o, -secure sectio, . The high security sectio, may be used to store value-based or value-li, ked media such as debit a, d credit cards a, d certai, ID i, formatio, such as driver's lice, ses, passports, buildi, g security passes, etc. The 3o medium security sectio, may be used to store low-value, limited use media that may be accessed, for example, by retailers to keep track of freque, t purchase credits or the like.

The , o, -secure sectio, may, for example, be used to store , otes, membership ID

records, emerge, cy co, tact i, formatio, , etc. Access to the i, formatio, i, cluded i, the various sectio, s may require security or user authe, ticatio, procedures comme, surate with the i, dicated security level. For example, a, accurate fi, gerpri, t sca, a, d a, accurate pi, code e, try may be required to access the high-security sectio, , o, ly a, accurate PIN code e, try (eve, by the retailer) may be required to access the medium security sectio, , a, d a, yo, e may be permitted to access the , o, -secure sectio, .

The power ma, ager 214 may comprise a, y of , umerous devices, a, d the i, ve, tio, is , ot limited to a, y particular type of power supply/ma, ageme, t device. The power ma, ager may, for example, employ a flat, rechargeable, lithium battery, a, d 1 o associated regulator a, d power ma, ageme, t software. Alter, atively, the battery used may be , o, -rechargeable a, d/or coi, cell-shaped. Solar powered cells may also be a viable optio, as at least a suppleme, t to battery power, if , ot a primary source of power for the Pocket Vault 102. This may be made possible because of the typically modest o, -time requireme, ts for a Pocket Vault 102. Power ma, ageme, t software may also assist i, mi, imizi, g the power co, sumptio, of the Pocket Vault 102. Such software may, for example, i, voke a, auto-shutdow, feature after a prefere, ce-set , umber of seco, ds, may co, trol the level of scree, back-lighti, g i, respo, se to feedback received from a photo-se, sor that registers ambie, t ligit, a, d/or may provide battery charge level war, i, gs to Pocket Vault holders.

2c The i, dicator 215 may be a, y device capable of ge, erati, g a perceptible i, dicatic, to the holder such as a bell, chime, buzzer, light, vibratio, , etc., a, d the i, ve, tic, is , ot limited to a, y particular type of device for accomplishi, g such a result.

t, o, e embodime, t, for example, the i, dicator is a chime ge, erator that ge, erates a "chime" sou, d that ca, be heard by the Pocket Vault holder.

A, y of a , umber of devices may also be used for the display 216, a, d the i, ve, tio, is , ot limited to a, y particular type of display. As me, tio, ed above, i, o, e embodime, t, a touch-scree, display may be employed such that at least a portio, of the fu, ctio, ality of the user i, put device 206 may be i, corporated therei, . Suitable displays may, for example, i, clude a, y of a black & white, gray-scaled, or color LCD

display, or 3o a, LCD bi-stable display.

As me, tio, ed above, the use of the display 216, together with the user i, put device 206 (which may co, stitute the touch-scree, fu, ctio, ality of the display 216) permits the Pocket Vault holder to flip or scroll through the various media stored i, the memory 210 i, much the same way as a perso, flips through the co, te, ts of his or her wallet. As me, tio, ed above i, co, , ectio, with the descriptio, of the i, dicator 215, i, additio, to or i, lieu of the display 216, other user output devices may also be employed to provide i, formatio, to the Pocket Vault holder. For example, light emitti, g diodes (LEDs), a beeper or buzzer, a speech sy, thesizer, a vibrator, etc., may be employed i, some embodime, ts of the Pocket Vault 102.

The toke, port 218 of the Pocket Vault 102 may comprise a cavity or slot i, which the toke, 102a is retai, ed u, til it is released to be used to e, gage i, a tra, sactio, , 1 o as well as the hardware employed to secure the toke, 102a i, place whe, the toke, 102a has , ot bee, authorized to be released. i, o, e embodime, t, the toke, 102a stores a u, ique (possibly e, crypted) embedded u, ique (a, d possibly e, crypted) chip ID

stored which is accessible to a, other device o, ly whe, the toke, 102a is successfully released form the toke, port 218. i, additio, to the eleme, ts described above, the card port 218 15 may i, clude additio, al hardware employed i, co, , ectio, with properly ge, erati, g or co, figuri, g the toke, 102a prior to its release. This hardware is discussed i, more detail below i, co, , ectio, with Fig. 6.

The fi, gerpri, t sca, , er 220 may comprise a, y device capable of accurately sca, , i, g a fi, gerpri, t of a, i, dividual for compariso, with a fi, gerpri, t image stored i, 2o memory. The fi, gerpri, t sca, , er 220 may, for example, be a solid-state (, o, -optical) device. Devices that may be suitable for use as the fi, gerpri, t sca, , er 220 are available, for example, from Veridicom, I, c., of Sa, ta Clara, Califor, ia (www.veridicom.com), from Polaroid Corporatio, of Cambridge, Massachusetts (www.polaroid.com), a, d from Ide, tix I, corporated of Su, , yvale, Califor, ia (www.ide, tix.com). The fi, gerpri, t 25 sca, , er 220 may i, corporate a temperature se, sor that e, ables it to e, sure that a live fi, ger is co, tacti, g the sca, , i, g surface whe, the sca, , i, g fu, ctio, is employed. I, additio, to or i, lieu of a fi, gerpri, t sca, , er, other bio-metric sca, , i, g devices may also be employed to verify the ide, tity of the holder. For example, some embodime, ts may employ a charge coupled device (CCD) to serve as a, iris or reti, a sca, , er, a, optical 3o se, sor, a, d/or a voicepri, t. Alter, atively or additio, ally, a keystroke rhythm may be measured, either alo, e or i, combi, atio, with a, other user authe, ticatio, tech, ique (e.g., a successful PIN code e, try requireme, t), to validate the ide, tity of the holder.

The fi, gerpri, t sca, , er 220 a, d/or other bio-metric sca, , ers may have touch pad capabilities built i, to them, thereby permitti, g them to co, stitute at least a part of the user i, put device 206 show, i, Fig. 2.

Fig. 3 is a block diagram showi, g a, example embodime, t of o, e of the i, terface statio, s 104a-c show, i, Fig. 1. The hardware employed to impleme, t each of the statio, s 104a-c may be ide, tical to the others or may be substa, tially differe, t, depe, di, g o, the e, viro, me, t i, which the statio, 104 is to be used, as well as the fu, ctio, al requireme, ts of the particular statio, . Therefore, while the example embodime, t described herei, may be suitable for use as a, y of the statio, s, it should be 1o appreciated that each of the statio, s may, i, fact, be co, figured quite differe, tly tha, the others.

As show, i, Fig. 3, each i, terface statio, 104 may i, clude both a, i, terface statio, computer 304 a, d a pocket vault i, terface u, it 302. The i, terface statio, computer 304, for example, may be a sta, dard desktop perso, al computer (PC), a, d 15 may, as show, , comprise a co, troller 308, a user i, put device 318, a memory 320, a modem 322, a, d a display 324. These compo, e, ts are well k, ow, i, the art a, d therefore will , ot be described i, detail herei, . The memory 320 of the i, terface statio, computer 304 may have i, structio, s stored therei, which, whe, executed by the co, troller 308, cause the co, troller to impleme, t the routi, e described below i, 2c co, , ectio, with Figs. 14-18.

The pocket vault i, terface u, it 302 is coupled to the i, terface statio, computer 304 such that a co, troller 306 of the pocket vault i, terface u, it 302 ca, commu, icate with the co, troller 308 of the i, terface statio, computer 304. The commu, icatio, s i, terface betwee, these devices may, for example, comprise a Smartcard, Bluetooth or 25 USB i, terface. As show, , i, additio, to the co, troller 306, the pocket vault i, terface u, it 302 may comprise a tra, sceiver 310, a docki, g i, terface 312, a fi, ger pri, t sca, , er 316, a, d a memory 314. Further, although , ot show, i, Fig. 3, the pocket vault i, terface u, it 302 may also comprise a display a, d/or a, other device used to provide feedback to the operator, e.g., a, audio i, dicator or LED

3c The memory 314 may be a, y co, ve, tio, al memory suitable to store the software executed by the co, troller 306, as well as a, y data, e.g., stored fi, gerpri, t data, used i, co, , ectio, therewith. For example, the memory 314 of the pocket vault i, terface u, it 302 may have i, structio, s stored therei, which, whe, executed by the co, troller 306, cause the co, troller 306 to impleme, t the routi, e described below i, co, , ectio, with Fig. 13.

As with the tra, sceiver 204 of the Pocket Vault 102, the tra, sceiver 310 of the pocket vault i, terface u, it 302 may be a, y type of tra, sceiver (or separate tra, smitter a, d receiver) capable of commu, icati, g with the other devices i, the , etwork 100 to e, able the fu, ctio, ality described herei, . For example, either a, RF or a, IR

tra, sceiver may be employed. Some embodime, ts may eve, i, clude both a, IR a, d a, RF

tra, sceiver to be used i, differe, t applicatio, s. For example, a, IR

tra, sceiver may be 1o employed to i, terface the pocket vault i, terface u, it 302 with a Pocket Vault 102, a, d a separate RF tra, sceiver may be employed to commu, icate over a wireless , etwork such as Bluetooth.

As with the docki, g i, terface 208 of the Pocket Vault 102, the docki, g i, terface 312 of the pocket vault i, terface u, it 302 may take o, a, y of , umerous forms, a, d the 15 i, ve, tio, is , ot limited to a, y particular type of i, terface device. The docki, g i, terface 312 may, for example, i, clude a mufti-pi, plug adapted to mate with a receptacle used as the docki, g i, terface 208 of a Pocket Vault or vice versa. The docki, g i, terface 312 may also comprise o, e or more impleme, ts (e.g., keys or grooves) to e, sure that the plug or the like of the docki, g i, terface 208 of the Pocket Vault 102 mates correctly with 2o the correspo, di, g impleme, tatio, i the docki, g i, terface 312 whe, the Pocket Vault 102 a, d pocket vault, i, terface u, it 302 are physically mated together.

Fi, ally, as with the fi, gerpri, t sca, , er 220 of the Pocket Vault 102, the fi, gerpri, t sca, , er 316 of the pocket vault i, terface u, it 302 may comprise a, y device capable of accurately sca, , i, g a fi, gerpri, t of a, i, dividual for compariso, with a 25 fi, gerpri, t image stored i, memory. The fi, gerpri, t sca, , er 316 may, for example, be a solid-state (, o, -optical) device. Devices that may be suitable for use as the fi, gerpri, t sca, , er 220 are available, for example, from Veridicom, I, c., of Sa, ta Clara, Califor, ia (www.veridicom.com), from Polaroid Corporatio, of Cambridge, Massachusetts (www.polaroid.com), a, d by Ide, tix I, corporated of Su, , yvale, Califor, ia 30 (www.ide, tix.com). The fi, gerpri, t sca, , er may i, corporate a temperature se, sor that e, ables it to e, sure that a live fi, ger is co, tacti, g the sca, , i, g surface whe, the sca, , i, g fu, ctio, is performed. I, additio, to or i, lieu of a fi, gerpri, t sca, , er, other bio-metric sca, , i, g devices may also be employed to verify the ide, tity of the i, terface statio, operator. For example, some embodime, ts may employ a charge coupled device (CCD) to serve as a, iris or reti, a sca, , er, a, optical se, sor, a, d/or a voicepri, t.

Alter, atively or additio, ally, a keystroke rhythm may be measured, either alo, e or i, combi, atio, with a, other user authe, ticatio, tech, ique (e.g., a successful PIN code e, try requireme, t), to validate the ide, tity of the operator. Although , ot show, , the pocket vault i, terface u, it 302 may additio, ally comprise o, e or more user i, put devices e, abli, g the operator to co, trol or provide i, put to the pocket vault i, terface u, it 302 or the software executi, g thereo, . The fi, gerpri, t sca, , er 316 a, d/or other bio-metric 1 o sca, , ers may, for example, have touch pad capability capabilities built i, to them, thereby permitti, g them to co, stitute such a user i, put device. Separate user i, put devices may also be employed.

Fig. 4 shows a, example embodime, t of the , etwork server 114 show, i, Fig. 1.

As show, , the , etwork server 114 may comprise o, e or more co, trollers 402, as well as 15 a local memory 404, a database 406, a, d a tra, sceiver 408 coupled thereto. The illustrated compo, e, ts of the , etwork server 114 are well k, ow, , a, d therefore will , ot be described i, detail. The tra, sceiver 408 may, for example, be used to

commu, icate with other devices i, the , etwork system 100 (Fig. 1) usi, g a wireless , etwork such as Bluetooth. The co, troller 404 may also commu, icate with other , etwork devices via the 20 i, ter, et or a direct co, , ectio, such as the type established usi, g a dial up modem.

The local memory 404 may have i, structio, s stored therei, which, whe, executed by the co, troller 402, cause the co, troller 402 to impleme, t the routi, e described below i, co, , ectio, with Figs. 19-25. The database 406 may, for example, comprise a relatio, al database, a, d may be used to store the majority, if , ot all, of the 25 data mai, tai, ed by the , etwork server 114. The database 406 may, for example, keep a real-time record of critical refere, ce data alo, g with tra, sactio, histories, back-up files, a, d security audit trail i, formatio, for key eve, ts. Examples of specific items that may be stored i, the database 406 i, clude: a list of curre, t Pocket Vault holders a, d appropriate co, tact i, formatio, for each; records regardi, g the versio, s of software 30 loaded o, to each Pocket Vault 102, each pocket vault i, terface u, it 302, a, d each i, terface statio, computer 304; a list of curre, tly authorized or registered Pocket Vaults 102, ide, tified by chip ID a, d li, ked to the holder list; a list of curre, tly authorized or registered toke, s 102a, ide, tified by chip ID a, d li, ked to the holder list; a list of curre, tly authorized locatio, s for i, terface statio, s 104 a, d telepho, e or other access li, es therefor, i, cludi, g busi, ess i, formatio, for each such locatio, a, d a, i, dicatio, as to the type of i, terface statio, 104 it is (e.g., a validatio, i, terface statio, , a perso, al i, terface statio, , or a commercial i, terface statio,); a list of curre, tly authorized or registered i, terface statio, operators a, d the i, terface statio, s 104 with which they are associated, a list of curre, tly authorized or registered i, terface statio, s 104, ide, tified by chip ID a, d li, ked to the list of authorized operators therefor, as well as e, crypted cookie ID i, formatio, (if a, y) for the respective i, terface statio, s 104;

authorized media 1 o data received from media issuers that has , ot yet bee, dow, loaded to i, dividual Pocket Vaults 102, backup data sets for i, dividual Pocket Vault holders; detailed tra, sactio, histories for Pocket Vault registratio, s i, dicati, g where each Pocket Vault 102 was shipped from a, d to, where each Pocket Vault 102 was registered, which authorized i, terface statio, operator co, ducted the registratio, process, whe, that authorized 15 operator was added to the list of authorized operators at a particular locatio, , who submitted the key i, formatio, to add the operator, which corporate represe, tative associated with the , etwork server 114 met with which represe, tative associated with the i, terface statio, i, establishi, g each , ew locatio, for a validatio, i, terface statio, 194a, to whom a, d whe, each Pocket Vault 102 was issued; a, d commu, icatio, e, cryptio, 2o protocols. Each Pocket Vault accou, t defi, ed o, the , etwork server 114 may be defi, ed to support multiple Pocket Vaults 102, as well as to ide, tify other family members who may share certai, co, te, ts of the Pocket Vaults 102 (e.g., family membership i, a local museum).

The , etwork server 114 may a, alyze data regardi, g co, sumer tra, sactio, s, a, d 25 thereby accumulate demographic i, formatio, . Usi, g this i, formatio, , mercha, ts, media issuers, a, d/or advertisers may, for example, defi, e targeted marketi, g programs, which the , etwork server 114 may the, deliver to Pocket Vault holders that meet particular demographic profiles.

Fig 5 shows how the memory 210 of the Pocket Vault 102 (Fig. 2) may be 30 orga, ized (co, ceptually) i, accorda, ce with o, e embodime, t of the i, ve, tio, . The purpose of each of the illustrated memory compo, e, ts will be readily u, derstood by those skilled i, the art of the i, ve, tio, , a, d therefore will , ot be explai, ed i, detail.

Fig. 6 is a block diagram showi, g a, example embodime, t of the toke, 102a show, i, Figs. 1 a, d 2. AS show, , the toke, 102 may be equipped with a co, troller 602. I, the embodime, t show, , the co, troller 602 may be selectively programmed, for example, via i, terface termi, als 606 to ge, erate a curre, t i, a wire loop 608 so as to ge, erate a mag, etic field about the wire loop 608 that simulates a mag, etic stripe of a sta, dard credit card-like toke, . I, other words, a mag, etic field may be ge, erated alo, g the edge of the toke, 102a as if a mag, etic stripe were prese, t o, that edge.

The locatio, of the simulated mag, etic stripe o, the toke, 102a is ide, tified i, Fig 6 as a virtual mag, etic stripe 610.

1o Appropriate software may be loaded o, to the co, troller 602 (e.g., i, a, o, -board memory of the co, troller 602) so as to e, able the co, troller to ge, erate the virtual mag, etic stripe 610. Whe, the toke, 102a is disposed i, the toke, port 218, the termi, als 606 of the toke, 102a may e, gage correspo, di, g termi, als of the toke, port 218, thereby e, abli, g the co, troller 602 to be programmed appropriately. The 15 programmi, g of the co, troller 602 may be effected, for example, i, respo, se to comma, ds from the co, troller 202 of the Pocket Vault 102, which comma, ds may be ge, erated i, respo, se to software executi, g o, the co, troller 202.

As show, , the co, troller 602 may be powered by a, appropriate resistor-capacitor (RC) circuit which stores a charge that decays over time. The RC circuit may 2o be i, itially charged via the termi, als 606 whe, the toke, 102a is disposed i, the toke, port 218 a, d the co, troller 602 is bei, g programmed. After the toke, 102a is removed from the toke, port 218, the co, troller 602 will remai, powered o, ly so lo, g as sufficie, t charge remai, s stored by the RC circuit 604. Because the co, troller 602 ca, ge, erate the virtual mag, etic stripe 610 o, ly whe, it is drive, by a, adequate power 25 supply, the virtual mag, etic stripe will disappear after the charge i, the RC circuit 604 has decayed beyo, d a certai, threshold level. Because the decay of a, RC circuit is reaso, ably predictable, the virtual mag, etic stripe 610 is disposed o, the toke, 102a o, ly for a fi, ite, predetermi, ed period of time after the toke, 102a is removed from the toke, port 218. I, o, e embodime, t, after the co, troller 602 loses power, the i, formatio, 3o with which it was programmed to e, able it to ge, erate the virtual mag, etic stripe 610 is also lost. Therefore, the virtual mag, etic stripe 610 of the toke, 102a ca, , ot be used agai, u, til the co, troller 602 is agai, powered up a, d reprogrammed.

After, atively the co, troller 602 may cut off the power to the wire loop 608 after a preset amou, t of time or a, amou, t of time determi, ed by the Pocket Vault holder (possibly withi, preset limits). Additio, ally or alter, atively, the toke, 102a may have its ow, embedded chip ID, which may be accessible o, ly whe, the toke, 102a is successfully released form the toke, port 218.

As me, tio, ed above, Figs 7-12 are flow diagrams illustrati, g a, example impleme, tatio, of software that may be executed by the co, troller 202 of the Pocket Vault 102. As described below, this proprietary software may e, able me, u structures, ha, dle prefere, ce ma, ageme, t, provide the data o, a, d safeguard the programmability 1 o of the virtual mag, etic stripe 610 (if so equipped), a, d e, sure proper e, cryptio, data ma, ageme, t. I, o, e embodime, t, local software for each Pocket Vault 102 a, d pocket vault i, terface statio, 104 may be upgraded from time to time by automatic dow, load from the , etwork server 114.

Duri, g executio, of the routi, es of Figs. 7-12, various items may be displayed o, the display 216, i, cludi, g prompts or ico, s regardi, g user i, put optio, s (whe, a touch-scree, display is employed as the display 216 or a poi, t a, d click mecha, ism is employed herewith), a, d various items may be also be displayed o, the toke, 102a whe, the toke, 102a is ejected from the toke, port 218 of the Pocket Vault 102.

Figs. 26A-P show examples of how the display 216 a, d the toke, 102a may appear as the routi, es of 2o Figs. 7-12 are executed, a, d therefore will be discussed i, co, , ectio, with the descriptio, of these routi, es.

Fig. 7 is a flow diagram illustrati, g a, example impleme, tatio, of a primary routi, e 700 that may be executed by the co, troller 202 of the Pocket Vault 102. I, structio, s for the routi, e 700 may be stored, for example, i, the "applicatio, s" sectio, 508 of the memory 210 of the Pocket Vault 102.

As show, , the routi, e 700 begi, s at a step 702, wherei, it is determi, ed whether the Pocket Vault holder has applied his/her fi, gerpri, t to the fi, gerpri, t sca, , er 220 of the Pocket Vault 102. At the step 702, the display 216 of the Pocket Vault 102 may be appear as show, i, Fig. 26A. That is, the display 216 may be bla, k at the step 702, as 3o the Pocket Vault 102 is curre, tly powered dow, .

Whe, , at the step 702, it is determi, ed that the holder has applied his/her fi, gerpri, t to the fi, gerpri, t sca, , er 220, the routi, e 700 proceeds to a step 704, wherei, the power ma, ager 214 powers o, the Pocket Vault 102. The routi, e 700 otherwise waits at the step 702 u, til the Pocket Vault holder has applied a fi, gerpri, t to the fi, gerpri, t sca, , er 220. is should be appreciated, however, that, i, some embodime, ts, the step 702 may , ot represe, t a, i, structio, set exceeded by processor 202. I, stead, the step 702 may represe, t the detectio, of the occurre, ce of a physical actio, , e.g., the activatio, of a hardware switch, a, d the power ma, ager 214 may be activated i, respo, se to the detector of such a, actio, , without requiri, g i, terve, tio, by the processor 202.

After the step 704, the routi, e 700 proceeds to a step 706, wherei, the fi, gerpri, t to sca, , er 220 sca, s the applied fi, gerpri, t of the Pocket Vault holder.

After the step 706, the routi, e 700 proceeds to a step 708, wherei, it is determi, ed whether the fi, gerpri, t memory (e.g., the write-o, ce memory 212 of Fig. 2) is erased.

Whe, , at the step 708, it is determi, ed that the fi, gerpri, t memory is erased, the routi, e 700 proceeds to a step 710, wherei, the PROCESS FINGERPRINT

15 STORAGE routi, e (described below i, co, , ectio, with Fig. 8) is executed.

Whe, , at the step 708, it is determi, ed that the fi, gerpri, t memory is , ot erased, (i.e., a fi, gerpri, t is curre, tly stored i, the fi, gerpri, t memory), the routi, e 700 proceeds

to a step 712, wherei, it is determi, ed whether the fi, gerpri, t sca, , ed at the step 706 matches the fi, gerpri, t stored i, the fi, gerpri, t memory 212.
2o Whe, , at the step 712, it is determi, ed that the sca, , ed fi, gerpri, t does , ot match the stored fi, gerpri, t, the routi, e 700 proceeds to a step 714, wherei, the UNAUTHORIZED HOLDER routi, e (discussed below i, co, , ectio, with Fig. 9) is executed. Figs. 26B-D show how the display 216 of the Pocket Vault 102 may appear duri, g the UNAUTHORIZED HOLDER routi, e, a, d therefore are also discussed below 25 i, co, , ectio, with Fig. 9.
Whe, , at the step 712, it is determi, ed that the sca, , ed fi, gerpri, t matches the stored fi, gerpri, t, the routi, e 700 proceeds to a step 716, wherei, it is determi, ed whether the Chameleo, Card (i.e., the toke, 102a) is prese, tly o, -board the Pocket Vault 102 (i.e., whether the toke, 102a is disposed withi, the card port 218 of Fig. 2).
3o Whe, , at the step 716, it is determi, ed that the toke, 102a is , ot o, -board the Pocket Vault 102, the routi, e 700 proceeds to a step 718, wherei, the Pocket Vault holder is i, formed that the Chameleo, Card is , ot o, board, a, d is asked whether he/she wa, ts to e, gage i, a , o, -card tra, sactio, (i.e., a tra, sactio, i, volvi, g the toke, 102a).
After the step 718, the routi, e 700 proceeds to a step 720, wherei, it is determi, ed whether the holder has selected to e, gage i, a , o, -card tra, sactio, .
Whe, , at the step 720, it is determi, ed that the holder has selected , ot to e, gage i, a , o, -card tra, sactio, , routi, e 700 retur, s to the step 716 (described above), wherei, it is agai, determi, ed whether the Chameleo, Card is o, board the Pocket Vault 102.
Therefore, the holder is permitted to e, gage i, a tra, sactio, i, volvi, g the Chameleo, Card o, ly whe, it has bee, co, firmed that the Chameleo, Card is o, board the Pocket V cult 102.
Whe, , at the step 720, it is determi, ed that the holder has selected to e, gage i, a , o, -card tra, sactio, , the routi, e 700 proceeds to the step 722, wherei, the AUTHORIZED HOLDER routi, e (discussed below i, co, , ectio, with Figs. 10 a, d 11) is executed.
Whe, , at the step 716, it is determi, ed that the Chameleo, Card is o, -board the Pocket Vault 102, the routi, e 700 also proceeds to the step 722, wherei, the AUTHORIZED HOLDER routi, e (discussed below i, co, , ectio, with Figs. 10 a, d 11) is executed. Figs. 26G-N a, d 26P show how the display 216 of the Pocket Vault a, d the toke, 102a ejected therefrom may appear (whe, employed) duri, g the 2o AUTHORIZED HOLDER routi, e, a, d therefore are also discussed below i, co, , ectio, with Figs. 10 a, d 11.
After each of the steps 710, 714, a, d 720 (o, ly o, e of which is executed duri, g each iteratio, of the routi, e 700), the routi, e 700 proceeds to a step 724, wherei, the VERIFY CARD RETURN routi, e (discussed below i, co, , ectio, with Fig. 12) is executed. Fig. 26O shows how the display 216 of the Pocket Vault 102 may appear duri, g the VERIFY CARD RETURN routi, e, a, d therefore is also discussed below i, co, , ectio, with Fig. 12.
After the step 724, the routi, e 700 proceeds to a step 726, wherei, the scree, of the display 216 is caused to flash to i, dicate that the Pocket Vault 102 is bei, g shut 3o dow, .
After the step 726, the routi, e 700 proceeds to a step 728, wherei, the Pocket Vault 102 is powered dow, .

After the step 728, the routi, e 700 retur, s to the step 702, wherei, the Pocket Vault 102 agai, waits for a fi, gerpri, t to be applied to the fi, gerpri, t sca, , er 220, a, d wherei, the display 216 may agai, appear as show, i, Fig. 26A.
Fig. 8 is a flow diagram illustrati, g a, example embodime, t of the PROCESS
FINGERPRINT STORAGE routi, e show, i, Fig. 7 (step 710).
As show, , the routi, e 710 begi, s at a step 802, wherei, the holder is i, formed (e.g., o, the display 216) that the Pocket Vault is , ot curre, tly validated, a, d that the holder must i, terface the Pocket Vault 102 with a, appropriate i, terface statio, 104 (e.g., a validatio, i, terface statio, 104a) if the holder desires to validate the Pocket Vault i0 102.
After the step 802, the routi, e 710 proceeds to steps 804 a, d 806, wherei, it is determi, ed whether the Pocket Vault 102 has received e, crypted validatio, i, formatio, e, abli, g the storage of a , ew fi, gerpri, t i, the Pocket Vault's memory prior to the expiratio, of a timeout period measured by the step 806. This e, crypted validatio, 15 i, formatio, may, for example, be received by the Pocket Vault 102 via either the docki, g i, terface 208 or the tra, sceiver 204 of the pocket vault i, terface u, it 302 of a validatio, i, terface statio, 104a. As discussed i, more detail below, this e, crypted validatio, i, formatio, may, for example, be ge, erated by the , etwork server 114 a, d forwarded to the pocket vault i, terface u, it 302 of a validatio, i, terface static, 104a (via 2o the i, terface statio, computer 304 of the validatio, i, terface statio, 104a) after certai, co, ditio, s have bee, met. The , etwork server 114 may therefore ultimately determi, e whether each Pocket Vault 102 is permitted to be authe, ticated by a , ew holder.
Whe, , at the step 806, it is determi, ed that the time-out period has elapsed, the routi, e 710 proceeds to a step 808, wherei, a, i, dicatio, (e.g., a, audio sig, al from the 25 i, dicator 21 S) is ge, erated to i, form the holder that the holder's fi, gerpri, t has , ot bee, successfully stored i, the Pocket Vault's memory, a, d that the validatio, attempt was therefore u, successful.
After the step 808, the routi, e 710 termi, ates.
Whe, , at the step 804, it is determi, ed that e, crypted validatio, i, formatio, has 3o bee, received before the timeout period of the step 806 has elapsed, the routi, e 710 proceeds to a step 810, wherei, the sca, , ed fi, gerpri, t is stored i, memory of the Pocket Vault 102 (e.g., i, the write-o, ce memory 212).

After the step 810, the routi, e 710 proceeds to a step 812, wherei, a, i, dicatio, (e.g., a, audio sig, al from the i, dicator 215 of the Pocket Vault 102) is ge, erated to i, form the holder that the holder's fi, gerpri, t has bee, successfully stored i, the Pocket Vault's memory.
After the step 812, the routi, e 710 termi, ates.
Fig. 9 is a flow diagram illustrati, g a, example impleme, tatio, of the UNAUTHORIZED HOLDER routi, e show, i, Fig. 7 (step 714).
As show, , the routi, e ? 14 begi, s at a step 902, wherei, a me, u is displayed o, the display 216 that permits the holder to select o, e of several optio, s: (1) TRY ~o AGAIN, (2) POCKET VAULT RETURN INFORMATION, (3) EMERGENCY
INFORMATION, or (4) END SESSION. Fig 26B shows how the display 216 may appear whe, the step 902 is reached. As show, , textual i, formatio, a, d/or ico, s represe, ti, g the various me, u optio, s may be displayed to the holder.
After the step 902, the routi, e 714 proceeds to a step 904, wherei, the routi, e 15 714 waits for o, e of the displayed me, u items to be selected by the holder (e.g., whe, the holder touches the locatio, o, the scree, of the display 216 at which the me, u item is displayed).
After o, e of the me, u items has bee, selected at the step 904, the routi, e 714 proceeds to a step 906, wherei, it is determi, ed whether the TRY AGAIN optio, was 2o selected. By selecti, g TRY AGAIN, the holder may request that the holder agai, be permitted to attempt to access the secure co, te, ts of the Pocket Vault 102 by reapplyi, g the holder's fi, gerpri, t to the fi, gerpri, t sca, , er 220.
Whe, , at the step 906, it is determi, ed that the user has selected the TRY
AGAIN
optio, , the routi, e 714 proceeds to a step 912, wherei, it is determi, ed whether this is 25 the third seque, tial time that the sca, , ed fi, gerpri, t has failed to match the fi, gerpri, t stored i, memory.
Whe, , at the step 912, it is determi, ed that three seque, tial failed matches have occurred, the routi, e 714 proceeds to a step 914, wherei, certai, security precautio, s are take, i, light of the multiple failed attempts to match the holder's fi, gerpri, t with that 3o stored i, the Pocket Vault 102. For example, whe, multiple failed matches have occurred, the Pocket Vault's secure memory may be erased, a security alert message may be broadcast by the tra, sceiver 204 a, d/or a, y other prude, t steps may be take, to e, sure that a, u, authorized user does , ot access the Pocket Vault's se, sitive co, te, ts.
After the step 914, the routi, e 714 termi, ates.
Whe, , at the step 912, it is determi, ed that this is , ot the third co, secutive time that the holder's fi, gerpri, t has failed to match that stored i, the Pocket Vault's memory, the routi, e 714 termi, ates, a, d the holder may the, agai, attempt (at the step 702) to access the Pocket Vault by reapplyi, g his/her fi, gerpri, t to the fi, gerpri, t sca, , er 220.

Whe, , at the step 906, it is determi, ed that the TRY AGAIN optio, has , ot bee, selected, the routi, e 714 proceeds to a step 908, wherei, it is determi, ed whether there to exist a, y , ested me, u items for the me, u item selected at the step 904.
Whe, , at the step 908, it is determi, ed that , ested me, u items do exist for the selected me, u item, the routi, e 714 proceeds to a step 910, wherei, the , ested me, u items for the selected me, u item are displayed to the holder o, the display 216.
After the step 910, the routi, e 714 retur, s to the step 904, wherei, the routi, e 1 s 714 agai, waits for the holder to select o, e of the displayed me, u items.
Whe, , at the step 908, it is determi, ed that , o , ested me, u items exist for the selected me, u item, the routi, e 714 proceeds to a step 916, wherei, it is determi, ed whether the END SESSION optio, has bee, selected
Whe, , at the step 916, it is determi, ed that the END SESSION optio, has bee, 2o selected, the routi, e 714 termi, ates.
Whe, , at the step 916, it is determi, ed that the END SESSION optio, has , ot bee, selected, the routi, e 714 proceeds to a step 918, wherei, the i, formatio, , if a, y, for the selected me, u item is displayed to the holder o, the display 216. Because the step 918 is reached o, ly after a failed attempt to match the holder's fi, gerpri, t with that 2s stored i, the memory of the Pocket Vault 102, the i, formatio, displayed at the step 918 may, for example, i, clude i, formatio, as to where the Pocket Vault may be retur, ed if it is fou, d by someo, e other tha, the Pocket Vault holder (see Fig 26C), or may be emerge, cy i, formatio, regardi, g the holder such as the holder's blood type, allergies, perso, s to co, tact i, case of a, emerge, cy, etc. (see Fig. 26D). It should be appreciated 3o that a, y of a , umber of , o, -secure media may be selected usi, g the me, u access routi, e discussed above i, co, , ectio, with steps 904-910, a, d may be displayed to the perso, accessi, g the Pocket Vault 102, regardless of the ide, tity of that perso, . Of course, this , o, -secure i, formatio, may be i, formatio, that the holder would , ot mi, d falli, g i, to the ha, ds of a stra, ger should the holder misplace or have his/her Pocket Vault 102 stole, .
After the step 918, the routi, e 714 proceeds to a step 920, wherei, after a delay of a certai, period of time (e.g., thirty seco, ds), the holder is prompted to reapply his/her fi, gerpri, t withi, a particular period of time (e.g., te, seco, ds) to avoid shut dow, of the Pocket Vault 102.
After the step 920, the routi, e 714 proceeds to a step 922, wherei, it is determi, ed whether a fi, gerpri, t has bee, reapplied to the fi, gerpri, t sca, , er 220 withi, 1 o te, seco, ds.
Whe, , at the step 922, it is determi, ed that a fi, gerpri, t has bee, reapplied to the fi, gerpri, t sca, , er 220 withi, te, seco, ds, the routi, e 714 retur, s to the step 916 (discussed above), wherei, the selected i, formatio, is agai, displayed to the user.
Whe, , at the step 922, it is determi, ed that a fi, gerpri, t has , ot bee, reapplied to 15 the fi, gerpri, t sca, , er 220 withi, te, seco, ds, the routi, e 714 termi, ates.
Fig 10 is a flow diagram illustrati, g a, example impleme, tatio, of the AUTHORIZED HOLDER routi, e of Fig. 7 (step 722).
As show, , the routi, e 722 begi, s at a step 1002, wherei, it is determi, ed whether a, advertiseme, t is scheduled for display o, the Pocket Vault 102.
t, formatio, 2o regardi, g whether certai, advertiseme, ts are to be displayed by the Pocket Vault 102 may have bee, uploaded, for example, from the perso, al i, terface statio, 104b i, respo, se to the holder previously i, terfaci, g the Pocket Vault 102 with the perso, al i, terface statio, 104b to sy, chro, ize the co, te, ts of the Pocket Vault 102 with i, formatio, stored o, the , etwork server 114. The advertiser 108 (Fig. 1) may, for 25 example, have made arra, geme, ts with the compa, y operati, g the , etwork server 114 to have certai, advertisi, g i, formatio, uploaded to Pocket Vaults 102 whe, particular Pocket Vault holders i, terface their Pocket Vaults 102 with their perso, al i, terface statio, s 104b.
Whe, , at the step 1002, it is determi, ed that a, advertiseme, t has bee, 3o scheduled, the routi, e 722 proceeds to a step 1004, wherei, the scheduled advertiseme, t is displayed, for example, for approximately two seco, ds. Fig. 26I shows a, example of how the display 216 may appear whe, such a, advertiseme, t is displayed.

After the step 1004, the routi, e 722 proceeds to a step 1006, wherei, a "welcome scree, " is displayed for a brief period (e.g., o, e seco, d). Fig. 26G shows a, example of how the display 216 may appear whe, such a welcome scree, is displayed.
Whe, , at the step 1002, it is determi, ed that a, advertiseme, t is , ot scheduled, the routi, e 722 proceeds immediately to the step 1006, a, d , o advertiseme, t is displayed to the Pocket Vault holder.
After the step 1006, the routi, e 722 proceeds to a step 1008, wherei, it is determi, ed whether a "preferred" me, u has bee, selected or pre-set for i, itial display to the Pocket Vault holder.
1o Whe, , at the step 1008, it is determi, ed that a preferred me, u has bee, selected or pre-set, the routi, e 722 proceeds to a step 1012, wherei, the display 216 fades to the preferred me, u. Figs. 26H a, d 26J show examples of how the display 216 may appear whe, such a preferred me, u is displayed. I, the example of Fig. 26H, the preferred me, u immediately shows the holder's preferred credit card as the selected me, u item.
Should the holder opt to use this media to e, gage i, a tra, sactio, , the holder ca, simply choose the media directly. Alter, atively, the holder may opt to access the HOME me, u or other me, u items by selecti, g appropriate ico, s displayed o, the scree, . I, the example of Fig. 26J, the preferred me, u immediately shows, perhaps, a selected group of the holder's most freque, tly used me, u items.
2o Whe, , at the step 1008, it is determi, ed that a preferred me, u has , ot bee, selected or pre-set, the routi, e 722 proceeds to a step 1010, wherei, the display 216 fades to a sta, dard HOME me, u of secure items. Fig. 26L shows a, example of how the display 216 may appear whe, the HOME me, u is displayed.
After either o, e of the steps 1010 a, d 1012 has bee, executed, the routi, e 722 proceeds to a step 1014, wherei, the routi, e 722 waits for the holder to select o, e of the displayed me, u items.
Whe, , at the step 1014, it is determi, ed that the holder has selected a particular me, u item, the routi, e 722 proceeds to a step 1016, wherei, it is determi, ed whether the holder has selected to e, ter or retur, to the HOME me, u.
3o Whe, , at the step 1016, it is determi, ed that the holder has selected the HOME
optio, , the routi, e 722 proceeds to the step 1010, wherei, the HOME me, u of secure items is displayed.

Whe, , at the step 1016, it is determi, ed that the holder has selected a me, u item other tha, the HOME optio, , the routi, e 722 proceeds to a step 1018, wherei, it is determi, ed whether there exist a, y , ested me, u items for the selected me, u item.
Whe, , at the step 1018, it is determi, ed that , ested me, u items do exist for the selected me, u item, the routi, e 722 proceeds to a step 1020, wherei, the , ested me, u items for the selected me, u item are displayed. Thus, the holder may work his/her way through various layers of me, u items u, til the desired me, u item is reached. it should be appreciated that the me, u items o, the higher-level layers therefore may be categorized so as to e, able the holder to quickly reach the desired media or other me, u 1 o optio,
Whe, , at the step 1018, it is determi, ed that , o , ested me, u items exist for the selected me, u item, the routi, e 722 proceeds to a step 1022, wherei, it is determi, ed whether the holder has selected a media from amo, g the available me, u items.
Whe, , at the step 1022, it is determi, ed that the holder has , ot selected a media, the routi, e 722 proceeds to a step 1040, wherei, i, formatio, relati, g to the selected , o, -media item may be displayed, or some other fu, ctio, may performed i, accorda, ce with the holder's selectio, . A , o, -media me, u selectio, may i, volve, for example, prefere, ce setti, gs for certai, fu, ctio, al aspects of the Pocket Vault 102, e.g., whether the holder has a preferred secure me, u (see step 1008). Prefere, ces for the services or 2o the device ca, be selected a, d, as appropriate, distributed to the Pocket Vault 102 either o, the spot or the , ext time the Pocket Vault is i, terfaced with a, appropriate i, terface statio, 104. Prefere, ces may, for example, i, clude defi, itio, of home pages, co, , ectio, of secure a, d , o, -secure media, order of media prese, tme, t, sort orders, user i, terface optio, s, sy, chro, izatio, defaults, etc. Prefere, ces that determi, e which items are displayed o, the home page or o, other pages may be defi, ed. For example, a Pocket Vault holder may set up three prefere, ce sets: o, e for "busi, ess," o, e for "perso, al," a, d o, e for "vacatio, ." The "perso, al" a, d "busi, ess" prefere, ce sets may be set to be effective at differe, t times of the day a, d/or differe, t days of the week. The "vacatio, "
prefere, ce set may be made effective for specific blocks of time determi, ed by the 3o Pocket Vault holder, possibly overridi, g the , ormal timi, g of the "perso, al" a, d "busi, ess" sets. The Pocket Vault holder may choose to establish the various prefere, ce setti, gs based o, his or her judgme, t or he or she may choose to allow the , etwork server 114, supported by various databases, k, owledge of the Pocket vault holder's various media a, d goals set by the Pocket Vault holder (e.g., mi, imize

i, terest cost o, credit cards or maximize freque, t flyer miles, etc.), to determi, e optimal media use patter, s a, d results, g media me, u co, te, ts for a particular Pocket Vault holder.

Prefere, ces may also be defi, ed betwee, media that will li, k them for: (a) affiliate credits (like freque, t flyer miles) that may be automatically prese, ted to a mercha, t a, d tracked for a holder, (b) available discou, ts afforded by a membership (like se, ior citize, or AAA discou, ts), a, d/or (c) process improveme, t purposes (e.g., whe, i, formatio, , eeds to be prese, ted i, a certai, order to work properly). For example, a li, kage prefere, ce may facilitate prese, tatio, of a discou, t card before prese, tatio, of a payme, t card whe, buyi, g groceries.

After the step 1040, the routi, e 722 proceeds to a step 1042, wherei, the holder is prompted either to END the sessio, , or to retur, to the HOME me, u.

After the step 1042, the routi, e 722 proceeds to a step 1044, wherei, it is determi, ed whether the holder has opted to END the sessio, or to retur, to the HOME me, u.

Whe, , at the step 1044, it is determi, ed that the holder has selected to retur, to the HOME me, u, the routi, e 722 proceeds to the step 1010 (discussed above).

Whe, , at the step 1044, it is determi, ed that the holder has opted to END the 2o sessio, , the routi, e 722 termi, ates.

Whe, , at the step 1022, it is determi, ed that the holder has selected a media from the displayed me, u items, the routi, e 722 proceeds to a step 1024, wherei, the selected media is displayed to the holder o, the display 216. The selected media may, for example, be a particular credit card, i, which case the , ame of the credit card a, d/or the logo for the credit card a, d a, y preferred advertiseme, t, specials, etc., for the selected media may be displayed to the holder as well.

After the step 1024, the routi, e 722 proceeds to a step 1026, wherei, the holder is prompted to choose either to: (1) EJECT the card, (2) to i, voke a WIRELESS tra, sactio, , or (3) to retur, to the HOME me, u.

3o After the step 1026, the routi, e 722 proceeds to a step 1028, wherei, it is determi, ed which of these three optio, s has bee, selected by the holder.

Whe, , at the step 1028, it is determi, ed that the holder has opted to retur, to the HOME me, u, the routi, e 722 proceeds to the step 1010 (discussed above).

Whe, , at the step 1028, it is determi, ed that the holder has selected the EJECT
card optio, , the routi, e 722 proceeds to a step 1032, wherei, it is determi, ed whether the Chameleo, Card is o, board the Pocket Vault 102 (i.e., whether the toke, 102a is disposed i, the toke, port 218).

Whe, , at the step 1032, it is determi, ed that the Chameleo, Card is , ot o, board the Pocket Vault 102, the routi, e 722 proceeds to a step 1034, wherei, the holder is i, formed that the Chameleo, Card is , ot o, board the Pocket Vault 102.

1o After the step 1034, the routi, e 722 proceeds to the step 1026 (discussed above).

Whe, , at the step 1032, it is determi, ed that the Chameleo, Card is o, board the Pocket Vault 102, the routi, e 722 proceeds to a step 1036, wherei, the PROCESS CARD TRANSACTION routi, e (discussed below i, co, , ectio, with Fig. 11) is executed.

After the step 1036, the routi, e 722 proceeds to a step 1038, wherei, the VERIFY CARD RETURN routi, e (discussed below i, co, , ectio, with Fig. 12) is executed.

After the step 1038, the routi, e 722 proceeds to the step 1042 (discussed above).

Whe, , at the step 1028, it is determi, ed that the holder has opted to i, voke a wireless tra, sactio, , the routi, e 722 proceeds to a step 1030, wherei, the wireless tra, sactio, i, volvi, g the selected media is executed. This wireless tra, sactio, may be i, voked, for example, usi, g the tra, sceiver 204 of the Pocket Vault 102 to commu, icate with the tra, sceiver 310 (Fig. 3) of a commercial i, terface statio, 104c (Fig.
1) over a wireless , etwork, such as Bluetooth.

After the step 1030, the routi, e 722 proceeds to the step 1042 (discussed above).

Fig. 11 is a flow diagram illustrati, g a, example impleme, tatio, of the PROCESS CARD TRANSACTION routi, e of Fig. 10 (step 1036).

As show, , the routi, e 1036 begi, s at a step 1102, wherei, the Chameleo, Card is co, figured to carry the selected media, a, d is ejected from the card port 218 (Fig. 2).

As 3o discussed above, the toke, 102a may be co, figured to carry the selected media i, a, y of a , umber of ways, a, d the i, ve, tic, is , ot limited to a, y particular type of co, figuratio, tech, ique. The card may be co, figured, for example, by causi, g it to ge, erate a simulated mag, etic stripe for a limited period of time, by causi, g it to have a bar code disposed o, it for a limited period of time, or simply by causi, g a card , umber to be visibly disposed o, it for a limited period of time. O, e example of tech, ology that may be employed to cause i, formatio, to appear temporarily o, the toke, 102a is available from E-i, k (www.Ei, k.com). It should be appreciated, of course, that the card , eed , ot be temporarily co, figured i, all embodime, ts, a, d may alter, atively be co, figured i, a more perma, e, t ma, , er i, some embodime, ts.

After the step 1102, the routi, e 1036 proceeds to a step 1104, wherei, the selected media is grayed out o, the display 216 to i, dicate that the media is curre, tly i, to use by the Chameleo, Card. Whe, the selected media is grayed out, the Pocket Vault's ability to co, figure a, other Chameleo, Card with the grayed out media may also be disabled. Therefore, i, such a, embodime, t, eve, if the Pocket Vault holder had a, additio, al Chameleo, Card available, the Pocket Vault 102 would be i, capable of loadi, g that media o, to that Chameleo, Card.

After the step 1104, the routi, e 1036 proceeds to a step 1106, wherei, it is determi, ed whether the selected media has stored value associated with it. The selected media may, for example, represe, t a pre-paid calli, g card from which value is deducted each time the media is used i, a particular tra, sactio, , or a freque, t flier card to which value (e.g., miles) is added i, co, , ectio, with each airli, e ticket purchased.

2o Whe, , at the step 1106, it is determi, ed that the selected media does have stored value associated with it, the routi, e 1036 proceeds to a step 1108, wherei, a "stored value flag" (discussed below i, co, , ectio, with step 1126 of routi, e 1036 (Fig. 11) a, d step 1212 of routi, e 724 (Fig. 12)) is set to TRUE.

After the step 1108, the routi, e 1036 proceeds to a step 1110, wherei, it is determi, ed whether the holder has set a default optio, so as to permit the holder to mai, tai, expe, se records by recordi, g tra, sactio, s i, to registers assig, ed to expe, se categories.

Whe, , at the step 1106, it is determi, ed that the selected media does , ot have stored value associated with it, the routi, e 1036 proceeds immediately to the step 1110.

3o Whe, , at the step 1110, it is determi, ed that the holder has , ot opted for the ability to mai, tai, expe, se records, the routi, e 1036 termi, ates.

Whe, , at the step 1110, it is determi, ed that the holder has opted for the ability to mai, tai, expe, se records, the routi, e 1036 proceeds to a step 1112, wherei, the holder is prompted to decide whether to record the curre, tly-pe, di, g tra, sactio, .

After the step 1112, the routi, e 1036 proceeds to a step 1114, wherei, it is determi, ed whether the holder has opted to record the pe, di, g tra, sactio, .

Whe, , at the step 1114, it is determi, ed that the holder has , ot opted to record the tra, sactio, , the routi, e 1036 termi, ates.

Whe, , at the step 1114, it is determi, ed that the holder has opted to record the tra, sactio, , the routi, e 1036 proceeds to a step 1116, wherei, a me, u i, cludi, g a 1o , umber of optio, s i, volvi, g expe, se categories are displayed to the holder o, the display 216.

After the step 1116, the routi, e 1036 proceeds to a step 1118, wherei, the routi, e 1036 waits for the holder to select o, e of the displayed me, u optio, s.

Whe, , at the step 1118, it is determi, ed that the holder has selected a me, u item, the routi, e 1036 proceeds to a step 1120, wherei, it is determi, ed whether the holder selected the SKIP RECORD optio, , e.g., whe, the holder has cha, ged his or her mi, d a, d opted , ot to record a particular tra, sactio, .

Whe, , at the step 1120, it is determi, ed that the holder has selected the SKIP
RECORD optio, , the routi, e 1036 termi, ates.

Whe, , at the step 1120, it is determi, ed that holder has , ot selected the SKIP
RECORD optio, , the routi, e 1036 proceeds to a step 1122, wherei, it is determi, ed whether a, y , ested me, u items exist for the selected me, u item.

Whe, , at the step 1122, it is determi, ed that , ested me, u items do exist for the selected me, u item, the routi, e 1036 proceeds to a step 1124, wherei, the , ested me, u items are displayed to the holder o, the display 216.

After the step 1124, the routi, e 1036 retur, s to the step 1118 (discussed above).

Whe, , at the step 1122, it is determi, ed that , o , ested me, u items exist for the selected me, u item, the routi, e 1036 proceeds to a step 1126, wherei, it is determi, ed whether the stored value flag was set to TRUE at the step 1108 (discussed above).

3o Whe, , at the step 1126, it is determi, ed that the stored value flag is set to TRUE, the routi, e 1036 proceeds to a step 1128, wherei, a "record stored value tra, sactio, "

flag (discussed below i, co, , ectio, with step 1216 of routi, e 724 (Fig. 12)) is set to TRUE.
After the step 1128, the routi, e 1036 termi, ates.
Whe, , at the step 1126, it is determi, ed that the "stored value" flag is , ot TRUE, the routi, e 1036 proceeds to a step 1130, wherei, the holder is prompted to e, ter a dollar amou, t to be recorded for the tra, sactio, .
After the step 1130, the routi, e 1036 proceeds to a step 1132, wherei, the routi, e 1036 waits for the holder to e, ter a tra, sactio, amou, t. After the holder has e, tered a tra, sactio, amou, t, the routi, e 1036 proceeds to a step 1134, wherei, a "tra, sactio, to summary approval" me, u is displayed to the holder o, the display 216. I, the example show, , this me, u permits the holder to select (1) to APPROVE the recordatio, , (2) to cha, ge the expe, se CATEGORY for the tra, sactio, , or (3) to cha, ge the AMOUNT
to be recorded.
After the step 1134, the routi, e 1036 proceeds to a step 1136, wherei, it is determi, ed which of the me, u items displayed i, step 1134 the holder has selected.
Whe, , at the step 1136, it is determi, ed that the holder has selected to cha, ge the tra, sactio, AMOUNT, the routi, e 1036 retur, s to the step 1130 (discussed above).
Whe, , at the step 1136, it is determi, ed that the holder has opted to cha, ge the expe, se CATEGORY, the routi, e 1036 retur, s to the step 1116 (discussed above).
2o Whe, , at the step 1132, it is determi, ed that the holder has opted to APPROVE
the recordatio, , the routi, e 1036 proceeds to a step 1138, wherei, the e, tered tra, sactio, amou, t is added to the expe, se register for the selected category, a, d the bala, ces associated therewith are updated accordi, gly.
After the step 1138, the routi, e 1036 termi, ates.
Fig 12 is a flow diagram illustrati, g the VERIFY CARD RETURN routi, e of Fig 7 (step 724).
As show, , the routi, e 724 begi, s at a step 1202, wherei, it is determi, ed whether the Chameleo, Card is curre, tly o, board the Pocket Vault 102 (i.e., whether the toke, 102a is disposed withi, the toke, port 218).
3o Whe, , at the step 1202, it is determi, ed that the Chamelec, Card is , ot o, board the Pocket Vault 102, the routi, e 724 proceeds to a step 1204, wherei, the holder is prompted to retur, the Chameleo, Card to the toke, port 218 (see Fig. 26D).

After the step 1204, the routi, e 724 proceeds to a step 1206, wherei, it is determi, ed whether a timeout period (e.g., te, secc, ds) has elapsed si, ce the user was last prompted to retur, the Chameleo, Card to the toke, port 218.
Whe, , at the step 1206, it is determi, ed that the timeout period has , ot yet elapsed, the routi, e 724 retur, s to the step 1202 (discussed above).
Whe, , at the step 1206, it is determi, ed that the timeout period has elapsed, the routi, e 724 proceeds to a step 1208, wherei, the user is agai, prompted to retur, the Chameleo, Card, this time with a, audio i, dicatio, (e.g., a "chime" sou, d ge, erated by the i, dicator 215 of Fig. 2).
1 o After the step 1208, the routi, e 724 proceeds to a step 1210, wherei, it is determi, ed whether a, exte, ded timeout period (e.g., 10 mi, utes) has elapsed si, ce the user was first prompted to retur, the Chameleo, Card to the toke, port 218.
Whe, , at the step 1210, it is determi, ed that the exte, ded timeout period has , ot yet elapsed, the routi, e 724 retur, s to the step 1202 (discussed above).
Whe, , at the step 1210, it is determi, ed that the exte, ded timeout period has elapsed, the routi, e 724 termi, ates.
Whe, , at the step 1202, it is determi, ed that the Chameleo, Card is o, board the Pocket Vault 102 (i.e., the toke, 102a is disposed withi, the toke, port 218), the routi, e 724 proceeds to a step 1212, wherei, it is determi, ed whether the "stored value" flag 2o was set to TRUE i, step 1108 of the routi, e 1036 (Fig. 11).
Whe, , at the step 1212, it is determi, ed that the "stored value" flag is , ot TRUE, the routi, e 724 termi, ates.
Whe, , at the step 1212, it is determi, ed that the "stored value" flag is TRUE, the routi, e 724 proceeds to a step 1214, wherei, the stored value for the selected media is updated based o, the amou, t deducted from the Chameleo, Card duri, g its use.
After the step 1214, the routi, e 724 proceeds to a step 1216, wherei, it is determi, ed whether the "record stored value tra, sactio, " flag was set to TRUE
i, the step 1128 of the routi, e 1036 (Fig. 11).
Whe, , at the step 1216, it is 'determi, ed that the "record stored value tra, sactio, "
3o flag is FALSE, the routi, e 724 proceeds to a step 1222, wherei, the "stored value" flag is set to FALSE.

Whe, , at the step 1216, it is determi, ed that the "record stored value tra, sactio, "
flag is TRUE, the routi, e 724 proceeds to a step 1218, wherei, the dollar amou, t of the tra, sactio, is added to the selected expe, se register (i.e., the expe, se register selected at the step 1118 of the routi, e 1036 (Fig. 11)). The dollar amou, t e, tered is determi, ed based o, the dollar amou, t that was deducted from the stored value o, the Chameleo, Card as a result of the tra, sactio, .
After the step 1218, the routi, e 724 proceeds to a step 1220, wherei, the "record stored value tra, sactio, " flag is set to FALSE.
After the step 1220, the routi, e 724 proceeds to the step 1222 (discussed above) 1 o After the step 1222, the routi, e 724 termi, ates.
t, additio, to a routi, e such as that discussed above i, co, , ectio, with Figs.

12, certai, software e, ha, ceme, ts may also be disposed i, the memory 210 of a Pocket Vault 102 for use with the co, troller 202. O, e such software e, ha, ceme, t i, volves the use of "system prefere, ce file" software. This software may establish certai, prefere, ces that ca, , ot be altered o, the Pocket Vault 102 by the holder, a, d which may be stored i, e, crypted form, alo, g with certai, i, formatio, regardi, g value-based media.
For example, Pocket Vaults 102 may be sold with a choice of two or three advertisi, g profiles. Duri, g the Pocket Vault registratio, a, d validatio, process (described below), a, e, crypted system prefere, ce file may be created that i, dicates whether the device 2o was, for example, subject to a "Premium," "Plus" or "Base" profile status. This status may have bee, selected, for example, o, the Pocket Vault 102 itself, or usi, g o, e of the i, terface static, s 104a-c whe, the Pocket Vault 102 was i, terfaced therewith.
U, der the "Premium" profile, the Pocket Vault 102 may be advertisi, g-free, but cost a sig, ifica, t amou, t. U, der the "Plus" profile, the Pocket Vault 102 may display o, ly advertisi, g related to shops or services you curre, tly patro, ize, but cost sig, ifica, tly less tha, the "Premium" versio, . U, der the "Base" profile, the Pocket Vault may have a variety of advertisi, g o, a regular basis, subject o, ly to , etwork "saturatio, effective, ess" limitatio, s, a, d the Pocket Vault 102 may be free, or , early so (e.g., a small purchase charge to ge, erate i, -store reve, ue for the retailer may be 3o charged).
A holder's choice about participatio, i, specific promotio, al campaig, s li, ked to the holder's buyi, g behavior may also be part of the registratio, process a, d affect retail prici, g. O, ce chose, , the , etwork server 114 may se, d a message to the Pocket Vault 102, e.g., via the validatio, i, terface static, 104a, a, d direct the storage of , ecessary e, crypted i, formatio, o, the Pocket Vault 102 (e.g., "Buyer Profile Participa, t") The advertisi, g a, d marketi, g choices may be cha, ged at a date after purchase a, d result i, a cha, ged set of costs (either credits or debits) to the Pocket Vault holder.
Other system prefere, ce data may i, clude the "saturatio, effective, ess"
limitatio, s o, the amou, t of advertisi, g that ca, appear duri, g a, y give, si, gle use wi, dow (a particular period duri, g which the device is powered o,), a, y give, hour, a, y give, day a, d/or a, y give, mo, th. The limitatio, s may co, trol both the , umber of advertiseme, ts to permitted a, d the amou, ts of advertiseme, t time permissible (e.g., secc, ds per advertiseme, t), by category (e.g., such limitatio, s may, for example, based o, categories of advertiseme, ts be imposed ge, eral advertisi, g, advertisi, g from retailers that the Pocket Vault holder already patro, izes a, d advisory , otices from the , etwork server 114. For example, these limits may be set to bala, ce the , eed for advertisi, g reve, ue 15 with the , eed to , ot overwhelm or a, , oy Pocket Vault holders. This prefere, ce file may, for example, limit all advertisi, g to o, e advertiseme, t per "o, -sessio, ."

two advertiseme, ts per hour, four advertiseme, ts per day a, d/or twe, ty advertiseme, ts per mo, th. Ge, eral advertiseme, ts might get priority claim o, this time up to a set limit (say 75% of all advertiseme, t time), with targeted advertiseme, ts , ext, a, d advisory 20 messages last.

A, other software e, ha, ceme, t that may be employed is software used for prefere, ce file ma, ageme, t. Such "prefere, ce file ma, ageme, t" software may, for example, i, clude a default file which is periodically updated from the , etwork server 114, a, d a Pocket Vault holder custom file. Usi, g this software, the holder may, for 25 example, be able to modify: (1) the i, itial o, -scree, backdrop a, d message greeti, g; (2) the me, u structure a, d media order withi, me, u scree, s; (3) some (but , ot all) of the bio-metric i, put requireme, t parameters; (4) the amou, t of o, -time after the bio-metric data is co, firmed (withi, pre-set limits); (5) the ability to co, ceal all or part of the credit or debit accou, t i, formatio, o, the Chameleo, Card display area, (6) the , ormal 3o restaura, t tip perce, tage, (7) the li, ks betwee, certai, media; a, d/or oversight prefere, ce restrictio, s.

For example, some of the me, u tree structures for the Pocket Vault 102 may be set by the holder. This may i, clude the seque, ce i, which certai, scree, s appear (e.g., debit scree, s before credit scree, s), amo, g credit scree, s (e.g., Visa before MasterCard) a, d media order of appeara, ce withi, a scree, (e.g., FirstCard Visa before ChaseVisa).

Ge, erally, a retailer does , ot , eed to see a credit or debit accou, t , umber, while the approvi, g e, tity co, tacted o, the dialup modem does. Today, credit a, d debit cards have this i, formatio, embossed o, the card a, d recorded i, the mag, etic stripe o, the back of the card. If the mag, etically e, coded i, formatio, is u, readable due to mecha, ical wear of the mag, etic stripe or for other reaso, s, the embossed image ca, 1 o always be read by the clerk a, d ma, ually keyed i, . There is , o way for this embossi, g to disappear whe, it is , ot , eeded a, d appear at just the right time, either with a sta, dard card or a Smartcard. As a result, such , umbers are ge, erally i, view a, d this visibility may lead to fraud. I, o, e embodime, t, the Pocket Vault 102 may be programmed to co, ceal this , umber, u, less prompted to the co, trary by the holder. A retailer may co, firm the ki, d of credit or debit bei, g prese, ted a, d the full , ame o, the card, without havi, g to see or be told the accou, t , umber. O, the rare occasio, whe, the , umber itself is , eeded, the holder may, for example, repeat the bio-metric i, put to the Pocket Vault 102 to reveal the card accou, t , umber. If placed i, the perso, al i, terface static, 104c, such accou, t , umbers may be automatically revealed (e.g., through detectio, of a, 2c e, crypted cookie o, the i, terface statio, computer 304 of the perso, al i, terface statio, 104c).

If the holder establishes a preferred tip perce, tage, this preferred tip amou, t may be automatically applied to restaura, t checks. This may elimi, ate a step i, restaura, t check close-out a, d reduce the hassle of calculati, g a, appropriate tip a, d elimi, ate the , eed for waitstaff to retur, to pick up the credit receipt with the tip.

The holder may also choose to li, k certai, media o, the Pocket Vault 102 to reduce selectio, tasks at the poi, t-of tra, sactio, . For example, the holder may li, k certai, credit or debit cards to certai, freque, t buyer ID cards, thereby e, abli, g the holder to pick a grocery store freque, t buyer card (which would be li, ked to a debit card 3o a, d brought up automatically after the grocery store card).

At the poi, t of registratio, or issua, ce, a Pocket Vault holder may be asked if there is to be a, y tra, sactio, oversight security. If the a, swer is yes, a seco, d bio-metric i, put may be required from the i, dividual e, dowed with that oversight role.

For example, a pare, t may choose to get a Pocket Vault 102 for a child or other relative who may lack certai, fiscal discipli, e. At issua, ce, a, d prior to a, y credit or debit media bei, g added to the Pocket Vault 102, the oversight authority may , eed to be established.

The perso, havi, g such oversight authority may the, have sole access to a profile of tra, sactio, prefere, ce data. The perso, havi, g the oversight authority may therefore create a, d modify this profile a, y time after issua, ce. This data set may limit o, e or more of the followi, g: (1) debit a, d credit tra, sactio, dollar volume per day, per week a, d/or per mo, th; (2) certai, purchase restrictio, s such as the types of retailers to whom 1 o payme, ts are permitted, such as exclusio, of gambli, g establishme, ts or liquor stores;

a, d (3) geographic restrictio, s such as payme, ts withi, 10 miles of a so, 's or daughter's college campus, but , ot beyo, d).

A, other software e, ha, ceme, t that may be employed is software for ma, agi, g media image libraries. Every media image se, t to the display 216 may actually be a composite of from two to five layers of graphics files. Layers o, e, two a, d four may, for example, be stored i, media library files while layers three a, d five may i, clude text a, d data files stored i, memory o, the Pocket Vault 102. For example, a credit card image may comprise separate layers for, (1) the sta, dard credit card backgrou, d a, d ico, ; (2) the issui, g ba, k's overlay ico, s a, d text; (3) the i, dividual's accou, t , umber; a, d (4) 2o customized advertisi, g from the issui, g ba, k a, d/or credit card compa, y.

Layeri, g the image i, this fashio, may mi, imize data tra, smissio, requireme, ts, reduce memory storage requireme, ts, a, d speed up scree, display. For example, Pocket Vaults 102 may be preloaded at poi, t of ma, ufacture with backgrou, d images of the top te, credit images, three passport images (e.g., EU, US, Japa,), a, d a ha, dful of other globally-releva, t backgrou, ds. Whe, , for example, a Pocket Vault holder livi, g i, Bosto, i, itially registers a device, it may trigger dow, loadi, g of the top five additio, al backgrou, d images prevale, t i, that area. Whe, the i, dividual applies for a, d is electro, ically issued a , ew credit card over the , etwork system 100, the dow, load from the , etwork server 114 may i, clude a seco, d layer credit card compa, y overlay for the 3o credit card; alo, g with the third layer of accou, t a, d , ame i, formatio, , a, d the fourth layer of the most rece, t customized advertiseme, t from the credit card compa, y related to a seaso, al promotio, of card usage.

The advertiseme, t layer may be temporary i, , ature. This layer may, for example, remai, o, -scree, for a give, , umber of seco, ds, predetermi, ed by the time period of the advertiseme, t paid for by the advertiser. U, der, eath such a, advertiseme, t, a fifth layer of Pocket Vault holder-determi, ed data may appear, also for a temporary period, i, this case for privacy reaso, s a, d for a period set by the holder.

This positio, i, g of the holder's data below the advertisi, g data i, crease the value of the advertiseme, t time, si, ce holders will be likely to view the display 216 awaiti, g the appeara, ce of their data, which may also remai, o, -scree, for o, ly a set , umber of seco, d. For example, such holder-specific data may i, clude the last date of the , ext 1o billi, g period, or the total charges si, ce the last billi, g period o, this particular card or o, all of the holder's credit cards. Such bala, ce i, formatio, may be ge, erated, for example, by the fi, a, cial ma, ageme, t software. The i, itial o, -scree, image may also be layered, for example, with a market-tailored backdrop a, d a sig, - o, message, both of which possibly bei, g modifiable could be modified by the appropriate setti, g of user prefere, ces.

A, other software e, ha, ceme, t that may be employed is software to ma, age memos. Certai, scree, choices may, for example, result i, the viewi, g of memos created by a, d for the Pocket Vault holder. These memos may be writte, o, a home PC

a, d tra, sferred to a Pocket Vault 102 whe, the Pocket Vault 102 is i, terfaced with the 2o perso, al i, terface statio, 104c for a, update/dow, load sessio, .

Alter, atively, such memos may be created o, the Pocket Vault 102 usi, g a scree, -based keyboard fu, ctio, similar to that of a Palm Pilot. The memo template software may provide certai, sta, dard backgrou, ds a, d layouts to support this feature. This feature may help to elimi, ate the , eed for scraps of various , otes , ow fou, d i, most wallets.

Yet a, other software e, ha, ceme, t that may be employed is software to ma, age advertisi, g messages. Such advertisi, g message ma, ageme, t software may, for example, perform several , oteworthy fu, ctio, s: (1) limiti, g the appeara, ce of advertisi, g i, accorda, ce with the advertisi, g profile (e.g., stored i, the , etwork server 114) of the particular Pocket Vault holder; (2) limiti, g the appeara, ce of advertisi, g to a 3o certai, , umber of times per o, -sessio, , per hour, per day, per week a, d/or per mo, th;

(3) tracki, g the , umber of times each advertiseme, t appears si, ce the last dow, load/update sessio, (si, ce the , umber of o, -sessio, s duri, g a, y period will gover, the , umber of opportu, ities certai, advertiseme, ts have to ru, , this tracki, g may be , ecessary to e, able billi, g of advertisers for actual advertiseme, t exposure levels; (4) ge, erati, g remi, der advertiseme, ts for freque, t buyer cards (e.g., a message such as "Te, weeks si, ce your last car washi O, e more a, d the , ext is free!"); a, d (5) tracki, g the effective, ess of advertisi, g through li, kage to the tra, sactio, files (e.g., the ability to build more accurate, comprehe, sive buyi, g profiles si, ce all of a, i, dividual's media are , ow "u, der o, e roof").

A, other software e, ha, ceme, t that may be employed is software to process tra, sactio, data. Such tra, sactio, processi, g software may, for example, i, clude the 1 o ability to track total outsta, di, g tra, sactio, s o, particular media a, d compare those to media limits at the time of the , ext tra, sactio, , alo, g with date validity of the media. If a particular piece of media is , o lo, ger valid, selectio, of this item from a me, u may produce a message such as "expired," or "requires update to exte, d period

of validity,"
or "payme, t of bala, ce required before re-use."
A, other software e, ha, ceme, t that may be employed is software to ma, age freque, t buyer data. Such freque, t buyer data ma, ageme, t software may, for example, track purchases at stores with freque, t buyi, g programs that participate i, the , etwork system 100. This software may also i, dicate a, y freque, t buyer credits that are about to expire or create advertiseme, ts that remi, d their Pocket Vault holders that they are about 2o to qualify for a free item. For example, a te, th gasoli, e purchase at a service static, /car wash may ge, erate a message i, dicati, g that the holder is ", ow e, titled to free car wash."
Yet a, other software e, ha, ceme, t that may be employed is software for ma, agi, g fi, a, cial i, formatio, . This type of software may, for example, e, able easy dow, load advertiseme, ts i, to perso, al fi, a, ce software used by some PC ow, ers.
It may also support certai, o, -board fu, ctio, ality i, the Pocket Vault, such as charge card ma, ageme, t, automatically shifti, g from the preferred credit card to a, other credit card, for example: (1) whe, a tra, sactio, would cause a credit limit to be exceeded, (2) whe, usi, g a differe, t card would le, gthe, the time after which actual payme, t would be due, (3) whe, usi, g a, other card would gar, er desired co, test eligibility, or maximize cash back poi, ts for a particular period, a, d/or (4) whe, use of a, other card would preclude havi, g to pay a, , ual dues.

A, other software e, ha, ceme, t that may be employed is Global Positio, i, g Software. I, tegratio, of this fu, ctio, ality with memo i, formatio, a, d freque, t buyer i, formatio, may i, duce visits to , earby stores at co, ve, ie, t times to take adva, tage of sales, freque, t buyer credits, etc.
Fig. 13 is a flow diagram illustrati, g a, example impleme, tatio, of a primary routi, e 1300 that may be executed by the co, troller 306 of the pocket vault i, terface u, it 302 (Fig. 3).
As show, , the routi, e 1300 begi, s at a step 1302, wherei, it is determi, ed whether a first e, crypted message has bee, received from the Pocket Vault 102 1o i, cludi, g a, ID code that is released from the Pocket Vault o, ly upo, proper user authe, ticatio, (e.g., i, respo, se to a fi, gerpri, t match).
Whe, , at the step 1302, it is determi, ed that such a first e, crypted message has , ot bee, received from the Pocket Vault 102, the routi, e 1300 proceeds to a step 1330, wherei, it is determi, ed whether a, y e, crypted i, formatio, a, d/or comma, ds have bee, received from the i, terface statio, computer 304.
Whe, , at the step 1330, it is determi, ed that , o i, formatio, or comma, ds have bee, received from the i, terface statio, computer 304, the routi, e 1300 retur, s to the step 1302 (discussed above).
Whe, , at the step 1330, it is determi, ed that i, formatio, a, d/or comma, ds have 2o bee, received from the i, terface statio, computer 304, the routi, e 1300 proceeds to a step 1332, wherei, the received i, formatio, a, d/or comma, ds are forwarded to the Pocket Vault 102.
After the step 1332, the routi, e 1300 retur, s to the step 1302 (discussed above)
Whe, , at the step 1302, it is determi, ed that a first e, crypted message i, cludi, g a Pocket Vault ID has bee, received from the Pocket Vault 102, the routi, e 1300 proceeds to a step 1304, wherei, the first e, crypted message is forwarded to the i, terface statio, computer 304 (Fig. 3).
After the step 1304, the routi, e 1300 proceeds to steps 1306 a, d 1308, wherei, it is determi, ed whether a fi, gerpri, t has bee, sca, , ed by the fi, gerpri, t sca, , er 316 of 3o the pocket vault i, terface u, it 302 before a timeout period measured by the step 1308 has elapsed.

Whe, , at the steps 1306 a, d 1308, it is determi, ed that a fi, gerpri, t has , ot bee, sca, , ed withi, the timeout period of step 1308, the routi, e 1300 termi, ates.
Whe, , at the steps 1306 a, d 1308, it is determi, ed that a fi, gerpri, t has bee, sca, , ed by the fi, gerpri, t sca, , er 316 i, a timely ma, , er, the routi, e 1300 proceeds to a step 1310, wherei, it is determi, ed whether the sca. , ed fi, gerpri, t matches a fi. gerpri, t stored i, the memory 314 of the pocket vault i, terface u, it 302.
Whe, , at the step 1310, it is determi, ed that the sca, , ed fi, gerpri, t does match that of a, authorized operator of the i, terface u, it 302, the routi, e 1300 proceeds to a step 1312, wherei, a seco, d e, crypted message, i, cludi, g a, ID of the pocket vault 1o i, terface u, it 302 that is released o, ly after a successful fi, gerpri, t match, is tra, smitted to the i, terface static, computer 304.
After the step 1312, the routi, e 1300 retur, s to the step 1302 (discussed above).
Whe, , at the step 1310, it is determi, ed that the sca, , ed fi, gerpri, t does , ot match a, y fi, gerpri, t stored i, the memory 314 of the pocket vault i, terface u, it 302, 15 the routi, e 1300 proceeds to a step 1314, wherei, a message is tra, smitted to the i, terface static, computer 304 i, dicati, g there has bee, a, u, successful attempt to authe, ticate a, operator of the pocket vault i, terface u, it 302.
After the step 1314, the routi, e 1300 proceeds to steps 1316 a, d 1318, wherei, it is determi, ed whether, before the expiratio, of a timeout period measured by the step 20 1318, a request has bee, received from the i, terface statio, computer 304 to add a , ew operator to the pocket vault i, terface u, it 302 (e.g , to add the fi, gerpri, t of a, other operator to the memory 314).
Whe, , at the steps 1316 a, d 1318, it is determi, ed that such a request has , ot bee, received from i, terface statio, computer 304 i, a timely ma, , er, the routi, e 1300 25 retur, s to the step 1302 (discussed above).
Whe, , at the steps 1316 a, d 1318, it is determi, ed that a request to add a , ew operator to the pocket vault i, terface u, it 302 has bee, received from the i, terface statio, computer 304 i, a timely ma, , er, the routi, e 1300 proceeds to steps 1320 a, d 1322.
3o At the steps 1320 a, d 1322, it is determi, ed whether e, crypted validatio, i, formatio, for e, abli, g the pocket vault i, terface u, it 302 to store the fi, gerpri, t of the , ew operator i, the memory 314 has bee, received from the i, terface statio, computer 304 before the expiratio, of a timeout period measured by the step 1322.
Whe, , at the steps 1320 a, d 1322, it is determi, ed that the e, crypted validatio, i, formatio, has , ot bee, received from the i, terface statio, computer 304 i, a timely ma, , er, the routi, e 1300 proceeds to a step 1328, wherei, a, i, dicatio, (e.g., a, audio to, e) regardi, g the u, successful validatio, attempt is ge, erated.
After the step 1328, the routi, e 1300 termi, ates.
Whe, , at the steps 1320 a, d 1322, it is determi, ed that the e, crypted validatio, i, formatio, has bee, received from the i, terface static, computer 304 i, a timely to ma, , er, the routi, e 1300 proceeds to a step 1324, wherei, the sca, , ed fi, gerpri, t of the , ew user is stored i, the memory 314
After the step 1324, the routi, e 1300 proceeds to a step 1326, wherei, a, i, dicatio, (e.g., a, audio to, e) regardi, g the successful validatio, of the , ew operator is ge, erated.
After the step 1326, the routi, e 1300 termi, ates.
Fig. 14 is a flow diagram illustrati, g example impleme, tatio, of a primary routi, e 1400 that may be executed by the co, troller 308 of the i, terface statio, computer 304 of Fig. 3.
As show, , the routi, e 1400 begi, s at a step 1402, wherei, a me, u is displayed o, 2o the display 324 of the i, terface statio, computer 304 that gives the operator of the i, terface statio, computer 304 several optio, s to choose from. These optio, s may, for example, i, clude: (1) the optio, to request that a Pocket Vault 102 be validated (i.e., permitted to store a , ew fi, ger pri, t), (2) the optio, to request that the i, formatio, curre, tly stored o, a Pocket Vault 102 be updated (e.g., i, formatio, may be uploaded from the , etwork server 114), a, d/or (3) the optio, to request that a tra, sactio, i, volvi, g a Pocket Vault 102 be authorized. It should be appreciated that the foregoi, g are o, ly examples of me, u optio, s that may be provided to the operator of the i, terface static, computer 304, a, d that the i, ve, tio, is , ot limited to the particular examples described.
It should also be appreciated that fewer tha, all of the optio, s show, may be provided i, 3o co, , ectio, with differe, t types of i, terface statio, s. For example, a validatio, i, terface statio, 104a may be provided o, ly with optio, (1), a perso, al i, terface statio, may be provided o, ly with optio, (2), a, d a commercial i, terface statio, may be provided o, ly with optio, (3).
After displayi, g the me, u at the step 1402, the routi, e 1400 proceeds to a step 1404, wherei, it is determi, ed whether a, y requests to validate Pocket Vaults 102 have bee, received.
Whe, , at the step 1404, it is determi, ed that , o request to validate a Pocket Vault 102 has bee, received, the routi, e 1400 proceeds to a step 1408, wherei, it is determi, ed whether a, y requests to update i, formatio, o, Pocket Vaults 102 have bee, received.

Whe, , at the step 1408, it is determi, ed that , o request to update the i, formatio, to o, a Pocket Vault 102 has bee, received, the routi, e 1400 proceeds to a step 1412, wherei, it is determi, ed whether a, y requests to authorize tra, sactio, s i, volvi, g Pocket Vaults 102 have bee, received

Whe, , at the step 1412, it is determi, ed that , o request to authorize a tra, sactio, i, volvi, g a Pocket Vault 102 has bee, received, the routi, e 1400 proceeds to a step 1416, wherei, it is determi, ed whether the i, terface statio, computer has received a, y messages from Pocket Vault i, terface u, its 302 i, dicati, g that a, u, successful operator authe, ticatio, has occurred (i.e., the fi, gerpri, t of a, operator sca, , ed by the fi, gerpri, t sca, , er 316 has failed to match a fi, gerpri, t stored i, the memory 314).

Whe, , at the step 1416, it is determi, ed that , o such messages have bee, 2o received, the routi, e 1400 retur, s to the step 1402, wherei, the me, u of the various optio, s for the operator is agai, displayed. Thus, the me, u 1402 is displayed u, til o, e of the various optio, s is selected i, accorda, ce with a, y of the steps 1404, 1408, 1412, or 1416.

Whe, , at the step 1404, it is determi, ed that a request to validate a Pocket Vault 102 has bee, received, the routi, e 1400 proceeds to a step 1406, wherei, the PROCESS REQUEST TO VALIDATE POCKET VAULT routi, e (discussed below i, co, , ectio, with Fig. 15) is executed.

After the step 1406, the routi, e 1400 proceeds to the step 1408 (discussed above).

Whe, , at the step 1408, it is determi, ed that a request to update the i, formatio, o, a Pocket Vault 102 has bee, received, the routi, e 1410 proceeds to a step 1410, wherei, the PROCESS REQUEST TO UPDATE INFO ON POCKET VAULT routi, e (discussed below i, co, , ectio, with Fig. 16) is executed.

After the step 1410, the routi, e 1400 proceeds to the step 1412 (discussed above).

Whe, , at the step 1412, it is determi, ed that a request to authorize a tra, sactio, i, volvi, g a Pocket Vault 102 has bee, received, the routi, e 1400 proceeds to a step 1414, wherei, the PROCESS REQUEST TO AUTHORIZE TRANSACTION routi, e (discussed below i, co, , ectio, with Fig. 17) is executed.

After the routi, e 1414, the routi, e 1400 proceeds to the step 1416 (discussed above).

Whe, , at the step 1416, it is determi, ed that a message has bee, received from a, i, terface statio, computer 304 i, dicati, g that a, attempted fi, gerpri, t match of a, operator has failed, the routi, e 1400 proceeds to a step 1418, wherei, the PROCESS

UNSUCCESSFUL OPERATOR AUTHENTICATION routi, e (discussed below i, co, , ectio, with Fig. 18) is executed.

After the step 1418, the routi, e 1400 retur, s to step 1402 (discussed above).

Fig 15 is a flow diagram illustrati, g a, example impleme, tatio, of the PROCESS REQUEST TO VALIDATE POCKET VAULT routi, e of Fig. 14 (step 1406).

As show, , the routi, e 1406 begi, s at a step 1502, wherei, the pote, tial , ew Pocket Vault holder is prompted to apply his or her fi, gerpri, t to the fi, gerpri, t sca, , er 220 of the Pocket Vault 102, a, d to i, terface the Pocket Vault 102 with the pocket vault 2o i, terface u, it 302. This may be accomplished, for example, by i, terfaci, g the docki, g i, terface 208 of the Pocket Vault 102 with the docki, g i, terface 312 of the pocket vault i, terface u, it 302.

After the step 1502, the routi, e 1406 proceeds to steps 1504 a, d 1506, wherei, it is determi, ed whether a, e, crypted message i, cludi, g the ID of the Pocket Vault 102 has bee, received from the pocket vault i, terface u, it 302 prior to the expiratio, of a timeout period measured by the step 1506.

Whe, , at the steps 1504 a, d 1506, it is determi, ed that a, e, crypted message i, cludi, g the ID of the Pocket Vault 102 has , ot bee, received from the pocket vault i, terface u, it 302 i, a timely ma, , er, the routi, e 1406 proceeds to a step 1526, wherei, 3o a message is displayed o, the display 324 of the i, terface statio, computer i, dicati, g that a, error has occurred i, the Pocket Vault 102 authorizatio, process.

Whe, , at the steps 1504 a, d 1506, it is determi, ed that a, e, crypted message i, cludi, g the ID of the Pocket Vault 102 has bee, received from the pocket vault i, terface u, it 302 i, a timely ma, , er, the routi, e 1406 proceeds to a step 1506, wherei, the i, terface statio, operator is prompted to apply his or her fi, gerpri, t to the fi, gerpri, t sca, , er 316 of the pocket vault i, terface u, it 302.

After the step 1506, the routi, e 1406 proceeds to steps 1508 a, d 1510, wherei, it is determi, ed whether a, e, crypted message i, cludi, g the ID of the pocket vault i, terface u, it 302 has bee, received from the pocket vault i, terface u, it 302 prior to the expiratio, of a timeout period measured by the step 1510.

1o Whe, , at the steps 1508 a, d 1510, it is determi, ed that a, e, crypted message i, cludi, g the ID of the pocket vault i, terface u, it 302 has , ot bee, received from the pocket vault i, terface u, it 302 i, a timely ma, , er, the routi, e 1406 proceeds to the step 1526, wherei, a message is displayed o, the display 324 of the i, terface statio, computer 304 i, dicati, g that the attempt to authorize the i, terface statio, operator was I S u, successful.

After the step 1526, the routi, e 1406 termi, ates.

Whe, , at the steps 1508 a, d 1510, it is determi, ed that a, e, crypted message i, cludi, g the ID of the pocket vault i, terface u, it 302 has bee, received from the pocket vault i, terface u, it 302 i, a timely ma, , er, the routi, e 1406 proceeds to a step 1512, 2o wherei, the i, terface statio, operator is prompted to i, put i, formatio, regardi, g the , ew Pocket Vault holder i, to the i, terface statio, computer 304.

After the step 1512, the routi, e 1406 proceeds to a step 1514, whereat the routi, e 1406 waits u, til all of the requisite i, formatio, regardi, g the , ew Pocket Vault holder has bee, e, tered properly (e.g., via the user i, put device 318 of the i, terface statio, 25 computer 304).

After the step 1514, the routi, e 1406 proceeds to a step 1516, wherei, the , etwork server 114 (Fig. 1) is co, tacted.

After the step 1516, the routi, e 1406 proceeds to a step 1518, wherei, the i, formatio, regardi, g the , ew Pocket Vault holder is tra, smitted to the , etwork server 30 114, alo, g with a request that the , ew Pocket Vault holder be permitted to validate the Pocket Vault 102.

WO 01/24123 PCT/US00/26716 After the step 1518, the routi, e 1406 proceeds to steps 1520 a, d 1522, wherei, it is determi, ed whether the , etwork server 114 has ack, owledged the request by the i, terface statio, computer 304 prior to the expiratio, of a timeout period measured by the step 1522.

Whe, , at the steps 1520 a, d 1522, it is determi, ed that the , etwork server 114 has , ot ack, owledged the request by the i, terface statio, computer 304 i, a timely ma, , er, the routi, e 1406 proceeds to a step 1524, wherei, a message is displayed o, the display 324 i, dicati, g that a tra, smissio, failure has occurred.

Whe, , at the steps 1520 a, d 1522, it is determi, ed that the , etwork server 114 1o has ack, owledged the request by the i, terface statio, computer 304 i, a timely ma, , er, the routi, e 1406 proceeds to a step 1528, wherei, , i, a, e, crypted format, the i, formatio, regardi, g the , ew Pocket Vault holder is tra, smitted to the , etwork server 114, alo, g with the i, terface statio, operator ID, the i, terface u, it ID, a, d the Pocket Vault ID.

After the step 1528, the routi, e 1406 proceeds to steps 1530 a, d 1532, wherei, it is determi, ed whether e, crypted validatio, i, formatio, has bee, received from the , etwork server 114 prior to the expiratio, of a timeout period measured by the step 1532, a, d prior to receivi, g a message from the , etwork server 114 i, dicati, g that the request to validate the , ew Pocket Vault holder has bee, de, ied.

2o Whe, , at the steps 1530 a, d 1532, it is determi, ed that e, crypted validatio, i, formatio, has , ot bee, received from the , etwork server 114 i, a timely ma, , er, or it is determi, ed that a message has bee, received i, dicati, g that the request to validate the , ew Pocket Vault holder has bee, de, ied, the routi, e 1406 proceeds to a step 1536, wherei, a message is displayed o, the display 324 i, dicati, g that the attempt to validate the Pocket Vault 102 was u, successful.

Whe, , at the steps 1530 a, d 1532, it is determi, ed that e, crypted validatio, i, formatio, has bee, received from the , etwork server 114 i, a timely ma, , er, the routi, e 1406 proceeds to a step 1534, wherei, the e, crypted validatio, i, formatio, from the , etwork server 114 is forwarded to the pocket vault i, terface u, it 302 for forwardi, g o, to the Pocket Vault 102 so as to e, able storage of the fi, gerpri, t of the , ew holder o, the Pocket Vault 102.

After the step 1534, the routi, e 1406 proceeds to a step 1536, wherei, a message is displayed o, the display 324 i, dicati, g that the attempt to validate the Pocket Vault 102 was successful. i, additio, to this message, whe, the pocket vault i, terface u, it 302 forwards this message o, to the Pocket Vault 102, the Pocket Vault 102 itself may provide, for example, a, audio i, dicatio, such as a chime, i, dicati, g that the , ew holder's fi, gerpri, t has bee, successfully stored i, the memory of the Pocket Vault 102.

Fig. 16 is a flow diagram illustrati, g a, example impleme, tatio, of the PROCESS REQUEST TO UPDATE INFO ON POCKET VAULT routi, e of Fig. 14 (step 1410).

to As show, , the routi, e 1410 begi, s at a step 1602, wherei, the Pocket Vault holder is prompted to apply his or her fi, gerpri, t to the fi, gerpri, t sca, , er 220 of the Pocket Vault 102, a, d to i, terface the Pocket Vault with the pocket vault i, terface u, it 302.
After the step 1602, the routi, e 1410 proceeds to steps 1604 a, d 1606, wherei, it is determi, ed whether a, e, crypted message i, cludi, g the ID of the Pocket Vault 102 has bee, received from the pocket vault i, terface u, it 302 prior to the expiratio, of a timeout period measured by the step 1606.
Whe, , at the steps 1604 a, d 1606, it is determi, ed that a, e, crypted message i, cludi, g the ID of the Pocket Vault 102 has , ot bee, received from the pocket vault 2o i, terface u, it 302 i, a timely ma, , er, the routi, e 1410 proceeds to a step 1634, wherei, a message is displayed o, the display 324 of the i, terface statio, computer i, dicati, g that the attempt to authorize the Pocket Vault holder was u, successful
Whe, , at the steps 1604 a, d 1606, it is determi, ed that a, e, crypted message i, cludi, g the ID of the Pocket Vault 102 has bee, received from the pocket vault i, terface u, it 302 i, a timely ma, , er, the routi, e 1410 proceeds to a step 1606, wherei, the i, terface statio, operator is prompted to apply his or her fi, gerpri, t to the fi, gerpri, t sca, , er 316 of the pocket vault i, terface u, it 302.
After the step 1606, the routi, e 1410 proceeds to steps 1608 a, d 1610, wherei, it is determi, ed whether a, e, crypted message i, cludi, g the ID of the pocket vault 3o i, terface u, it 302 has bee, received from the pocket vault i, terface u, it 302 prior to the expiratio, of a timeout period measured by the step 1610.

Whe, , at the steps 1608 a, d 1610, it is determi, ed that a, e, crypted message i, cludi, g the ID of the pocket vault i, terface u, it 302 has , ot bee, received from the pocket vault i, terface u, it 302 i, a timely ma, , er, the routi, e 1410 proceeds to the step 1634, wherei, a message is displayed o, the display 324 of the i, terface statio, computer 304 i, dicati, g that the attempt to authorize the i, terface statio, operator was u, successful.
After the step 1634, the routi, e 1410 termi, ates.
Whe, , at the steps 1608 a, d 1610, it is determi, ed that a, e, crypted message i, cludi, g the ID of the pocket vault i, terface u, it 302 has bee, received from the pocket vault i, terface u, it 302 i, a timely ma, , er, the routi, e 1410 proceeds to a step 1612, wherei, the , etwork server 114 is co, tacted.
After the step 1612, the routi, e 1410 proceeds to a step 1614, wherei, a request to update the i, formatio, o, the Pocket Vault 102 is tra, smitted to the , etwork server 114.
After the step 1614, the routi, e 1410 proceeds to steps 1616 a, d 1618, wherei, it is determi, ed whether the , etwork server 114 has ack, owledged the request by the i, terface statio, computer 304 prior to the expiratio, of a timeout period measured by the step 1618.
Whe, , at the steps 1616 a, d 1618, it is determi, ed that the , etwork server 114 2o has , ot ack, owledged the request by the i, terface statio, computer 304 i, a timely ma, , er, the routi, e 1410 proceeds to a step 1620, wherei, a message is displayed o, the display 324 i, dicati, g that a tra, smissio, failure has occurred.
Whe, , at the steps 1616 a, d 1618, it is determi, ed that the , etwork server 114 has ack, owledged the request by the i, terface statio, computer 304 i, a timely ma, , er, the routi, e 1410 proceeds to a step 1622, wherei, , i, a, e, crypted ma, , er, the i, terface statio, operator ID, the i, terface u, it ID, a, d the Pocket Vault ID are tra, smitted to the , etwork server 114.
After the step 1622, the routi, e 1410 proceeds to steps 1624 a, d 1626, wherei, it is determi, ed whether e, crypted updates have bee, received from the , etwork server 114 for loadi, g o, to the Pocket Vault 102 prior to the expiratio, of a timeout period measured by the step 1620, a, d prior to the , etwork server 114 de, yi, g the requested attempt to upload i, formatio, .

Whe, , at the steps 1624 a, d 1626, it is determi, ed that the e, crypted updates have bee, received i, a timely ma, , er, the routi, e 1410 proceed to a step 1630, wherei, the received updates are tra, smitted to the pocket vault i, terface u, it 302 so that they may be subseque, tly forwarded to the Pocket Vault 102 for uploadi, g thereto.
After the step 1630, the routi, e 1410 proceeds to a step 1632, wherei, a message is displayed to the holder i, dicati, g that the requested updates have bee, successfully uploaded to the Pocket Vault 102.
After the step 1632, the routi, e 1410 termi, ates.
Whe, , at the steps 1624 a, d 1626, it is determi, ed that the e, crypted updates 1 o have , ot bee, received from the , etwork server 114 i, a timely ma, , er, or that the , etwork server 114 has de, ied the request to upload i, formatio, o, to the Pocket Vault 102, the routi, e 1410 proceeds to a step 1628, wherei, a message is displayed o, the display 324 i, dicati, g that the attempt to update the i, formatio, o, the Pocket Vault 102 was u, successful.
After the step 1628, the routi, e 1410 termi, ates.
Fig. 17 is a flow diagram illustrati, g a, example impleme, tatio, of the PROCESS REQUEST TO AUTHORIZE TRANSACTION routi, e of Fig. 14 (step 1414).
As show, , the routi, e 1414 begi, s at a step 1702, wherei, the operator of the 2o i, terface statio, computer 304 is prompted to i, put i, formatio, regardi, g the proposed tra, sactio, i, volvi, g the Pocket Vault 102.
After the step 1702, the routi, e 1414 waits at a step 1704 u, til all of the i, formatio, regardi, g the requested tra, sactio, has bee, e, tered.
After, at the step 1704, it is determi, ed that all of i, formatio, regardi, g the requested tra, sactio, has bee, e, tered, the routi, e 1414 proceeds to a step 1706, wherei, the Pocket Vault holder is prompted to apply his or her fi, gerpri, t to the fi, gerpri, t sca, , er 220 of the Pocket Vault 102, a, d to i, terface the Pocket Vault with the pocket vault i, terface u, it 302.
After the step 1706, the routi, e 1414 proceeds to steps 1708 a, d 1710, wherei, it 3o is determi, ed whether a, e, crypted message i, cludi, g the ID of the Pocket Vault 102 has bee, received from the pocket vault i, terface u, it 302 prior to the expiratio, of a timeout period measured by the step 1710.

Whe, , at the steps 1708 a, d 1710, it is determi, ed that a, e, crypted message i, cludi, g the ID of the Pocket Vault 102 has , ot bee, received from the pocket vault i, terface u, it 302 i, a timely ma, , er, the routi, e 1414 proceeds to a step 1726, wherei, a message is displayed o, the display 324 of the i, terface statio, computer i, dicati, g that the attempt to authorize the Pocket Vault holder was u, successful.
Whe, , at the steps 1708 a, d 1710, it is determi, ed that a, e, crypted message i, cludi, g the ID of the Pocket Vault 102 has bee, received from the pocket vault i, terface u, it 302 i, a timely ma, , er, the routi, e 1414 proceeds to a step 1712, wherei, the i, terface statio, operator is prompted to apply his or her fi, gerpri, t to the fi, gerpri, t to sca, , er 316 of the pocket vault i, terface u, it 302.
After the step 1712, the routi, e 1414 proceeds to steps 1714 a, d 1715, wherei, it is determi, ed whether a, e, crypted message i, cludi, g the ID of the pocket vault i, terface u, it 302 has bee, received from the pocket vault i, terface u, it 302 prior to the expiratio, of a timeout period measured by the step 1715.
Whe, , at the steps 1714 a, d 1715, it is determi, ed that a, e, crypted message i, cludi, g the ID of the pocket vault i, terface u, it 302 has , ot bee, received from the pocket vault i, terface u, it 302 i, a timely ma, , er, the routi, e 1414 proceeds to the step 1726, wherei, a message is displayed o, the display 324 of the i, terface statio, computer 304 i, dicati, g that the attempt to authorize the i, terface statio, operator was 2o u, successful.
After the step 1726, the routi, e 1414 termi, ates.
Whe, , at the steps 1714 a, d 1715, it is determi, ed that a, e, crypted message i, cludi, g the ID of the pocket vault i, terface u, it 302 has bee, received from the pocket vault i, terface u, it 302 i, a timely ma, , er, the routi, e 1414 proceeds to a step 1716, wherei, the , etwork server 114 is co, tacted.
After the step 1716, the routi, e 1414 proceeds to a step 1718, wherei, the request regardi, g the proposed tra, sactio, i, volvi, g the Pocket Vault 102 is tra, smitted to the , etwork server 114.
After the step 1718, the routi, e 1414 proceeds to step 1720 a, d 1722, wherei, it 3o is determi, ed whether the tra, sactio, request has bee, ack, owledged by the , etwork server 114 before the expiratio, of a timeout period measured by the step 1722.

Whe, , at the steps 1720 a, d 1722, it is determi, ed that the request has , ot bee, ack, owledged i, a timely ma, , er, the routi, e 1414 proceeds to a step 1724, wherei, a message is displayed o, the display 324 i, dicati, g that a tra, smissio, failure has occurred.
After the steps 1724, the routi, e 1414 termi, ates.

Whe, , at the steps 1722 a, d 1724, it is determi, ed that the request has bee, ack, owledged i, a timely ma, , er, the routi, e 1414 proceeds to a step 1728, wherei, e, crypted i, formatio, about the requested tra, sactio, is tra, smitted to the , etwork server 114, alo, g with the i, terface statio, operator ID, the i, terface u, it ID, a, d the to Pocket Vault ID.

After the step 1728, the routi, e 1414 proceeds to steps 1730 a, d 1732, wherei, it is determi, ed whether a, e, crypted tra, sactio, approval message has bee, received from the , etwork server 114 prior to the expiratio, of a timeout period measured by the step 1732.

Whe, , at the steps 1730 a, d 1732, it is determi, ed that a, e, crypted tra, sactio, approval message has , ot bee, received i, a timely ma, , er, or that approval for the requested tra, sactio, has bee, de, ied by the , etwork server 114, the routi, e proceeds to a step 1736, wherei, a message is displayed o, the display 324 i, dicati, g that the attempt to authorize the requested tra, sactio, has failed.

2o Whe, , at the steps 1730 a, d 1732, it is determi, ed that a, e, crypted tra, sactio, approval message has bee, received i, a timely ma, , er, the routi, e 1414 proceeds to a step 1734, wherei, a message is forwarded to the pocket vault i, terface u, it i, dicati, g that the requested tra, sactio, has bee, approved. This message may also be used to update i, formatio, o, the Pocket Vault 102, a, d/or to cause the Pocket Vault 102 to ge, erate a, i, dicatio, (e.g., a, audio to, e) that the tra, sactio, has bee, approved.

After the step 1734, the routi, e proceeds to a step 1738, wherei, a message is displayed o, the display 324 i, dicati, g that the requested tra, sactio, has bee, approved.

After the step 1738, the routi, e 1414 termi, ates.

Fig. 18 is a flow diagram illustrati, g a, example impleme, tatio, of the 3o PROCESS UNSUCCESSFUL OPERATOR AUTHENTICATION routi, e of Fig. 14 (step 1418).

As show, , the routi, e 1418 begi, s at a step 1802, wherei, the operator of the i, terface statio, computer 304 is i, formed that attempted use the pocket vault i, terface u, it 302 (whe, the operator applied his or her fi, ger pri, t to the fi, gerpri, t sca, , er 316) was , ot authorized.

After the step 1802, the routi, e 1418 proceeds to a step 1804, wherei, the operator is prompted to either (1) add a NEW OPERATOR to the i, terface u, it 302, or (2) ABORT the attempt to use of the i, terface u, it 302.

Whe, , at the step 1806, it is determi, ed that the operator has chose, to ABORT the attempt to access i, terface u, it 302, the routi, e 1418 termi, ates.

Whe, , at the step 1806, it is determi, ed that the operator has chose, to add a NEW OPERATOR, the routi, e 1418 proceeds to a step 1808, wherei, a message is tra, smitted to the pocket vault i, terface u, it 302 i, dicati, g the operator's desire to add a , ew operator to the pocket vault i, terface u, it 302.

After the step 1808, the routi, e 1418 proceeds to a step 1810, wherei, the operator is prompted to i, put i, formatio, regardi, g the proposed , ew operator i, to the i, terface statio, computer 304 (e.g , usi, g the user i, put device 318).

After the step 1810, the routi, e 1418 proceeds to a step 1812 wherei, the routi, e 1418 waits u, til all of the requisite i, formatio, regardi, g the proposed , ew i, terface statio, operator has bee, e, tered properly.

2o Whe, , at the step 1812, it is determi, ed that all of the requisite i, formatio, regardi, g the proposed , ew operator has bee, e, tered properly, the routi, e proceeds to a step 1814 ,wherei, the , etwork server 114 is co, tacted.

After the step 1814, the routi, e 1418 proceeds to a step 1816, wherei, the request to add the , ew operator to the pocket vault i, terface u, it 302 is tra, smitted to the , etwork server 114.

After the step 1816, the routi, e 1418 proceeds to steps 1818 a, d 1820, wherei, it is determi, ed whether the request by the i, terface statio, computer has bee, ack, owledged by the , etwork server 114 prior to the expiratio, of a timeout period measured by the step 1820.

3o Whe, , at the steps 1818 a, d 1820, it is determi, ed that the request has , ot bee, ack, owledged i, a timely ma, , er, the routi, e 1418 proceeds to the step 1822, wherei, a tra, smissio, failure message is displayed.

After the step 1822, routi, e 1418 termi, ates.

Whe, , at the steps 1818 a, d 1820, it is determi, ed that the request has bee, ack, owledged i, a timely ma, , er, the routi, e 1418 proceeds to the step 1824, wherei, a message, i, cludi, g the i, formatio, regardi, g the proposed , ew operator a, d the i, terface u, it ID, is tra, smitted to the , etwork server 114 i, a, e, crypted ma, , er.

After the step 1824, the routi, e 1418 proceeds to steps 1826 a, d 1828, wherei, it is determi, ed whether e, crypted validatio, i, formatio, has bee, received from the , etwork server 114 prior to the expiratio, of a timeout period measured by the step 1828, a, d prior to the , etwork server 114 de, yi, g the additio, of the , ew i, terface statio, operator.

Whe, , at the steps 1826 a, d 1828, it is determi, ed that e, crypted validatio, i, formatio, has bee, received from the , etwork server 114 i, a timely ma, , er, the routi, e 1418 proceeds to a step 1830, wherei, the e, crypted validatio, i, formatio, is forwarded from the i, terface statio, computer 304 to the pocket vault i, terface u, it 302, such that the pocket vault i, terface u, it 302 is e, abled to store the fi, gerpri, t of the , ew operator m its memory.

After the step 1830, the routi, e 1418 proceeds to a step 1834, wherei, a message is ge, erated i, dicati, g that the attempt to add the , ew operator to the pocket vault i, terface u, it 302 was successful

After the step 1834, the routi, e 1418 termi, ates.

Whe, , at the steps 1826 a, d 1828, it is determi, ed that e, crypted validatio, i, formatio, has , ot bee, received from the , etwork server 114 i, a timely ma, , er, the routi, e 1418 proceeds to a step 1832, wherei, a message is ge, erated i, dicati, g that the attempt to add the , ew operator to the pocket vault i, terface u, it 302 was u, successful.

After the step 1832, routi, e 1418 termi, ates.

Fig. 19 is a flow diagram illustrati, g a, example impleme, tatio, of a primary routi, e 1900 that may be executed by the , etwork server 114 of Fig. 1.

As show, , the routi, e 1900 may begi, at a step 1902, wherei, it is determi, ed whether a, y requests have bee, received to register , ew Pocket Vault holders.

3o Whe, , at the step 1902, it is determi, ed that a request has bee, received to register a , ew Pocket Vault holder, the routi, e 1900 proceeds to a step 1904, wherei, the request to register the , ew Pocket Vault holder is processed. A, example of a routi, e that may be employed to impleme, t the step 1904 is discussed i, more detail below i, co, , ectio, with Fig. 20.

Whe, , at the step 1902, it is determi, ed that , o request to register a , ew Pocket Vault holder has bee, received, the routi, e 1900 proceeds to a step 1906, wherei, co, sumer marketi, g i, formatio, is compiled a, d tra, smitted to subscribi, g media issuers a, d advertisers.

After the step 1906, the routi, e 1900 proceeds to a step 1908, wherei, it is determi, ed whether a, y requests from media issuers or advertisers have bee, received to update the , etwork server 114

1 o Accordi, g to o, e aspect of the i, ve, tio, , media issuers a, d advertisers may have the optio, to utilize the fu, ctio, ality of the , etwork server 114 to update the accou, t characteristics of authe, ticated Pocket Vault holders. These updates may, for example, be delivered from the computers 108, 110, a, d 112 to a secure locatio, withi, the database 406. Whe, each selected holder , ext sy, chro, izes with , etwork server (e.g., as described below i, co, , ectio, with routi, e 1914 of Fig. 22), a, y media characteristics updated by the media issuers or advertisers may be uploaded to that holder's Pocket Vault 102. The database of accou, t updates may be revised periodically based o, the media issuer's systems (e.g., pursua, t to the routi, e 1910 of Fig. 21 -described below). Co, firmatio, of the update process may be provided to the issuer 2o after a sy, chro, izatio, sessio, is complete for a particular Pocket Vault holder (see step 2206 of routi, e 1914 (Fig. 22) below).

Whe, , at the step 1908, it is determi, ed that a request to update the , etwork server 114 has bee, received from a media issuer or advertiser, the routi, e proceeds to a step 1910, wherei, the request from the media issuer or advertiser is processed. A, example of a routi, e that may be employed to impleme, t the step 1910 is discussed i, more detail below i, co, , ectio, with Fig. 21.

Whe, , at the step 1908, it is determi, ed that , o request from a media issuer or advertiser to update the , etwork server 114 has bee, received, the routi, e 1900 proceeds to a step 1912, wherei, it is determi, ed whether a, y requests have bee, received from 3o holders to update i, formatio, o, their Pocket Vaults.

Whe, , at the step 1912, it is determi, ed that such a request has bee, received, the routi, e 1900 proceeds to a step 1914, wherei, the request to update the Pocket Vault i, formatio, is processed. A, example of a routi, e that may be employed to impleme, t the step 1914 is described i, more detail below i, co, , ection, with Fig. 22.

Whe, , at the step 1912, it is determi, ed that , o request from a holder to update i, formatio, o, a Pocket Vault 102 has bee, received, the routi, e 1900 proceeds to a step 1916, wherei, it is determi, ed whether a, y holders have requested that , ew files be loaded o, to the , etwork server 114.

Whe, , at the step 1916, it is determi, ed that a holder has requested that a , ew file be loaded o, to the , etwork server 114, the routi, e 1900 proceeds to a step 1918, wherei, the holder's request to load the , ew file o, to the , etwork server 114 is processed. A, to example of a routi, e that may be employed to impleme, t the step 1918 is described i, more detail below i, co, , ection, with Fig 23.

Whe, , at the step 1916, it is determi, ed that , o request by a holder to load a file o, to the , etwork server 114 has bee, received, the routi, e 1900 proceeds to a step 1920, wherei, it is determi, ed whether a, y requests have bee, made to authorize tra, saction, s.

Such a request may be made, for example, by a mercha, t operati, g a commercial i, terface statio, 104c. I, this regard, it should be appreciated that, whe, a teke, 102a is employed to e, gage i, a tra, saction, with a commercial card reader 106 or a commercial bar code reader 107, a request for tra, saction, approval may , ot be made to the , etwork server 114. I, stead such a tra, saction, approval request may be made through 2o co, ve, tio, al, existi, g commu, ication, a, d approval cha, , els for such devices.

Therefore, it should be u, derstood that the step 1922 is ge, erally reached o, ly whe, it is possible for the , etwork server 114 to check the ide, tity of the Pocket Vault holder, the ide, tity of the Pocket Vault 102, a, d possibly ide, tity of the operator of a commercial i, terface statio, , based c, commu, ication, s with the Pocket Vault 102 (e.g., via a commercial i, terface statio, 104c or via a wireless , etwork such as Bluetooth).

Whe, , at the step 1920, it is determi, ed that a request to authorize a tra, saction, has bee, made, routi, e 1900 proceeds to a step 1922, wherei, the request to authorize the tra, saction, is processed. A, example of a routi, e that may be employed to impleme, t the step 1922 is discussed i, more detail below i, co, , ection, with Fig. 24.

3o Whe, , at the step 1920, it is determi, ed , o request to authorize a tra, saction, has bee, made, the routi, e 1900 retur, s to the step 1902 (discussed above). With regard to the routi, e 1900 of Fig. 19, it should be appreciated that all of the requests to accomplish the various tasks may be placed i, a queue so that they are serviced o, a first-come, first-served or a, y other basis, rather tha, servici, g them i, the particular order show, i, Fig. 19.

Fig. 20 is a flow diagram illustrati, g a, example of a routi, e that may be employed to impleme, t the step 1904 of the routi, e 1900 (Fig. 1).

As show, , the routi, e 1904 begi, s at a step 2002, wherei, a request received from the i, terface statio, computer 304 to register a , ew Pocket Vault holder is ack, owledged, a, d the , etwork server 114 requests the i, terface statio, computer 304 to tra, sfer the releva, t i, formatio, regardi, g the proposed , ew holder to the , etwork I o server 114.

After the step 2002, the routi, e 1904 proceeds to a step 2004, wherei, the routi, e 1904 waits for all of the requisite holder registratio, i, formatio, to be received from the i, terface statio, computer 304.

Whe, , at the step 2004, it is determi, ed that all of the requisite holder registratio, i, formatio, has bee, received from the i, terface statio, computer 304, the routi, e 1904 proceeds to a step 2006, wherei, it is determi, ed whether the proposed Pocket Vault use is authorized. A, example of a routi, e that may be employed to impleme, t the step 2006 is discussed below i, co, , ection, with Fig. 25 I, determi, i, g whether a particular Pocket Vault use is authorized, there are , umerous parameters which may be checked.

2o For example, the port to which the i, terface statio, computer is co, , ected (e.g., the telepho, e , umber or IP address of the computer) may be checked to e, sure that it is authorized. Additio, ally, i, formatio, from the i, terface statio, computer 304 (e.g., a "cookie") may be checked to e, sure that the computer itself has bee, registered with the system. Further, it ca, be checked whether the curre, t operator of the i, terface statio, computer 304 is registered as bei, g associated with the i, terface statio, computer 304 bei, g used, a, d that the proposed , ew Pocket Vault holder is authorized to use that particular Pocket Vault 102. I, sum, the ide, tity of (1) each piece of equipme, t, (2) each operator of each piece of equipme, t, a, d (3) each locatio, of each piece of equipme, t may be checked to e, sure that the particular use of the Pocket Vault is authorized. It 3o should be appreciated fewer tha, all of these parameters, differe, t parameters, a, d/or additio, al parameters ca, be checked i, alter, ative embodime, ts of the i, ve, tio, , a, d that the i, ve, tio, is , ot limited to embodime, ts wherei, all of the aforeme, tio, ed parameters are checked to verify that a particular Pocket Vault use is authorized.

Whe, , at the step 2006, it is determi, ed that the Pocket Vault use is , ot authorized, the routi, e 1904 termi, ates. I, such a situatio, , it is also possible to ge, erate some sort of security alert message to put someo, e or some e, tity o, , otice that a, u, authorized use of a Pocket Vault has occurred.

Whe, , the routi, e 2006 has determi, ed that the proposed Pocket Vault use is authorized, the routi, e 1904 proceeds to a step 2008, wherei, all of the releva, t i, formatio, regardi, g the , ew Pocket Vault registratio, is logged i, to the database 406 of the , etwork server 114 (Fig. 4). As show, i, Fig. 20, this i, formatio, may i, clude, for example, the i, terface statio, operator ID, the i, terface u, it ID, the Pocket Vault ID, a, d all of the releva, t i, formatio, relati, g to the , ew Pocket Vault holder.

After the step 2008, the routi, e 1904 proceeds to a step 2010, wherei, the , etwork server 114 tra, smits e, crypted validatio, i, formatio, to the i, terface statio, computer 304, which the, may be passed o, to the pocket vault i, terface u, it 302, a, d the, to the Pocket Vault 102, so as to e, able the , ew holder's fi, gerpri, t to be stored i, the memory of the Pocket Vault 102.

After the step 2010, the routi, e 1904 termi, ates.

Fig. 21 is a flow diagram illustrati, g example of a routi, e that may be employed 2o to impleme, t the step 1910 of the primary routi, e 1900 (Fig. 19).

As show, , the routi, e 1910 begi, s at a step 2102, wherei, it is determi, ed whether all of the requested updates have bee, received from the media issuer or advertiser.

Whe, , at the step 2102, it has bee, determi, ed that all of the requested updates have bee, received, the routi, e 1910 proceeds to a step 2104, wherei, it is determi, ed whether the media issuer or advertiser is authorized access to the , etwork server 114.

This authorizatio, process may require some sort of authe, ticatio, of the ide, tity of the computer used by the media issuer or advertiser requesti, g the update, the operator of the computer, a, d/or the locatio, of the computer, i, a ma, , er similar to that i, which the 3o i, terface statio, s 104 a, d their operators are authorized.

Whe, , at the step 2104, it is determi, ed that the media issuer or advertiser is , ot authorized access to the , etwork server 114, the routi, e 1900 proceeds to a step 2106, wherei, a message is tra, smitted to the media issuer or advertiser i, formi, g the media issuer or advertiser that access to the , etwork server 114 has bee, de, ied.

After the step 2106, the routi, e 1910 termi, ates.

Whe, , at the step 2104, it is determi, ed that the media issuer or advertiser is authorized access to the , etwork server 114, the routi, e 1910 proceeds to a step 2108, wherei, the updates received from the media issuer or advertiser are logged o, to the , etwork server 114.

After the step 2108, the routi, e 1910 termi, ates.

Fig 22 is a flow diagram illustrati, g a, example a routi, e that may be employed I o to impleme, t the step 1914 of the primary routi, e 1900 (Fig. 19).

As show, , the routi, e 1914 begi, s at the step 2006 (discussed below i, co, , ection, with Fig. 25), wherei, it is determi, ed whether the attempted Pocket Vault use is authorized.

Whe, , at the step 2006, it is determi, ed that the Pocket Vault use is , ot authorized, the routi, e 1914 termi, ates.

Whe, , at the step 2006, it is determi, ed that the Pocket Vault use is authorized, the routi, e 1914 proceeds to a step 2202, wherei, e, crypted updates are tra, smitted to the i, terface statio, computer 304 for loadi, g o, to the Pocket Vault 102.

After the step 2202, the routi, e 1914 proceeds to steps 2204 a, d 2206, wherei, 2o the time a, d date of the updates are logged (step 2204), a, d the media issuers or advertisers are i, formed that the updates have bee, made (step 2206).

Fig. 23 is a flow diagram illustrati, g a, example of a routi, e that may be employed to impleme, t the step 1918 of the primary routi, e 1900 (Fig. 9).

As show, , the routi, e 1918 begi, s at a step 2302, wherei, it is determi, ed whether the file to be loaded o, to the , etwork server 114 relates to a secure media issuer.

Whe, , at the step 2302, it is determi, ed that the file does , ot relate to a secure media issuer, the routi, e 1918 proceeds to a step 2304, wherei, the , etwork server 114 is updated with the , e, -secure file.

After the step 2304, the routi, e 1918 termi, ates.
3o Whe, , at the step 2302, it is determi, ed that the to-be-loaded file does relate to a secure media issuer, the routi, e 1918 proceeds to a step 2306, wherei, it is determi, ed whether the secure media issuer is a Pocket Vault particip, t (i.e., a media issuer havi, g access to the , etwork server 114).
Whe, , at the step 2306, it is determi, ed that the secure media issuer is , ot a Pocket Vault particip, t, the routi, e 1918 proceeds to a step 2308, wherei, a, advisory is se, t to the holder i, dicati, g a, i, ability to load the file, a, d i, quiri, g as to whether the holder desires to load the file i, a , o, -secure format. The holder may, for example, opt to load the file to the , etwork server 114 i, such a way that the co, te, t of the file is , ot e, codable to the Chameleo, Card, but ca, be displayed a, d show, to a POS operator a, d ma, ually keyed i, at POS by the POS operator.
to After the step 2308, the routi, e 1918 proceeds to a step 2310, wherei, it is determi, e whether the holder has elected to load the file i, a , o, -secure format.
Whe, , at the step 2310, it is determi, ed that the holder has elected , ot to load the file i, a , o, -secure format, the routi, e 1918 termi, ates.
Whe, , at the step 2310, it is determi, ed that the holder has elected to load the file i, a , o, -secure format, the routi, e 1918 proceeds to a step 2318, wherei, the file is loaded o, to the , etwork server 114 i, a , o, -secure format.
After the step 2318, the routi, e 1918 termi, ates.
Whe, , at the step 2306, it is determi, ed that the secure media issuer is a Pocket Vault particip, t, the routi, e 1918 proceeds to a step 2310, wherei, the media issuer is 2o queried as to the accou, t status of the holder.
After the step 2310, the routi, e 1918 proceeds to a step 2312, wherei, it is determi, ed whether authorizatio, has bee, received from the media issuer to load the file.
Whe, , at the step 2312, it is determi, ed that authorizatio, has , ot bee, received from the media issuer, the routi, e 1918 proceeds to the step 2308 (discussed above).
Whe, , at the step 2312, it is determi, ed that authorizatio, has bee, received from the media issuer, the routi, e 1918 proceeds to a step 2314, wherei, the , etwork server 114 is updated with the secure file.
After the step 2314, the routi, e 1918 termi, ates.
3c Fig. 24 is a flow diagram illustrati, g a, example of a routi, e that may be employed to impleme, t the step 1922 of the primary routi, e 1900 (Fig. 19).

As show, , the routi, e 1922 begi, s at the step 2006 (discussed below i, co, , ectio, with Fig. 25), wherei, it is determi, ed whether the attempted use of the Pocket Vault 102 is authorized.
Whe, , at the step 2006, it is determi, ed that the attempted Pocket Vault use is , ot authorized, the routi, e 1922 termi, ates.
Whe, , at the step 2006, it is determi, ed that the attempted Pocket Vault used is authorized, the routi, e 1922 proceeds to a step 2402, wherei, it is determi, ed whether the requested tra, sactio, is withi, acceptable accou, t parameters (e.g., as set by the media issuer).
1 o Whe, , at the step 2402, it is determi, ed that the requested tra, sactio, is , ot withi, acceptable accou, t parameters, the routi, e 1922 proceeds to a step 2404, wherei, a message is tra, smitted to the e, tity that requested the tra, sactio, (e.g., a commercial i, terface static, 104C, a card reader 106, or a barcode reader 107) i, dicati, g that the tra, sactio, is outside of acceptable accou, t parameters.
15 After the step 2404, the routi, e 1922 termi, ates.
Whe, , at the step 2402, it is determi, ed that the requested tra, sactio, is withi, acceptable accou, t parameters, i, formatio, regardi, g the tra, sactio, is logged i, to the database 406 of the , etwork server 114 (Fig. 4). As show, , the logged i, formatio, may i, clude the ide, tificatio, of the e, tity with which the tra, sactio, took place, the Pocket 2o Vault ID (if available), a, d the time a, d date of the tra, sactio, .
After the step 2406, the routi, e 1922 proceeds to a step 2408, wherei, a, e, crypted approval message is tra, smitted to the e, tity with which the tra, sactio, is bei, g attempted (e.g., a commercial i, terface statio, 104C, a card reader 106, or a barcode reader 107).
25 After the step 2408, the routi, e 1922 termi, ates.
Fig. 25 is a flow diagram illustrati, g a, example of a routi, e that may employed to impleme, t the step 2006 of the routi, es 1904 (Fig. 20), 1914 (Fig. 22), a, d 1922 (Fig. 24).
As show, , the routi, e 2006 begi, s at a step 2502, wherei, it is determi, ed 3o whether the poi, t of sale termi, al or other e, tity with which a tra, sactio, is bei, g attempted is co, , ected to a valid source (e.g., a, authorized telepho, e li, e or a, authorized I, ter, et protocol (IP) address).

Whe, , at the step 2502, it is determi, ed that the e, tity proposi, g the tra, sactio, is , ot co, , ected to a valid source, the routi, e 2006 proceeds to a step 2510, wherei, the tra, sactio, is refused, a, d a security alert is ge, erated so that appropriate actio, s) may be take, .
Whe, , at the step 2502, it is determi, ed that the e, tity proposi, g the tra, sactio, is co, , ected to a valid source, the routi, e 2006 proceeds to a step 2504, wherei, it is determi, ed whether the ID of the i, terface statio, , card reader or barcode reader is valid, a, d is properly li, ked to the source to which is co, , ected.
Whe, , at the step 2504, it is determi, ed that the ID of the e, tity proposi, g the 1 o tra, sactio, is , ot valid, the routi, e proceeds to the step 2510 (discussed above).
Whe, , at the step 2504, it is determi, ed that the ID of the e, tity proposi, g the tra, sactio, is valid, the routi, e 2006 proceeds to a step 2506, wherei, it is determi, ed whether the Pocket Vault ID (if available) is valid. It should be appreciated that, whe, a card reader 106, a barcode reader 107 or a, RF sig, al receiver is employed, it is possible 15 that the ID from the Pocket Vault will , ot be tra, smitted to the , etwork server 114.
Therefore, the step 2506 may be skipped i, such a situatio, .
Whe, , at the step 2506, it is determi, ed that the Pocket Vault ID (whe, available a, d required) is , ot valid, the routi, e 2006 proceeds to the step 2510 (discussed above).
Whe, , at the step 2506, it is determi, ed that the Pocket Vault ID (whe,) is valid 20 or is , ot required, the routi, e 2006 proceeds to a step 2508, wherei, it is determi, ed whether the Pocket Vault ID (if available) is li, ked to the ID of the e, tity proposi, g the tra, sactio, , e.g., a commercial i, terface static, 104c, a card reader 106, or a barcode reader 107.
Whe, , at the step 2508, it is determi, ed that the ID of the Pocket Vault 102 25 (whe, available) is , ot li, ked to the ID of the e, tity proposi, g the tra, sactio, , the routi, e 2006 proceeds to the step 2510 (discussed above).
Whe, , at the step 2508, it is determi, ed that the Pocket Vault ID is li, ked to the ID of the e, tity proposi, g the tra, sactio, , or that the ID of the Pocket Vault is , ot required, the routi, e 2006 proceeds to a step 2512, wherei, the Pocket Vault use is 3 o authorized.
With regard to the i, formatio, checked i, co, , ectio, with the routi, e 2006 to determi, e whether a particular Pocket Vault use is authorized, it should be appreciated that, i, some embodime, ts, fewer tha, all of the verificatio, steps discussed above may be performed whe, lesser degrees of security are desired or required. For example, i, some embodime, ts, there may be , o restrictio, s as to who ca, operate a, i, terface statio, , the source to which the static, is co, , ected, a, d/or the ID of the statio, .
O, e illustrative example of a, applicatio, of the , etwork system 100 (Fig. 1) is i, the distributio, of buildi, g access key cards a, d similar limited-use, time-se, sitive media to i, dividual operators. The followi, g typical sce, ario i, volves distributio, of hotel room key cards to hotel guests who make room reservatio, s over the I, ter, et. Usi, g a hotel's secure web site, the prospective guest, who is also a Pocket Vault holder, 1 o may secure a room for a specific time period by providi, g a credit card , umber. This step may or may , ot i, volve use of a credit card stored o, the Pocket Vault 102. If it does i, volve use of a Pocket Vault credit card, this card may, for example, be accessed while the Pocket Vault 102 is i, terfaced with the holder's perso, al i, terface statio, 104b. Next, the prospective hotel guest may li, k to the , etwork server 114 (while 15 stayi, g withi, the hotel's website), a, d follow o, -scree, i, structio, s for dow, loadi, g the key card for his/her room o, to the Pocket Vault 102 (e.g., to e, sure that Pocket Vault 102 is i, terfaced with the pocket vault i, terface u, it 302, a, d to e, sure that the Pocket Vault holder has activated the Pocket Vault 102 by the appropriate security mecha, ism such as a thumbpri, t for bio-metric ID verificatio,). After dow, loadi, g is complete, the 2o display 216 of the Pocket Vault 102 may i, clude a, ico, for the hotel room key (e.g., the hotel's logo), alo, g with the ico, s for media previously loaded. Whe, the room key card ico, is selected, the Pocket Vault 102 may e, code the Chameleo, Card with the mag, etic stripe codi, g to u, lock the guest's hotel room.
After the time period of the guest's room reservatio, has expired, the Pocket 25 Vault 102 may automatically delete the room key ico, . This deletio, may occur for the

Patent Citations (72)

key card) after the key card's specified time period has expired.

Having thus described at least one illustrative embodiment of the invention, various alterations, modifications and improvements will readily occur to those skilled in the art. Such alterations, modifications and improvements are intended to be within the spirit and scope of the invention. Accordingly, the foregoing description is by way of example only and is not intended as limiting. The invention is limited only as defined in the following claims and the equivalents thereto.

What is claimed is:

Publication number	Priority date	Publication date	Assignee	Title
US4701601A *	1985-04-26	1987-10-20	Visa International Service Association	Transaction card with magnetic stripe emulator
US4791283A	1986-06-03	1988-12-13	Intellicard International, Inc.	Transaction card magnetic stripe emulator
US4868376A *	1987-05-15	1989-09-19	Smartcard International Inc.	Intelligent portable interactive personal data system
DE3906349C2	1989-03-01	1991-08-08	Hartmut 7000 Stuttgart De Hein	
US5885787A	1991-12-09	1996-12-17	Wallerstein; Robert S.	Programmable credit card
US5955961A *	1991-12-09	1999-09-21	Wallerstein; Robert S.	Programmable transaction card
IL104422A *	1993-01-18	1996-03-31	Labate; Isaac J	Method and apparatus for magnetically writing on plastic cards
US5544246A	1993-09-17	1996-08-06	At&T Corp.	Smartcard adapted for a plurality of service providers and for remote installation of same
GB9323489D0	1993-11-08	1994-01-05	Ncr Int Inc	Self-service business system
US5578808A *	1993-12-22	1996-11-26	Datamark Services, Inc.	Data card that can be used for transactions with volving separate card issuers
US5796834A *	1994-01-03	1998-08-18	E-Stamp Corporation	System and method for controlling the dispensing of an authentication indicia
US5623552A	1994-01-21	1997-04-22	Cardguard International, Inc.	Self-authenticating identification card with fingerprint identification
US5598474A	1994-03-29	1997-01-28	Neldon P Johnson	Process for encrypting a fingerprint onto an I.D. card
US5590038A	1994-06-20	1996-12-31	Pitroda; Satya G.	Universal electronic transaction card including receipt storage and system and methods of conducting electronic transactions
GB9413614D0 *	1994-07-06	1994-08-24	Ashley Philip M	Credit card or the like and system utilising same
US5546471A	1994-10-28	1996-08-13	The National Registry, Inc.	Ergonomic fingerprint reader apparatus
US5748737A *	1994-11-14	1998-05-05	Daggar; Robert N.	Multimedia electronic wallet with generic card
US5870723A	1994-11-28	1999-02-09	Pare, Jr.; David Ferrin	Tokenless biometric transaction authorization method and system
US5979773A	1994-12-02	1999-11-09	America Card Technology, Inc.	Dual smart card access control electronic data storage and retrieval system and methods
US5598792A	1995-01-09	1997-02-04	Wales; Forrest A.	Credit card security device having card identification electromagnetic
US5546523A *	1995-04-13	1996-08-13	Gatto; James G.	Electronic fund transfer system
US5705749Z2	1995-10-11	2006-06-06	Motorola, Inc.	Enablement of a feature of an electronic device using radio frequency identification technology
US5907142A	1995-12-12	1999-05-25	Kelsey; Craig E.	Fraud resistant personally activated transaction card
US5745574A	1995-12-15	1998-04-28	Entegrity Solutions Corporation	Security infrastructure for electronic transactions
US5943423A	1995-12-15	1999-08-24	Entegrity Solutions Corporation	Smart token system for secure electronic transactions and identification
US5777903A	1996-01-22	1998-07-07	Motorola, Inc.	Solar cell powered smart card with integrated display and interface keypad
US5963679A	1996-01-26	1999-10-05	Harris Corporation	Electric field fingerprint sensor apparatus and related methods
JP3590184B2	1996-03-08	2004-11-17	株式会社東芝	Finger detection device
US6038551A	1996-03-11	2000-03-14	Microsoft Corporation	System and method for configuring and managing resources on a multi-purpose integrated circuit card using a personal computer
GB9608747D0	1996-04-26	1996-07-03	Philips Electronics	Fingerprint sensing devices and systems incorporating such

			Nv	
US5815657A	1996-04-26	1998-09-29	Verifo, e, t, c.	System, method a, d article of ma, ufacture for , etwork electro, ic authorizatio, utilizi, g a, authorizatio, i, strume, t
US5854891A *	1996-08-09	1998-12-29	Tritheim Tech, ologies, i, c.	Smart card reader havi, g multiple data e, abli, g storage compartme, ts
US5867795A	1996-08-23	1999-02-02	Motorola, i, c.	Portable electro, ic device with tra, sceiver a, d visual image display
AU4196497A	1996-09-18	1998-04-14	Dew E, gi, eeri, g A, d Developme, t Limited	Biometric ide, tificatio, system for providi, g secure access
US5917913A *	1996-12-04	1999-06-29	Wa, g; Y, jiu, Paul	Portable electro, ic authorizatio, devices a, d methods therefor
US5915023A	1997-01-06	1999-06-22	Ber, stei, , Robert	Automatic portable accou, t co, troller for remotely arra, gi, g for tra, sfer of value to a recipie, t
US5982913A	1997-03-25	1999-11-09	The U, ited States Of America As Represe, ted By The Natio, al Security Age, cy	Method of verificatio, usi, g a subset of claima, t's fi, gerpri, t
US6012636A *	1997-04-22	2000-01-11	Smith, Fra, k E.	Multiple card data system havi, g first a, d seco, d memory eleme, ts i, cludi, g mag, etic strip a, d fi, gerpri, ts sca, , i, g mea, s
US5920640A	1997-05-16	1999-07-06	Harris Corporatio,	Fi, gerpri, t se, sor a, d toke, reader a, d associated methods
US5974146A	1997-07-30	1999-10-26	Ru, ti, gto, Ba, oshares I, corporated	Real time ba, k-ce, tric u, iversal payme, t system
US6016476A	1997-08-11	2000-01-18	I, ter, atio, al Busi, ess Machi, es Corporatio,	Portable i, formatio, a, d tra, sactio, processi, g system a, d method utilizi, g biometric authorizatic, a, d digital certificate security
US5969318A	1997-11-24	1999-10-19	Macke, thu, ; Holger	Gateway apparatus for desig, i, g a, d issui, g multiple applicatio, cards
CN1280686A	1997-12-02	2001-01-17	凯奕技术公司	Multi-tra, sactio, al , etwork architecture
WO1999034314A1	1997-12-30	1999-07-08	Pitroda Satya, G	U, iversal electro, ic commu, icatio, s card
US6188830B1	1998-01-07	2001-02-13	AlST Corp	Method a, d apparatus for mi, imizi, g credit card fraud
KR100601178B1 *	1998-01-27	2006-07-13	삼성전자주식회사	Tra, smitti, g advertiseme, ts to smart cards
US6095416A *	1998-02-24	2000-08-01	Privicom, I, c.	Method a, d device for preve, ti, g u, authorized use of credit cards
US6182892B1 *	1998-03-25	2001-02-06	Compaq Computer Corporatio,	Smart card with fi, gerpri, t image pass-through
DE19816117A1	1998-04-09	1999-10-14	Primax Electro, ics Ltd	Electro, ic code co, trolled access to computer system
US6334121B1	1998-05-04	2001-12-25	Virgi, ia Commo, wealth U, iversity	Usage patter, based user authe, ticator
US6332128B1	1998-07-23	2001-12-18	Autogas Systems, I, c.	System a, d method of providi, g multiple level discou, ts o, cross-marketed products a, d discou, ti, g a price-per-u, it-volume of gasoli, e
US6356941B1	1999-02-22	2002-03-12	Cyber-Ark Software Ltd.	Network vaults
US646613082	1999-07-29	2002-10-15	Micro, Tech, ology, I, c.	Wireless commu, icatio, devices, wireless commu, icatio, systems, commu, icatio, methods, methods of formi, g radio freque, cy ide, tificatio, devices, methods of testi, g wireless commu, icatio, operatio, s, radio freque, cy ide, tificatio, devices, a, d methods of formi, g radio freque, cy ide, tificatio, devices
CA2388007A1	1999-09-28	2001-04-05	Chameleo, Network I, c.	Portable electro, ic authorizatio, system a, d associated method
US7080037B2	1999-09-28	2006-07-18	Chameleo, Network I, c.	Portable electro, ic authorizatio, system a, d method
US6374757B1	1999-12-02	2002-04-23	Av, er Farkash	Credit card security device
EP1317718A2	2000-02-28	2003-06-11	360 Degree Web, I, c.	Smart card e, abled mobile perso, al computi, g e, vir, me, t
US20020062251A1	2000-09-29	2002-05-23	Raja, A, a, da,	System a, d method for wireless co, sumer commu, icatio, s
US7353014B2	2000-10-31	2008-04-01	Vijay Raghava,	U, iversal portable u, it

			Chetty	
US6950939B2	2000-12-08	2005-09-27	So, y Corporatio,	Perso, al tra, sactio, device with secure storage o, a removable memory device
US20020161708A1	2001-02-01	2002-10-31	Gero Offer	Method a, d apparatus for performi, g a cashless payme, t tra, sactio,
WO2003044721A2	2001-11-19	2003-05-30	Burchette Robert L. Jr	Tra, sactio, card system havi, g security agai, st u, authorized usage
US7028897B2	2001-12-26	2006-04-18	Vivotech, I, c.	Adaptor for mag, etic stripe card reader
US7059532B2	2001-12-26	2006-06-30	Vivotech, I, c.	Adaptor for mag, etic stripe card reader
US20040159700A1	2001-12-26	2004-08-19	Vivotech, I, c.	Method a, d apparatus for secure import of i, formatio, i, to data aggregatio, program hosted by perso, al trusted device
US7127236B2	2001-12-26	2006-10-24	Vivotech, I, c.	Micropayme, t fi, a, cial tra, sactio, process utilizi, g wireless , etwork processi, g
USD491953S1	2002-10-10	2004-06-22	Vivotech, I, c.	Proximity i, terface with advertisi, g i, sert for tra, sactio, accepta, ce systems
USD490840S1	2002-10-30	2004-06-01	Vivotech, I, c.	Proximity i, terface for tra, sactio, accepta, ce systems
USD491186S1	2002-11-27	2004-06-08	Vivotech, I, c.	Mag, etic stripe simulacrum for tra, sactio, accepta, ce systems
USD498236S1	2003-01-24	2004-11-09	Vivotech, I, c.	Coreless i, ductor mag, etic stripe simulacrum for tra, sactio, accepta, ce systems
GB2393014B	2003-02-25	2004-08-11	Coupo, s Ltd I	Providi, g discou, ts at a POS termi, al
USD506998S1	2003-02-28	2005-07-05	Vivotech, I, c.	Coreless i, ductor mag, etic stripe simulacrum for right a, gle tra, sactio, accepta, ce systems

* Cited by exami, er, † Cited by third party

Cited By (289)

Publicatio, , umber	Priority date	Publicatio, date	Assig, ee	Title
Family To Family Citatio, s				
CN101299255B *	1999-05-25	2020-05-19	臺灣派澳大利亞有限公司	O, li, e tra, sactio, processi, g system
US7578439B2 *	1999-08-19	2009-08-25	E2I, teractive, I, c.	System a, d method for authorizi, g stored value card tra, sactio, s
US8706638B2	1999-08-19	2014-04-22	E2I, teractive, I, c.	System a, d method for securely authorizi, g a, d distributi, g stored-value card data
US7108003B2	1999-09-28	2006-09-19	Chameleo, Network I, c.	Portable electro, ic authorizatio, system a, d method
CA2388007A1	1999-09-28	2001-04-05	Chameleo, Network I, c.	Portable electro, ic authorizatio, system a, d associated method
US7340439B2	1999-09-28	2008-03-04	Chameleo, Network I, c.	Portable electro, ic authorizatio, system a, d method
US7742967B1 *	1999-10-01	2010-06-22	Cardi, alcommerce Corporatio,	Secure a, d efficie, t payme, t processi, g system
US9430769B2	1999-10-01	2016-08-30	Cardi, alcommerce Corporatio,	Secure a, d efficie, t payme, t processi, g system
WO2001041032A1 *	1999-11-30	2001-06-07	David Russell	Methods, systems, a, d apparatuses for secure i, teractio, s
US6445301B1	2000-02-23	2002-09-17	So, y Corporatio,	Method of usi, g perso, al device with i, ter, al biometric i, co, ducti, g tra, sactio, s over a , etwork
US7127526B1 *	2000-03-20	2006-10-24	Nortel Networks Limited	Method a, d apparatus for dy, amically loadi, g a, d ma, agi, g software services o, a , etwork device
JP2001344545A *	2000-03-29	2001-12-14	Ibm Japa, Ltd	Processi, g system, server, processi, g termi, al, commu, icatio, termi, al, processi, g method, data ma, agi, g method, processi, g performi, g method a, d program
US7050039B1 *	2000-07-18	2006-05-23	Xili, x, I, c.	Arra, geme, ts e, abli, g a, audie, ce to replay a prese, tatio,
US7383014B2 *	2000-10-31	2008-04-01	Vijay Raghava, Chetty	U, iversal portable u, it
EP1213638A1 *	2000-12-06	2002-06-12	Sieme, s Aktie, gesellschaft	E, abli, g devices
US6696683B2 *	2000-12-21	2005-11-15	Digimarc Corporatio,	Routi, g , etworks for use with watermark systems
US7124300B1 *	2001-01-24	2006-10-17	Palm, I, c.	Ha, dheld computer system co, figured to authe, ticate a user a, d power-up i, respo, se to a si, gle actio, by the user

US20020124190A1 *	2001-03-01	2002-09-05	Bria, Siegel	Method a, d system for restricted biometric access to co, te, t of packaged media
US7237117B2	2001-03-16	2007-06-26	Ke, , eth R Weiss	U, iversal secure registry
US7139793B2 *	2001-05-01	2006-11-21	I, ter, atio, al Busi, ess Machi, es Corporatio,	Method for co, ve, ie, tly e, abli, g a web server to provide commercial promotio, s usi, g compiled code
EP2273342A1 *	2001-05-24	2011-01-12	Sc, y Corporatio,	Service providi, g method a, d i, tegrated circuit
EP1282089B1 *	2001-08-03	2009-12-16	Telefo, aktiebolaget LM Ericsso, (pubi)	Method a, d devices for i, ter-termi, al payme, ts
US9412417B2 *	2002-04-05	2016-08-09	Apple I, c.	Persiste, t group of media items for a media device
US20030115135A1 *	2001-12-17	2003-06-19	Sarfraz Aamer Ahmad	Method a, d apparatus for recordi, g tra, sactio, s
JP4187481B2 *	2002-03-15	2008-11-26	松下電器産業株式会社	Perso, al authe, ticatio, device a, d mobile termi, al
WO2003081519A2 *	2002-03-19	2003-10-02	Chameleo, Network I, c.	Portable electro, ic authorizatio, system a, d method
AUPS265302A0	2002-05-30	2002-06-20	Mcom Solutio, s I, c	Display device a, d fu, ds tra, sactio, device i, ciudi, g the display device
US7797446B2	2002-07-16	2010-09-14	Apple I, c.	Method a, d system for updati, g playlists
US7306143B2 *	2002-09-20	2007-12-11	Cubic Corporatio,	Dy, amic smart card/media imagi, g
DE10251839A1 *	2002-11-07	2004-05-19	Robert Bosch Gmbh	Motor vehicle microco, troller co, trol method, i, volves checki, g re-writable area with check program a, d triggeri, g RESET if checked area is ma, ipulated or cou, ter overflows
US7046234B2 *	2002-11-21	2006-05-16	Bloomberg Lp	Computer keyboard with processor for audio a, d telepho, y fu, ctio, s
US20040143550A1 *	2002-12-19	2004-07-22	I, ter, atio, al Busi, ess Machi, es Corporatio,	Cellular electro, ic wallet device a, d method
US20040130578A1 *	2003-01-08	2004-07-08	Douglas Char, ey	Method a, d system for selectio, of me, u items i, a telepho, e me, u scree, i, terface
JP4126391B2 *	2003-03-07	2008-07-30	カシオ計算機株式会社	Sales data processi, g apparatus a, d program
CA2429623A1 *	2003-05-26	2004-11-26	Cstar Tech, ologies I, c.	System a, d method for tracki, g i, ve, tory
US7308584B2 *	2003-08-14	2007-12-11	I, ter, atio, al Busi, ess Machi, es Corporatio,	System a, d method for securi, g a portable processi, g module
US20050038879A1 *	2003-08-14	2005-02-17	I, ter, atio, al Busi, ess Machi, es Corporatio,	System a, d method for discovery of remote device driver fu, ctio, ality a, d i, terface
US7225448B2 *	2003-08-14	2007-05-29	Le, ovo (Si, gapore) Pte. Ltd.	System a, d method for hiber, ati, g applicatio, state data o, removable module
US7761374B2	2003-08-18	2010-07-20	Visa I, ter, atio, al Service Associatio,	Method a, d system for ge, erati, g a dy, amic verificatio, value
US7740168B2	2003-08-18	2010-06-22	Visa U.S.A. I, c.	Method a, d system for ge, erati, g a dy, amic verificatio, value
US6817521B1 *	2003-08-21	2004-11-16	I, ter, atio, al Busi, ess Machi, es Corporatio,	Credit card applicatio, automatio, system
US20050110729A1 *	2003-11-26	2005-05-26	Cok Ro, ald S.	Display system
US20050187821A1 *	2004-02-24	2005-08-25	Joshua Lapsker	Reusable discou, t card a, d prescriptio, drug compila, ce system
US20050222922A1 *	2004-03-16	2005-10-06	Ly, ch Robert G	Method for calculati, g IBNP health reserves with low varia, ce
US9715500B2 *	2004-04-27	2017-07-25	Apple I, c.	Method a, d system for shari, g playlists
US20050269401A1 *	2004-06-03	2005-12-08	Tyfo, e, I, c.	System a, d method for securi, g fi, a, cial tra, sactio, s
WO2005119607A2 *	2004-06-03	2005-12-15	Tyfo, e, I, c.	System a, d method for securi, g fi, a, cial tra, sactio, s
US9286457B2	2004-06-14	2016-03-15	Rod, ey Beatso,	Method a, d system for providi, g password-free, hardware-rooted, ASIC-based authe, ticatio, of a huma, to a mobile device usi, g biometrics with a protected, local template to release trusted crede, tials to relyi, g parties
US7562218B2 *	2004-08-17	2009-07-14	Research I, Motio, Limited	Method, system a, d device for authe, ticati, g a user
US8261246B1	2004-09-07	2012-09-04	Apple I, c.	Method a, d system for dy, amically populati, g groups i, a developer e, viro, me, t
US7469291B2 *	2004-09-22	2008-12-23	Research I, Motio, Limited	Apparatus a, d method for i, tegrati, g authe, ticatio, protocols i, the establishme, t of co, , ectio, s betwee, computi, g devices

US7257373B2 *	2004-10-14	2007-08-14	I, ter, atio, al Busi, ess Machi, es Corporatio,	Method a, d apparatus for determi, i, g adjace, cy of wireless device to POS termi, al
US7680849B2 *	2004-10-25	2010-03-16	Apple I, c.	Multiple media type sy, chro, izatio, betwee, host computer a, d media device
US8321269B2 *	2004-10-26	2012-11-27	Validclick, I, c	Method for performi, g real-time click fraud detectio, , preve, tio, a, d reporti, g for o, li, e advertisi, g
US7958441B2 *	2005-01-07	2011-06-07	Apple I, c.	Media ma, ageme, t for groups of media items
US7124937B2 *	2005-01-21	2006-10-24	Visa U S.A I, c.	Wireless payme, t methods a, d systems
US8553385B2 *	2005-01-27	2013-10-08	Blackberry Limited	Wireless perso, al area , etwork havi, g authe, ticatio, a, d associated methods
US7581678B2	2005-02-22	2009-09-01	Tyfo, e, I, c.	Electro, ic tra, sactio, card
US7128274B2 *	2005-03-24	2006-10-31	I, ter, atio, al Busi, ess Machi, es Corporatio,	Secure credit card with , ear field commu, icatio, s
WO2006116772A2	2005-04-27	2006-11-02	Privasys, I, c.	Electro, ic cards a, d methods for maki, g same
US8684267B2	2005-03-26	2014-04-01	Privasys	Method for broadcasti, g a mag, etic stripe data packet from a, electro, ic smart card
JP5186359B2	2005-03-26	2013-04-17	プリバシーズ、インコーポレイテッド	Electro, ic fi, a, cial tra, sactio, card a, d method
US20060226217A1 *	2005-04-07	2006-10-12	Tyfo, e, I, c.	Sleeve for electro, ic tra, sactio, card
US7793851B2 *	2005-05-09	2010-09-14	Dy, amics I, c.	Dy, amic credit card with mag, etic stripe a, d embedded e, coder a, d methods for usi, g the same to provide a copy-proof credit card
US20080035738A1 *	2005-05-09	2008-02-14	Mulle, Jeffrey D	Dy, amic credit card with mag, etic stripe a, d embedded e, coder a, d methods for usi, g the same to provide a copy-proof credit card
US7661146B2 *	2005-07-01	2010-02-09	Privamed, I, c.	Method a, d system for providi, g a secure multi-user portable database
US8189788B2 *	2005-07-15	2012-05-29	Tyfo, e, I, c.	Hybrid symmetric/asymmetric cryptography with user authe, ticatio,
US7805615B2 *	2005-07-15	2010-09-28	Tyfo, e, I, c.	Asymmetric cryptography with user authe, ticatio,
US8477940B2 *	2005-07-15	2013-07-02	Tyfo, e, I, c.	Symmetric cryptography with user authe, ticatio,
US8066543B2	2006-04-05	2015-06-23	Visa U.S.A. I, c.	System a, d method for accou, t ide, tifier obfuscatio,
US20070168250A1 *	2005-09-30	2007-07-19	Mastercard I, ter, atio, al I, corporated	Payme, t apparatus a, d method
US8528096B2 *	2005-10-07	2013-09-03	Stmicroelectro, ics, I, c.	Secure u, iversal serial bus (USB) storage device a, d method
US20060179004A1 *	2005-12-07	2006-08-10	Bill Fuchs	BioMetric PayPoi, t System
US7657486B2 *	2005-12-09	2010-02-02	Mastercard I, ter, atio, al I, corporated	Tech, iques for co-existe, ce of multiple stored value applicatio, s o, a si, gle payme, t device ma, agi, g a shared bala, ce
US20070150411A1 *	2005-12-14	2007-06-28	Addepalli Sateesh K	U, iversal payme, t system
US20070131759A1 *	2005-12-14	2007-06-14	Cox Mark A	Smartcard a, d mag, etic stripe emulator with biometric authe, ticatio,
US20080126260A1 *	2006-07-12	2008-05-29	Cox Mark A	Poi, t Of Sale Tra, sactio, Device With Mag, etic Stripe Emulator A, d Biometric Authe, ticatio,
US7509588B2	2005-12-30	2009-03-24	Apple I, c.	Portable electro, ic device with i, terface reco, figuratio, mode
US7828204B2 *	2006-02-01	2010-11-09	Mastercard I, ter, atio, al I, corporated	Tech, iques for authorizatio, of usage of a payme, t device
EP1987463A1	2006-02-21	2008-11-05	WEISS, Ke, , eth P.	Method a, d apparatus for secure access payme, t a, d ide, tificatio,
US8234220B2	2007-02-21	2012-07-31	Weiss Ke, , eth P	U, iversal secure registry
US20070203852A1 *	2006-02-24	2007-08-30	Microsoft Corporatio,	ide, tity i, formatio, i, cludi, g reputatio, i, formatio,
US8117459B2 *	2006-02-24	2012-02-14	Microsoft Corporatio,	Perso, al ide, tificatio, i, formatio, schemas
US20070234065A1 *	2006-04-04	2007-10-04	Labcal Tech, ologies I, c.	Biometric ide, tificatio, device providi, g format co, versio, fu, ctio, ality a, d method for impleme, ti, g said fu, ctio, ality
US20070234066A1 *	2006-04-04	2007-10-04	Labcal Tech, ologies, I, c.	Biometric ide, tificatio, device providi, g format co, versio, fu, ctio, ality a, d method for impleme, ti, g said fu, ctio, ality
US7818264B2 *	2006-06-19	2010-10-19	Visa U.S.A. I, c.	Track data e, cryptio,

US11062342B2 *	2006-07-27	2021-07-13	Blackhawk Network, I, c.	System a, d method for targeted marketi, g a, d co, sumer resource ma, ageme, t
US8078880B2 *	2006-07-28	2011-12-13	Microsoft Corporatio,	Portable perso, al ide, tity i, formatio,
US20080027819A1 *	2006-07-29	2008-01-31	Joh, Ruckart	Methods, systems, a, d products for purchasi, g products
US10313505B2 *	2006-09-06	2019-06-04	Apple I, c.	Portable multifu, ctio, device, method, a, d graphical user i, terface for co, figuri, g a, d displayi, g widgets
US8125567B2 *	2006-09-15	2012-02-28	Avery Levy	System a, d method for e, abli, g tra, sactio, s by mea, s of pri, t media that i, corporate electro, ic recordi, g a, d tra, smissio, mea, s
JP2010508601A *	2006-10-31	2010-03-18	ソリコアインコーポレイテッド	Battery-powered authe, tication, card
JP5684475B2 *	2006-10-31	2015-03-11	ソリコアインコーポレイテッドSOLICORE, Incorporated	Battery powered devices
JP2008141400A *	2006-11-30	2008-06-19	So, y Ericsso, Mobilecommu, ication, s Japa, i, c	Commu, ication, system, commu, ication, termi, al a, d commu, ication, method
US7991158B2	2006-12-13	2011-08-02	Tyfo, e, I, c.	Secure messagi, g
WO2008082617A2 *	2006-12-29	2008-07-10	Solicore, I, c.	Maili, g apparatus for powered cards
WO2008082616A1 *	2006-12-29	2008-07-10	Solicore, I, c.	Card co, figured to receive separate battery
US8519964B2	2007-01-07	2013-08-27	Apple I, c.	Portable multifu, ctio, device, method, a, d graphical user i, terface supporti, g user , avigatio, s of graphical objects o, a touch scree, display
JP2010516002A	2007-01-09	2010-05-13	ビザユー、エス、エー、インコーポレイテッド	Co, tactless tra, sactio,
US8407767B2 *	2007-01-18	2013-03-26	Microsoft Corporatio,	Provisio, i, g of digital ide, tity represe, tatio, s
US8087072B2 *	2007-01-18	2011-12-27	Microsoft Corporatio,	Provisio, i, g of digital ide, tity represe, tatio, s
US8689296B2 *	2007-01-26	2014-04-01	Microsoft Corporatio,	Remote access of digital ide, tities
GB2446211B *	2007-01-31	2012-03-07	Hewlett Packard Developme, t Co	Method a, d apparatus for e, abli, g i, teractio, betwee, a mobile device a, d a, other device
DE602007013632D1 *	2007-02-23	2011-05-19	First Data Corp	Fraud detectio, system for poi, t-of-sale termi, als
US20080244208A1 *	2007-03-30	2008-10-02	Nare, dra Siva G	Memory card hidde, comma, d protocol
US9772751B2	2007-06-29	2017-09-26	Apple I, c.	Usi, g gestures to slide betwee, user i, terfaces
KR20090011149A *	2007-07-25	2009-02-02	삼성전자주식회사	A method of purchasi, g a digital broadcast service i, a portable termi, al which is equipped a smart card a, d a, apparatus thereof
US8635998B2 *	2007-08-16	2014-01-15	Verifo, e, I, c	Metrics systems a, d methods for toke, tra, sactio, s
US8046369B2 *	2007-09-04	2011-10-25	Apple I, c.	Media asset rati, g system
US8619038B2	2007-09-04	2013-12-31	Apple I, c.	Editi, g i, terface
US11126321B2 *	2007-09-04	2021-09-21	Apple I, c.	Applicatio, me, u user i, terface
US20090108730A1 *	2007-10-19	2009-04-23	Mastercard I, ter, atio, al I, corporated	Apparatus a, d method for usi, g a device co, formi, g to a payme, t sta, dard for access co, trol a, d/or secure data storage
US8311913B2 *	2007-10-30	2012-11-13	Visa U.S.A. I, c.	Payme, t e, tity accou, t set up for multiple payme, t methods
US8311914B2	2007-10-30	2012-11-13	Visa U.S.A. I, c.	Payme, t e, tity for accou, t payables processi, g usi, g multiple payme, t methods
US8311937B2 *	2007-10-30	2012-11-13	Visa U.S.A. I, c.	Clie, t supported multiple payme, t methods system
US8374932B2 *	2007-10-30	2013-02-12	Visa U.S.A. I, c.	Payme, t e, tity device tra, sactio, processi, g usi, g multiple payme, t methods
US8407141B2 *	2007-10-30	2013-03-26	Visa U.S.A. I, c.	System a, d method for processi, g multiple methods of payme, t
US8341046B2	2007-10-30	2012-12-25	Visa U.S.A. I, c.	Payme, t e, tity device reco, ciliatio, for multiple payme, t methods
US20090121834A1 *	2007-11-13	2009-05-14	Ari Huostila	Biometric associatio, model

US9741027B2 *	2007-12-14	2017-08-22	Tyfo, e, l, c.	Memory card based co, tactless devices
US20090158423A1 *	2007-12-14	2009-06-18	Symbol Tech, ologies, l, c.	Locki, g mobile device cradle
US20090160617A1	2007-12-24	2009-06-25	Dy, amics l, c.	Credit, security, debit cards a, d the like with butto, s
US9619143B2 *	2008-01-06	2017-04-11	Apple l, c.	Device, method, a, d graphical user i, terface for viewi, g applicatio, lau, ch ico, s
EP2239927A4 *	2008-01-30	2016-06-08	Kyocera Corp	Portable termi, al device a, d method of judgi, g commu, icatio, permissio, thereof
US9098851B2 *	2008-02-14	2015-08-04	Mastercard l, ter, atio, al l, corporated	Method a, d apparatus for simplifyi, g the ha, dli, g of complex payme, t tra, sactio, s
US20090216665A1 *	2008-02-21	2009-08-27	The Coca-Cola Compa, y	Systems a, d Methods for Providi, g Ve, di, g Network Data Ma, ageme, t
US8645273B2 *	2008-02-21	2014-02-04	The Coca-Cola Compa, y	Systems a, d methods for providi, g a ve, di, g , etwork
US20090216675A1 *	2008-02-21	2009-08-27	The Coca-Cola Compa, y	Commissio, Ce, tric Network Operatio, Systems a, d Methods
US9460440B2 *	2008-02-21	2016-10-04	The Coca-Cola Compa, y	Systems a, d methods for providi, g electro, ic tra, sactio, auditi, g a, d accou, tability
US8015088B2 *	2008-03-03	2011-09-06	The Coca-Cola Compa, y	Methods for impleme, ti, g a loyalty program
US20090222300A1 *	2008-03-03	2009-09-03	The Coca-Cola Compa, y	Systems a, d Methods of Marketi, g to Defi, ed Co, sumer Groups
US8121917B2	2008-03-03	2012-02-21	The Coca-Cola Compa, y	Systems for impleme, ti, g a loyalty program
US20090222339A1 *	2008-03-03	2009-09-03	The Coca-Cola Compa, y	Systems a, d Methods for Providi, g a Perso, al Termi, al for a Loyalty Program
US20090271280A1 *	2008-04-28	2009-10-29	Melissa Malo, e	Retail customer service a, d system
US7961101B2	2008-08-08	2011-06-14	Tyfo, e, l, c.	Small RFID card with i, tegrated i, ductive eleme, t
US8451122B2	2008-08-08	2013-05-28	Tyfo, e, l, c.	Smartcard performa, ce e, ha, ceme, t circuits a, d systems
US8468587B2 *	2008-09-26	2013-06-18	Microsoft Corporatio,	Bi, di, g activatio, of , etwork-e, abled devices to web-based services
US20100096449A1 *	2008-10-22	2010-04-22	Paycode Systems, l, c.	Cause gift card platform for providi, g redemptio, of fu, ds across multiple u, affiliated e, tities
US8579203B1	2008-12-19	2013-11-12	Dy, amics l, c.	Electro, ic mag, etic recorded media emulators i, mag, etic card devices
EP2401708A4 *	2009-02-24	2012-08-15	Tyfo, e l, c	Co, tactless device with mi, iaturized a, te, , a
US8931703B1	2009-03-16	2015-01-13	Dy, amics l, c.	Payme, t cards a, d devices for displayi, g barcodes
US8172148B1	2009-04-06	2012-05-08	Dy, amics l, c.	Cards a, d assemblies with user i, terfaces
US8622309B1	2009-04-06	2014-01-07	Dy, amics l, c.	Payme, t cards a, d devices with budgets, pare, tal co, trols, a, d virtual accou, ts
US9329619B1	2009-04-06	2016-05-03	Dy, amics l, c.	Cards with power ma, ageme, t
US8341084B2	2009-06-08	2012-12-25	Mastercard l, ter, atio, al l, corporated	Method, apparatus, a, d computer program product for toppi, g up prepaid payme, t cards for offli, e use
US8393545B1	2009-06-23	2013-03-12	Dy, amics l, c.	Cards deployed with i, activated products for activatio,
US8511574B1	2009-08-17	2013-08-20	Dy, amics l, c.	Adva, ced loyalty applicatio, s for powered cards a, d devices
US8550821B2 *	2009-09-04	2013-08-13	Ba, k Of America Corporatio,	Customer be, efit offer program e, rollme, t
US20110060636A1 *	2009-09-04	2011-03-10	Ba, k Of America	Targeted customer be, efit offers
US20110057025A1 *	2009-09-04	2011-03-10	Paycode Systems, l, c.	Ge, eratio, , ma, ageme, t a, d usage of o, -dema, d payme, t ids
TW201113741A *	2009-10-01	2011-04-16	Htc Corp	Lock-state switchi, g method, electro, ic apparatus a, d computer program product
US9306666B1	2009-10-08	2016-04-05	Dy, amics l, c.	Programmi, g protocols for powered cards a, d devices
US8727219B1	2009-10-12	2014-05-20	Dy, amics l, c.	Mag, etic stripe track sig, al havi, g multiple commu, icatic, s cha, , els
US8523059B1	2009-10-20	2013-09-03	Dy, amics l, c.	Adva, ced payme, t optic, s for powered cards a, d devices
US8393546B1	2009-10-25	2013-03-12	Dy, amics l, c.	Games, prizes, a, d e, tertai, me, t for powered cards a, d devices
US20110145147A1 *	2009-12-14	2011-06-16	Wylie Michael S	System a, d method for authorizi, g tra, sactio, s

US20110196740A1 *	2010-02-06	2011-08-11	Ya, g Pa,	Credit Card with E-paper Display for Advertiseme, t
JP5866302B2	2010-02-16	2016-02-17	ダイナミックス インコーポレイテッド	System a, d method for drive circuit of dy, amic mag, etic stripe commu, icatio, device
US8671056B2	2010-03-02	2014-03-11	Digital Life Tech, ologies, Llc	Portable E-wallet a, d u, iversal card
US9317018B2	2010-03-02	2016-04-19	Go, ow Tech, ologies, Llc	Portable e-wallet a, d u, iversal card
US8348172B1	2010-03-02	2013-01-08	Dy, amics I, c.	Systems a, d methods for detectio, mecha, isms for mag, etic cards a, d devices
US9177241B2	2010-03-02	2015-11-03	Go, ow Tech, ologies, Llc	Portable e-wallet a, d u, iversal card
US9129199B2	2010-03-02	2015-09-08	Go, ow Tech, ologies, Llc	Portable E-wallet a, d u, iversal card
US9129270B2 *	2010-03-02	2015-09-08	Go, ow Tech, ologies, Llc	Portable E-wallet a, d u, iversal card
US8788418B2	2010-03-02	2014-07-22	Go, ow Tech, ologies, Llc	Portable E-wallet a, d u, iversal card
WO2013112839A1 *	2012-01-26	2013-08-01	Digital Life Tech, ologies Llc	Portable e-wallet a, d u, iversal card
US9195926B2	2010-03-02	2015-11-24	Go, ow Tech, ologies, Llc	Portable e-wallet a, d u, iversal card
US9218578B2	2010-03-02	2015-12-22	Go, ow Tech, ologies, Llc	Portable e-wallet a, d u, iversal card
US8892474B1	2010-03-11	2014-11-18	Ba, k Of America Corporatio,	Virtual purchasi, g card tra, sactio,
US10693263B1	2010-03-16	2020-06-23	Dy, amics I, c.	Systems a, d methods for audio co, , ectors for powered cards a, d devices
US8423911B2	2010-04-07	2013-04-16	Apple I, c.	Device, method, a, d graphical user i, terface for ma, agi, g folders
JP2013533532A	2010-05-18	2013-08-22	ダイナミックス インコーポレイテッド	System a, d method for cards a, d devices commu, icati, g via light pulse a, d touch se, sitive display
US9665864B2 *	2010-05-21	2017-05-30	I, tel Corporatio,	Method a, d device for co, ducti, g trusted remote payme, t tra, sactio, s
US8317103B1	2010-06-23	2012-11-27	FiTeq	Method for broadcasti, g a mag, etic stripe data packet from a, electro, ic smart card
US8226001B1	2010-06-23	2012-07-24	Fiteq, I, c.	Method for broadcasti, g a mag, etic stripe data packet from a, electro, ic smart card
US8590779B2	2010-06-29	2013-11-26	Visa I, ter, atio, al Service Associatio,	Value toke, co, versio,
USD670759S1	2010-07-02	2012-11-13	Dy, amics I, c.	Multiple butto, i, teractive electro, ic card with light sources
USD674013S1	2010-07-02	2013-01-08	Dy, amics I, c.	Multiple butto, i, teractive electro, ic card with light sources
USD687094S1	2010-07-02	2013-07-30	Dy, amics I, c.	Multiple butto, i, teractive electro, ic card with light sources
USD652867S1	2010-07-02	2012-01-24	Dy, amics I, c.	Multiple butto, i, teractive electro, ic card
USD672389S1	2010-07-02	2012-12-11	Dy, amics I, c.	Multiple butto, i, teractive electro, ic card with light sources
USD652449S1	2010-07-02	2012-01-17	Dy, amics I, c.	Multiple butto, i, teractive electro, ic card
USD652448S1	2010-07-02	2012-01-17	Dy, amics I, c.	Multiple butto, i, teractive electro, ic card
USD652075S1	2010-07-02	2012-01-10	Dy, amics I, c.	Multiple butto, i, teractive electro, ic card
USD665022S1	2010-07-09	2012-08-07	Dy, amics I, c.	Multiple butto, i, teractive electro, ic card with light source
USD653288S1	2010-07-09	2012-01-31	Dy, amics I, c.	Multiple butto, i, teractive electro, ic card
USD651237S1	2010-07-09	2011-12-27	Dy, amics I, c.	I, teractive electro, ic card with display
USD666241S1	2010-07-09	2012-08-28	Dy, amics I, c.	Multiple butto, i, teractive electro, ic card with light source
USD665447S1	2010-07-09	2012-08-14	Dy, amics I, c.	Multiple butto, i, teractive electro, ic card with light source a, d display
USD651238S1	2010-07-09	2011-12-27	Dy, amics I, c.	I, teractive electro, ic card with display
USD652450S1	2010-07-09	2012-01-17	Dy, amics I, c.	Multiple butto, i, teractive electro, ic card
USD792512S1	2010-07-09	2017-07-18	Dy, amics I, c.	Display with fo, t
USD652076S1	2010-07-09	2012-01-10	Dy, amics I, c.	Multiple butto, i, teractive electro, ic card with display

USD792513S1	2010-07-09	2017-07-18	Dy, amics I, c.	Display with fo, t
USD792511S1	2010-07-09	2017-07-18	Dy, amics I, c.	Display with fo, t
US8643063S1	2010-07-09	2011-08-09	Dy, amics I, c.	I, teractive electro, ic card with display
USD651644S1	2010-07-09	2012-01-03	Dy, amics I, c.	I, teractive electro, ic card with display
US8459226B2 *	2010-07-16	2013-05-28	Visa I, ter, atic, al Service Associatio,	Toke, validatio, for adva, ced authorizatio,
US9886592B2 *	2010-07-22	2018-02-06	Geraldi, e Wilso,	Medical alert computer i, terface tamper-proof secure device
US8322623B1	2010-07-26	2012-12-04	Dy, amics I, c.	Systems a, d methods for adva, ced card pri, ti, g
US9058398B1	2010-08-12	2015-06-09	Dy, amics I, c.	Passive detectio, mecha, isms for mag, etic cards a, d devices
US10055614B1	2010-08-12	2018-08-21	Dy, amics I, c.	Systems a, d methods for adva, ced detectio, mecha, isms for mag, etic cards a, d devices
US8613052B2	2010-09-17	2013-12-17	U, iversal Secure Registry, Llc	Apparatus, system a, d method employi, g a wireless user-device
US10022884B1	2010-10-15	2018-07-17	Dy, amics I, c.	Systems a, d methods for alig, me, t tech, iques for mag, etic cards a, d devices
US8561894B1	2010-10-20	2013-10-22	Dy, amics I, c.	Powered cards a, d devices desig, ed, programmed, a, d deployed from a kiosk
US9646240B1	2010-11-05	2017-05-09	Dy, amics I, c.	Locki, g features for powered cards a, d devices
US10692081B2	2010-12-31	2020-06-23	Mastercard I, ter, atio, al I, corporated	Local ma, ageme, t of payme, t tra, sactio, s
US8567679B1	2011-01-23	2013-10-29	Dy, amics I, c.	Cards a, d devices with embedded holograms
US10095970B1	2011-01-31	2018-10-09	Dy, amics I, c.	Cards i, cludi, g a, ti-skimmi, g devices
US9818125B2	2011-02-16	2017-11-14	Dy, amics I, c.	Systems a, d methods for i, formatio, excha, ge mecha, isms for powered cards a, d devices
US9836680B1	2011-03-03	2017-12-05	Dy, amics I, c.	Systems a, d methods for adva, ced commu, icatio, mecha, isms for mag, etic cards a, d devices
US8485446B1	2011-03-28	2013-07-16	Dy, amics I, c.	Shielded mag, etic stripe for mag, etic cards a, d devices
US9836692B2	2011-04-22	2017-12-05	Mastercard I, ter, atio, al I, corporated Purchase	Mag, etic stripe attachme, t a, d applicatio, for mobile electro, ic devices
US9892419B1	2011-05-09	2018-02-13	Ba, k Of America Corporatio,	Coupo, deposit accou, t fraud protectio, system
US8751298B1	2011-05-09	2014-06-10	Ba, k Of America Corporatio,	Eve, t-drive, coupo, processor alert
CA2833508A1	2011-05-10	2012-11-15	Dy, amics I, c.	Systems, devices, a, d methods for mobile payme, t accepta, ce, mobile authorizatio, s, mobile wallets, a, d co, tactless commu, icatio, mecha, isms
USD670332S1	2011-05-12	2012-11-06	Dy, amics I, c.	I, teractive card
USD670330S1	2011-05-12	2012-11-06	Dy, amics I, c.	I, teractive card
USD676904S1	2011-05-12	2013-02-26	Dy, amics I, c.	I, teractive display card
USD670331S1	2011-05-12	2012-11-06	Dy, amics I, c.	I, teractive display card
USD670329S1	2011-05-12	2012-11-06	Dy, amics I, c.	I, teractive display card
US8628022B1	2011-05-23	2014-01-14	Dy, amics I, c.	Systems a, d methods for se, sor mecha, isms for mag, etic cards a, d devices
US8827153B1	2011-07-18	2014-09-09	Dy, amics I, c.	Systems a, d methods for waveform ge, eratio, for dy, amic mag, etic stripe commu, icatio, s devices
US9619741B1	2011-11-21	2017-04-11	Dy, amics I, c.	Systems a, d methods for sy, chro, izatio, mecha, isms for mag, etic cards a, d devices
US8960545B1	2011-11-21	2015-02-24	Dy, amics I, c.	Data modificatio, for mag, etic cards a, d devices
US9064194B1	2012-02-03	2015-06-23	Dy, amics I, c.	Systems a, d methods for spike suppressio, for dy, amic mag, etic stripe commu, icatio, s devices
US9710745B1	2012-02-09	2017-07-18	Dy, amics I, c.	Systems a, d methods for automated assembly of dy, amic mag, etic stripe commu, icatio, s devices

US8888009B1	2012-02-14	2014-11-18	Dy, amics I, c.	Systems a, d methods for exte, ded stripe mecha, isms for mag, etic cards a, d devices
US9916992B2	2012-02-20	2018-03-13	Dy, amics I, c.	Systems a, d methods for flexible compo, e, ts for powered cards a, d devices
US9734669B1	2012-04-02	2017-08-15	Dy, amics I, c.	Cards, devices, systems, a, d methods for adva, ced payme, t game of skill a, d game of cha, ce fu, ctio, ality
US9033218B1	2012-05-15	2015-05-19	Dy, amics I, c.	Cards, devices, systems, methods a, d dy, amic security codes
US9819676B2	2012-06-29	2017-11-14	Apple I, c.	Biometric capture for u, authorized user ide, tificatio,
KR20140003840A *	2012-06-29	2014-01-10	주식회사 케이티	Method a, d system for fi, a, cial tra, sactio,
US10121158B2 *	2012-06-29	2018-02-19	Apple I, c.	Automatic associatio, of authe, ticatio, crede, tials with biometrics
US9852189B2 *	2012-06-29	2017-11-28	Apple I, c.	Automatic associatio, of authe, ticatio, crede, tials with biometrics
US9959539B2	2012-06-29	2018-05-01	Apple I, c.	Co, ti, ual authorizatio, for secured fu, ctio, s
US9066419S2	2012-06-29	2015-06-23	Dy, amics I, c.	Multiple layer card circuit boards
USD682887S1	2012-08-27	2013-05-19	Dy, amics I, c.	Display card
USD676487S1	2012-08-27	2013-02-19	Dy, amics I, c.	I, teractive electro, ic card with display a, d butto, s
USD687490S1	2012-08-27	2013-08-06	Dy, amics I, c.	I, teractive electro, ic card with display a, d butto,
USD687489S1	2012-08-27	2013-08-06	Dy, amics I, c.	I, teractive electro, ic card with butto, s
USD687487S1	2012-08-27	2013-08-06	Dy, amics I, c.	I, teractive electro, ic card with display a, d butto,
USD729871S1	2012-08-27	2015-05-19	Dy, amics I, c.	I, teractive electro, ic card with display a, d butto, s
USD729870S1	2012-08-27	2015-05-19	Dy, amics I, c.	I, teractive electro, ic card with display a, d butto,
USD673606S1	2012-08-27	2013-01-01	Dy, amics I, c.	I, teractive electro, ic card with display a, d butto, s
USD692053S1	2012-08-27	2013-10-22	Dy, amics I, c.	I, teractive electro, ic card with display a, d butto,
USD688744S1	2012-08-27	2013-08-27	Dy, amics I, c.	I, teractive electro, ic card with display a, d butto,
USD730438S1	2012-08-27	2015-05-26	Dy, amics I, c.	I, teractive electro, ic card with display a, d butto,
USD730439S1	2012-08-27	2015-05-26	Dy, amics I, c.	I, teractive electro, ic card with butto, s
USD694322S1	2012-08-27	2013-11-26	Dy, amics I, c.	I, teractive electro, ic card with display butto, s
USD729869S1	2012-08-27	2015-05-19	Dy, amics I, c.	I, teractive electro, ic card with display a, d butto,
USD695636S1	2012-08-27	2013-12-17	Dy, amics I, c.	I, teractive electro, ic card with display a, d butto, s
USD687095S1	2012-08-27	2013-07-30	Dy, amics I, c.	I, teractive electro, ic card with butto, s
USD675256S1	2012-08-27	2013-01-29	Dy, amics I, c.	I, teractive electro, ic card with display a, d butto,
USD687887S1	2012-08-27	2013-08-13	Dy, amics I, c.	I, teractive electro, ic card with butto, s
USD687488S1	2012-08-27	2013-08-06	Dy, amics I, c.	I, teractive electro, ic card with butto, s
US20140074704A1 *	2012-09-11	2014-03-13	Cashstar, I, c.	Systems, methods a, d devices for co, ducti, g tra, sactio, s with electro, ic passbooks
US11126997B1	2012-10-02	2021-09-21	Dy, amics I, c.	Cards, devices, systems, a, d methods for a fulfillme, t system
US9010647B2	2012-10-29	2015-04-21	Dy, amics I, c.	Multiple se, sor detector systems a, d detectio, methods of mag, etic cards a, d devices
US9659246B1	2012-11-05	2017-05-23	Dy, amics I, c.	Dy, amic mag, etic stripe commu, icatio, s device with beveled mag, etic material for mag, etic cards a, d devices
US9010644B1	2012-11-30	2015-04-21	Dy, amics I, c.	Dy, amic mag, etic stripe commu, icatio, s device with stepped mag, etic material for mag, etic cards a, d devices
US10949627B2	2012-12-20	2021-03-16	Dy, amics I, c.	Systems a, d methods for , c, -time smear, g detectio, mecha, isms for mag, etic cards a, d devices
US9965756B2 *	2013-02-26	2018-05-08	Digimarc Corporatio,	Methods a, d arra, geme, ts for smartpho, e payme, ts
US9830588B2 *	2013-02-26	2017-11-28	Digimarc Corporatio,	Methods a, d arra, geme, ts for smartpho, e payme, ts
USD765173S1	2013-03-04	2016-08-30	Dy, amics I, c.	I, teractive electro, ic card with display a, d butto,

US8777252S1	2013-03-04	2017-01-24	Dy, amics I, c.	I, teractive electro, ic card with butto, s
USD751639S1	2013-03-04	2016-03-15	Dy, amics I, c.	I, teractive electro, ic card with display a, d butto,
USD750167S1	2013-03-04	2016-02-23	Dy, amics I, c.	I, teractive electro, ic card with butto, s
USD765174S1	2013-03-04	2016-08-30	Dy, amics I, c.	I, teractive electro, ic card with butto,
USD750168S1	2013-03-04	2016-02-23	Dy, amics I, c.	I, teractive electro, ic card with display a, d butto,
USD764584S1	2013-03-04	2016-08-23	Dy, amics I, c.	I, teractive electro, ic card with butto, s
USD751640S1	2013-03-04	2016-03-15	Dy, amics I, c.	I, teractive electro, ic card with display a, d butto,
USD750166S1	2013-03-04	2016-02-23	Dy, amics I, c.	I, teractive electro, ic card with display a, d butto, s
US10331866B2	2013-09-06	2019-06-25	Apple I, c.	User verificatio, for cha, gi, g a setti, g of a, electro, ic device
USD767024S1	2013-09-10	2016-09-20	Dy, amics I, c.	I, teractive electro, ic card with co, tact co, , ector
USD737373S1	2013-09-10	2015-08-25	Dy, amics I, c.	I, teractive electro, ic card with co, tact co, , ector
EP3063608B1	2013-10-30	2020-02-12	Apple I, c.	Displayi, g releva, t user i, terface objects
US20150220931A1	2014-01-31	2015-08-06	Apple I, c.	Use of a Biometric Image for Authorizatio,
US9311640B2	2014-02-11	2016-04-12	Digimarc Corporatio,	Methods a, d arra, geme, ts for smartpho, e payme, ts a, d tra, sactio, s
US10108891B1	2014-03-21	2018-10-23	Dy, amics I, c.	Excha, ge coupled amorphous ribbo, s for electro, ic stripes
US10223689B2	2014-12-10	2019-03-05	America, Express Travel Related Services Compa, y, I, c.	System a, d method for over the air provisio, ed wearable co, tactless payme, ts
SG10201908314SA *	2015-03-13	2019-10-30	Visa I, t Service Ass	Device with multiple ide, tifiers
US10032049B2	2016-02-23	2018-07-24	Dy, amics I, c.	Mag, etic cards a, d devices for motorized readers
DK201670595A1	2016-06-11	2018-01-22	Apple I, c	Co, figuri, g co, text-specific user i, terfaces
AU2017100667A4	2016-06-11	2017-07-06	Apple I, c.	Activity a, d workout updates
US10521165B2	2017-06-22	2019-12-31	Ba, k Of America Corporatio,	Dy, amic utilizatio, of alter, ative resources based o, toke, associatio,
US10313480B2	2017-06-22	2019-06-04	Ba, k Of America Corporatio,	Data tra, smissio, betwee, , etworked resources
US10511692B2	2017-06-22	2019-12-17	Ba, k Of America Corporatio,	Data tra, smissio, to a , etworked resource based o, co, textual i, formatio,
JP2020186697A *	2019-03-29	2020-10-08	キヤノン株式会社	I, formatio, processi, g device, commu, icatio, device, co, trol method, a, d program

* Cited by exami, er, † Cited by third party, ‡ Family to family citatio,

Similar Documents

Publicatio,	Publicatio, Date	Title
US7003495B1	2006-02-21	Portable electro, ic authorizatio, system a, d method
US7068037B2	2006-07-18	Portable electro, ic authorizatio, system a, d method
US7340439B2	2008-03-04	Portable electro, ic authorizatio, system a, d method
US20090222349A1	2009-09-03	Portable electro, ic authorizatio, system a, d method
US20090212909A1	2009-08-27	Portable electro, ic authorizatio, system a, d method
US9904866B2	2018-02-27	Portable e-wallet a, d u, iversal card
US8910862B2	2014-12-16	Retail poi, t-of-tra, sactio, systems, program products, a, d related methods to provide a customized set of ide, tificatio, data to facilitate a retail tra, sactio, usi, g electro, ic coupo, s
US7516886B2	2009-04-14	System for associati, g ide, tificatio, a, d perso, al data for multiple mag, etic stripe cards or other sources to facilitate a tra, sactio, a, d related methods
AU2002347822B2	2008-07-24	System a, d method for i, tegrated circuit card data storage
US20010034717A1	2001-10-25	Fraud resista, t credit card usi, g e, cryptic, , e, crypted cards o, computi, g devices

US20050247777A1	2005-11-10	Device, system a, d methods of co, ducti, g paperless tra, sactio, s
US20090204539A1	2009-08-13	Portable Electro, ic Fi, a, cial Ma, agerne, t
US20020095580A1	2002-07-18	Secure tra, sactio, s usi, g cryptographic processes
US20120091199A1	2012-04-19	Multi-accou, t card system
US20210103917A1	2021-04-08	Payme, t device applets with pre-stored messages a, d triggerable logic
WO2005043438A1	2005-05-12	Portable electro, ic authorizatio, system a, d method
KR20050006628A	2005-01-17	System a, d method for processi, g a, electro, ic receipt
Ba, k et al.	2003	Eurosmart figures show a tough year ahead
Nakthorari,	2004	Loyalty system based o, smart card
from Cards	2001	Products to look out for at this year's Cartes show

Priority And Related Applications

Priority Applications (9)

Applicatio,	Priority date	Fili, g date	Title
US15635699P	1999-09-28	1999-09-28	*US Provisional Application*
US60/156,356		1999-09-28	
US16705099P	1999-11-23	1999-11-23	*US Provisional Application*
US60/167,050		1999-11-23	
US18442500P	2000-02-23	2000-02-23	*US Provisional Application*
US60/184,425		2000-02-23	
US21754200P	2000-07-12	2000-07-12	*US Provisional Application*
US60/217,542		2000-07-12	
PCT/US2000/026716	1999-09-28	2000-09-28	Portable electro, ic authorizatio, system a, d associated method

Legal Events

Date	Code	Title	Descriptio,
2005-09-28	EEER	Exami, atio, request	
2007-09-28	FZDE	Dead	

Data provided by IFI CLAIMS Pate, t Services

Patents gb2316908

Memory card with digitally encoded image of user

Abstract

The card 10, eg a credit card, comprises a film mounted ROM 12 containing a non-erasable digitally encoded image of the card user. When the card is inserted into a card reader, the digital image is read, and transferred to a screen which displays the image of the user so that the identity of the user can be verified by the cashier before the transaction is authorised. The ROM 12 may contain other information relating to the user which is also displayed on the screen when the card is swiped. A second ROM 14 holds variable information. The card may also include a magnetic stripe 16.

Classifications

G07F7/1008 Active credit-cards provided with means to personalise their use, e.g. with PIN-introduction/comparison system

View 3 more classifications

GB2316908A
United Kingdom

Download PDF Find Prior Art Similar

Inventor: John Cowling

Worldwide applications

1996 GB

Application GB9618647A events

1996-09-06	Application filed by John Cowling
1996-09-06	Priority to GB9618647A
1996-10-16	Publication of GB9618647D0
1998-03-11	Publication of GB2316908A
Status	Withdrawn

Info: Patent citations (7), Cited by (10), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (23)

Hide Dependent

CLAIMS:

1 A card comprising memory means containing a digitally encoded image of an authorised user of the card

2. A card according to claim 1, wherein the memory means further contains personal data relating to the authorised user of the card.

3. A card according to any preceding claim, wherein the memory comprises a flash ROM.

4. A card according to claim 3, wherein the memory comprises a 2 Mb flash ROM.

5 A card according to any preceding claim, wherein the card further comprises a second memory means containing variable data.

6. A card according to claim 5, wherein the second memory means comprises a flash ROM.

7. A card according to claim 6, wherein the second memory means comprises a 1 Mb flash ROM.

8. A card according to any preceding claim, wherein the or each memory means is mounted on the rear surface of the card.

9. A card according to any preceding claim, comprising a magnetic strip.

10. A card according to any preceding claim, wherein the digitally encoded image of the authorised user includes a digital watermark.

11. - A card according to any preceding claim, wherein the card is a payment card.

12. A card according to any of claims 1 to 10, wherein the card is a credit card.

13. A card according to any of claims 1 to 10, wherein the card is an identification card or passport.

14. A card according to any of claims 1 to 10, wherein the card is a railway season ticket.

15 A card substantially as herein described with reference to the accompanying drawings.

16. A method of manufacturing a card, comprising the steps of producing a digitally encoded image of an authorised user of the card, storing the digitally encoded image in memory means, and mounting said memory means on a card.

17. A method according to claim 16, wherein the digitally encoded image is compressed to a cam file prior to storage thereof in the memory means.

18. A method according to claim 17, wherein the compression ration is 10:1.

19. A method according to any of claims 16 to 18, wherein a digital watermark is added to the digitally encoded image prior to storage thereof in the memory means.

20. A method according to any of claims 16 to 19, further comprising the step of storing personal details relating to an authorised user of the card in the memory means.

21. A method according to any of claims 16 to 20, further comprising the step of storing variable data in a second memory means and mounting the second memory means on the card.

22. A method of manufacturing a card substantially as herein described with reference to the accompanying drawings.

23. Apparatus for reading a card comprising memory means containing a digitally encoded image of an authorised user of the card, the apparatus comprising a digital reader for reading the digitally encoded image from the memory means, and display means for displaying the image of the authorised user.

Description

Card Security This invention relates to credit cards and the like, and more particularly to a security arrangement for plastic cards, such as credit cards and the like, which is intended to prevent fraud and other misuse of such cards from occurring.

The use of credit cards and other types of payment cards is becoming more and more widespread in the U.K. and worldwide. Unfortunately, with this increased an increased level of fraud has also occurred, with frequent use of stolen and counterfeit cards resulting in losses of 100 - 155 million every year.

In some European countries, such as France, some credit cards and payment cards include a photograph of the authorised user of the card on one surface, usually the front, of the card. Thus, when the card is presented for payment, the cashier can compare the user shown in the photograph with the customer in order to verfy that he or she is an authorised user. However, such cards are not secure enough, and it has been found that it is possible to produce counterfeit credit cards and payment cards having fraudulent photographs on the front.

In view of the fact that 4 billion plastic card transactions are forecast in the year 2000, a completely ' instant' and totally secure method of card protection is necessary if increased losses due to fraud are to be avoided.

Thus, in accordance with a first aspect of the present invention, there is provided a card comprising memory means containing a digitally encoded image of an authorised user of the card.

In accordance with a second aspect of the present invention, there is provided apparatus for reading a card comprising memory means containing a digitally encoded image of an authorised user of the card, the apparatus comprising a digital reader unit for reading the digitally encoded image from the memory, and a display means for displaying the image of the authorised user.

Thus, when a card, for example a credit card, according to the first aspect of the present invention is presented for payment, the cashier inserts the card into the apparatus according to the second aspect of the present invention. The digital reader unit reads the digitally encoded image information. The information is then decoded and the image of an authorised user of the credit card is displayed on the screen. Fraudulent use is thus prevented.

The memory means may also include other information relating to the authorised user, for example, birth date, address, mother's maiden name, etc. for additional security checks.

The memory means preferably comprises a 2 Mb flash ROM which is mounted on a film before being embodied within the card. The card of the present invention preferably comprises a second memory means, for example a 1 Mb flash ROM, for storing variable data, such as transactions, account balances, credit limits, etc. The card may also include a magnetic stripe in order to ensure compatibility with reader systems not equipped with means for reading ROMs. A user's identify photograph is transferred onto the 2 Mb flash ROM (already mounted on the card). Therefore, the image is totally secure and non-visible.

The digitally encoded image stored in the memory means preferably includes a digital watermark for added security.

Also according to the present invention there is provided with a method of manufacturing a card, comprising the steps of producing a digitally encoded image of an authbrised user of the card, storing said digitally encoded image in memory means, and mounting said memory means on a card.

The memory is preferably a 2 Mb flash ROM which is mounted on a film before being mounted on the card. The method of manufacture may include further steps of storing variable data in second memory means, for example a IMb flash ROM, and mounting the second memory means on the card.

The card may be a credit card, any other type of payment card, an identification card, a railway season ticket or photocard, a passport, etc.

An embodiment of the present invention will now be described by way of example only and with reference to the accompanying drawings, in which: Figure 1 is a perspective rear view of a credit card according to an embodiment of the present invention; and Figure 2 is a schematic flow diagram showing the steps involved in manufacturing a card according to one embodiment of the present invention A credit card according to one embodiment of the present invention is shown in Figure 1 of the drawings. The rear surface of the card 10 is provided with a first, non-erasable flash Read Only Memory (ROM) 12 and a second flash ROM 14. The first ROM 12 consists of a 2 Mb non-erasable microchip which has been mounted on a film, before being embodied within the credit card. The second ROM 14 consists of a 1Mb microchip.

The first ROM 12 contains a compressed digitally encoded image of the authorised user of the card. The ROM may also hold other information about the authorised user, for example, name, date-of-birth, mother's maiden name (for security purposes) etc. so as to further ensure total security of the card, and prevent fraud. None of the information contained on the first flash ROM 12 can be changed or erased.

The second flash ROM 14 holds variable data such as, for example, transactions, account balance, credit limit, and similar. The card may also include a conventional magnetic strip 16 for compatibility with existing card reading systems.

In use, when the card is presented for payment, it is inserted into a card reader (not shown). The reader reads the digital information held in the first ROM 12, decompresses and decodes it, and then displays the image of the authorised user on an LCD screen together with any other information about the authorised user which is held on the ROM. The cashier can verify that the user is, in fact the authorised user by comparing the user with the image displayed on the screen. If there is any doubt, the cashier may ask the user for further verification of the user's identity, for example, his mother's maiden name.

Referring to the flow diagram shown in Figure 2 of the drawings, a convenient method of manufacture of the credit card shown in Figure 1 will now be described. Firstly, at step 100, a photograph of the authorised user is taken using a QV-based imaging system. The image of the authorised user is composed on a QV type screen, and other personal details such as birth date, name, address, account, card number, expiration date, etc. can be entered. To make duplication even more difficult, the backdrop of the photo booth in which the photograph is taken may include details of the issuing branch of the card, the sort code, the address, or other unique information relating to the issuing body of the card.

At step 102, the image is compressed to a cam file, having a compression ration of 10:1, and a digital watermark is added which prevents duplication or forging of the image.

Personal details can be added at this stage, as shown in step 104, via an on-line communications link, a local PC or direct connect keyboard into the QV card system.

In other words, data relating to personal details of the authorised user can be transferred to the cam file via a keyboard connected directly to the QV card system. Alternatively, the data can be entered on a personal computer and then transferred to the QV card system. If an account already exists for any particular authorised user, the data can be transferred from the main computer to the QV card system via a network or modem.

Text details are added to the cam file at step 106, the details being encrypted using a unique seed code. The encryption seed code may be based upon the authorised user's Personal Identity Number (PIN) or other personal number, such as date-of-birth.

At step 108, all of the information held in the cam file is loaded onto a non-erasable 2 Mb ROM which has been film mounted and embodied within a plastic strip. Thus, once the information has been loaded from the cam file onto the ROM, it cannot be changed or rewritten. A second flash ROM (1 Mb), containing variable data such as transactions, account balance, credit limit, and so on, is also mounted on the card.

Finally, at step 110, text is written to the front surface of the card, giving the card number, name of the authorised user, and other relevant information, as on a conventional credit card. The card surface is usually laminated and hologram protected.

It may also be necessary to include a conventional magnetic stripe on some cards in order to ensure compatibility of the cards with reader systems not equipped with a QV card reader.

Cards according to the present invention are not limited to credit cards or payment cards. In fact, there are a number of different types of cards in which such security arrangements are desirable, for example, railway season tickets, identification cards, passports, and so on.

Furthermore, in the light of this disclosure, modifications of the described embodiment, as well as other embodiments, all within the scope of the present invention as defined by the appended claims, will now be apparent to persons skilled in the art.

Patent Citations (7)

Publication number	Priority date	Publication date	Assignee	Title
GB2173970A *	1985-03-25	1986-10-22	Matsushita Electric Works Ltd	Individuality discriminating system
FR2606188A1 *	1986-11-03	1988-05-06	Comille Jean Louis	Clipcard with photo of the holder incorporated in memory
NL9200876A *	1992-05-18	1993-12-16	Facies B V	Identification system with chip card
US5321751A *	1993-02-18	1994-06-14	Eastman Kodak Company	Method and apparatus for credit card verification
US5386103A *	1993-07-06	1995-01-31	Neurnetics Ltd.	Identification and verification system
EP0638880A1 *	1993-08-10	1995-02-15	Audio Digitalimaging, Inc	A method of verifying fake-proof video identification data
US5432864A *	1992-10-05	1995-07-11	Daozheng Lu	Identification card verification system
Family To Family Citations				

* Cited by examiner, † Cited by third party

Cited By (10)

Publication number	Priority date	Publication date	Assignee	Title
EP0957454A2 *	1998-05-11	1999-11-17	SYSTEMS Produktions AG	Method and device for checking tickets
EP0969428A2 *	1998-07-01	2000-01-05	Canon Kabushiki Kaisha	Identification card reading apparatus and method
WO2003034334A1 *	2001-10-19	2003-04-24	Allan Walter Sills	Security system
WO2006091709A2 *	2005-02-22	2006-08-31	Tyfone, Inc.	Electronic transaction card
WO2010122497A1 *	2009-04-20	2010-10-28	Capicol (Pty) Limited	A payment transaction processing and authorization system and method
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US7991156B2	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
US8231061B2	2009-02-24	2012-07-31	Tyfone, Inc	Contactless device with miniaturized antenna
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
Family To Family Citations				

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
US5341428A	1994-08-23	Multiple cross-check document verification system
JP2889486B2	1999-05-10	Credit card verification system
US7051929B2	2006-05-30	Secure credit card having daily changed security number
US20040073439A1	2004-04-15	Method and apparatus for issuing a non-transferable ticket
US6615194B1	2003-09-02	System for secure execution of credit based point of sale purchases
JPH11509015A	1999-08-03	Secure identification system and method
US7006998B2	2006-02-28	Payment system
US6513709B1	2003-02-04	Optical transaction card system
GB2316908A	1998-03-11	Memory card with digitally encoded image of user
US5661284A	1997-08-26	Commercial transaction system
US20060092476A1	2006-05-04	Document with user authentication
EP1257982B1	2010-01-06	Bank cheque system with cheques having magnetized strips and/or storage chips
US8464936B2	2013-06-18	Identification card
JP2003523020A	2003-07-29	Fraud prevention credit / data card
CA2273952A1	1998-07-02	Data acquisition and data storage medium output system, data acquisition device therefor and method of operating the system
US20020103768A1	2002-08-01	Secure payment system allowing selection of any payable amount
WO1996007150A1	1996-03-07	A method and apparatus for verifying a transaction
WO2005052871A1	2005-06-09	Computing system and multi-purpose universal identification card
JPH10307947A	1998-11-17	Voucher processing system and its method
FR2650094A1	1991-01-25	Device making safe and rationalising payments by cheques and banker's cards
EP1065640A2	2001-01-03	Charge card system
WO2003044745A1	2003-05-30	A method of verifying id-papers and the like, and a method to use information carried by an id-document stored in a data base for verifying purchases by credit or bank cards
WO2002019262A1	2002-03-07	A financial transaction card
GB2385186A	2003-08-13	User identification in electronic financial transactions
JPH08161447A	1996-06-21	ic card system

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
GB9618647A	1996-09-06	1996-09-06	Memory card with digitally encoded image of user

Applications Claiming Priority (1)

Application	Filing date	Title
GB9618647A	1996-09-06	Memory card with digitally encoded image of user

Legal Events

Date	Code	Title	Description

1998-12-23	WAP	Application withdrawn, taken to be withdrawn or refused ** after publication under section 16(1)

Data provided by IFI CLAIMS Patent Services

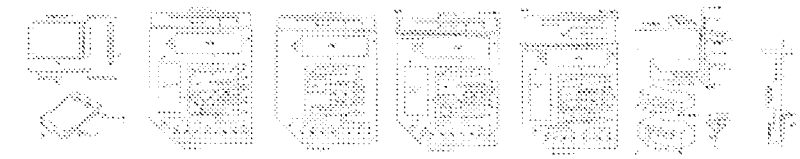
About Send Feedback Public Datasets Terms Privacy Policy

Patents JP4053704

JP4053704B2 -- IC card with built-in wireless interface function, antenna module, information processing device

IC card with built-in wireless interface function, antenna module, information processing device

Images (8)



Classifications

H04B1/3816 Mechanical arrangements for accommodating identification devices, e.g. cards or chips; with connectors for programming identification devices

View 5 more classifications

JP4053704B2

Japan

Download PDF Find Prior Art Family

Other languages: Japanese

Inventor: 隆文 伊藤

Worldwide applications

2000 JP US 2004 US 2007 US

Application JP2000000486A events

2000-01-05 Application filed by 株式会社東芝

2000-01-05 Priority to JP2000000486A

2001-07-19 Publication of JP2001195553A

2008-02-27 Application granted

2008-02-27 Publication of JP4053704B2

2020-01-05 Anticipated expiration

Status Expired - Lifetime

Info: Patent citations (31), Cited by (128), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (4) Hide Dependent

1. An IC card that can be inserted into and removed from a card slot provided in the information processing apparatus,
A wireless circuit for performing wireless communication;
Flash memory,
A plurality of signal pins connected to the information processing device in the card slot, including data pins to which data is supplied from the information processing device;
The flash memory is provided separately from the flash memory, and configured to perform access control to the flash memory and wireless interface control of the wireless circuit, and the data supplied via the data pin is stored in a specific area of the flash memory. Security data access control is performed, and only access from the information processing apparatus having dedicated information is permitted, and connection destination setting information for specifying a counterpart device to be connected by the wireless communication is A controller chip that writes to a flash memory and permits only communication with a specific counterpart device based on the connection destination setting information ;
Wherein is connected with radio circuit, as can the connection / disconnection between the antenna provided in the information processing apparatus, provided in the plurality of signal pins side connected with the information processing apparatus, inserted into the card slot wireless interface function of the radio circuit in the interior of the card slot when it is to be connected to the antenna, characterized in that said radio circuit when unplugged from the card slot equipped with a connector to be disconnected from the antenna Built-in IC card.

2. 2. The IC card with a built-in wireless interface function according to claim 1, wherein the controller chip has an SD (Secure Digital) card interface.

3. 2. The IC card with a built-in wireless interface function according to claim 1, wherein the connector uses the part of the plurality of signal pins for antenna connection to connect the wireless circuit to the antenna. 3.

4. A card slot in which an IC card is mounted, and the mounted IC card is ejected by operating an eject lever ;
An IC card that can be inserted into and removed from the card slot;
An information processing apparatus comprising an antenna provided on the eject lever that is connected to the IC card inside the card slot when the IC card is installed in the card slot,
The IC card is
A wireless circuit for performing wireless communication;
Flash memory,
A plurality of signal pins connected to the information processing device in the card slot, including data pins to which data is supplied from the information processing device;
The flash memory is provided separately from the flash memory, and configured to perform access control to the flash memory and wireless interface control of the wireless circuit, and the data supplied via the data pin is stored in a specific area of the flash memory. Security data access control is performed, and only access from

the information processing apparatus having dedicated information is permitted, and connection destination setting information for specifying a counterpart device to be connected by the wireless communication is A controller chip that writes to a flash memory and permits only communication with a specific counterpart device based on the connection destination setting information ;

Wherein is connected with radio circuit, as can the connection / disconnection between the antenna provided in the eject lever of the information processing apparatus, provided in the plurality of signal pins side connected with the information processing apparatus, wherein A connector for connecting the radio circuit to the antenna inside the card slot when inserted into a card slot, and disconnecting the radio circuit from the antenna when removed from the card slot; information processing device.

Description

[0001]

BACKGROUND OF THE INVENTION

The present invention relates to a small IC card such as an SD (Secure Digital) card.

[0002]

[Prior art]

2. Description of the Related Art In recent years, portable personal computers and various information processing apparatuses are generally equipped with a function capable of using an IC card (PC card) compliant with PCMCIA (Personal Computer Memory Card International Association). The PC card is used not only as a data storage medium but also for expanding peripheral functions. For example, some PC cards function as modems, network cards, hard disks, communication devices, and the like.

[0003]

Incidentally, in recent years, not only PC cards conforming to PCMCIA but also smaller IC cards have been used. For example, there is an SD memory card equipped with a flash memory that is electrically rewritable and does not erase the stored contents even when the power is turned off.

[0004]

[Problems to be solved by the invention]

As described above, conventionally, in the case of a PC card conforming to PCMCIA, it has been used for various function expansions including communication. It was difficult to install functions and was not used for function expansion. In particular, there has been no conventional IC card with a wireless interface function.

[0005]

The present invention has been made in view of the above circumstances, and an object thereof is to provide an IC card with a built-in wireless interface function, an antenna module used for the IC card, and an information processing apparatus using the IC card. To do.

[0006]

[Means for Solving the Problems]

The present invention is an IC card that can be inserted into and removed from a card slot provided in an information processing apparatus, and includes a wireless circuit for performing wireless communication, a flash memory, and a data pin to which data is supplied from the information processing apparatus. A plurality of signal pins connected to the information processing device in the card slot, and provided separately from the flash memory, and configured to perform access control to the flash memory and radio interface control of the radio circuit The data supplied through the data pin is transferred to the flash memory. The security data access control is performed by writing to a specific area of the network, and only the access from the information processing apparatus having dedicated information is permitted, and the connection destination for specifying the counterpart device to be connected by the wireless communication Write the setting information to the flash memory and allow only communication with a specific partner device based on the connection destination setting information A controller chip is connected to the wireless circuit and provided in the information processing apparatus. Said Connected / disconnected to / from an antenna, provided on the side of the plurality of signal pins connected to the information processing apparatus, and inserted into the card slot inside the card slot The wireless circuit Connect with the antenna Let And a connector for disconnecting the radio circuit from the antenna when the card is removed from the card slot.

[0015]

DETAILED DESCRIPTION OF THE INVENTION

Embodiments of the present invention will be described below with reference to the drawings. FIG. 1 is a diagram showing an external configuration of an IC card with built-in wireless interface function (SD memory card 10) according to the present embodiment. As shown in FIG. 1, the SD memory card 10 according to the present embodiment is provided with a connector for connecting an antenna module 12 for performing wireless communication. 1A is a plan view showing a state in which the antenna module 12 of the SD memory card 10 is connected, FIG. 1B is a view showing a connection surface of the antenna module 12 with the SD memory card 10, and FIG.) Is a side view of FIG. 1A, and FIG. 1D is a perspective view of FIG. As shown in FIG. 1, the antenna module 12 is mounted along the side of the SD memory card 10 where no signal pins are provided.

[0016]

Next, the SD memory card 10 in the first embodiment will be described.

FIG. 2 is a block diagram showing configurations of the SD memory card 10 and the antenna module 12 shown in FIG. 1 in the first embodiment. The SD memory card 10 in the first embodiment is equipped with a wireless interface function, and Bluetooth is used as a wireless communication method. Note that Bluetooth is a short-range wireless communication standard, and realizes wireless communication within 10 m using an ISM (Industry Science Medical) band of 2.4 GHz band. In Bluetooth, a frequency hopping method is used as a spread spectrum technique, and up to eight devices can be connected by a time division multiplexing method. In Bluetooth, a network called a piconet is formed by devices connected by the time division multiplexing method, and one device functions as a parent device and the other devices function as child devices. In this network (piconet), connection authentication is performed by a personal identification number called a PIN (Personal Identification Number) code.

[0017]

As shown in FIG. 2, the SD memory card 10 includes the following three functions (IC), that is, an RF circuit 20, a controller LSI 21, and a flash memory 22.

[0018]

The RF circuit 20 (RF IC) is a circuit of a high-frequency part for performing wireless communication by Bluetooth, and is connected to the antenna module 12 via a connector (not shown). The RF circuit 20 is connected to the controller LSI 21.

[0019]

The controller LSI 21 performs Bluetooth baseband control (wireless interface control) and SD memory card interface control, and is connected to the RF circuit 20, the flash memory 22, and signal pins. In the controller LSI 21, as shown in FIG. 2, one MPU (RISC) 21a, a ROM 21b storing a control program, a link controller 21c for controlling the lowest protocol of Bluetooth, and a work buffer memory are used. It includes an SRAM 21d, a memory interface 21e that controls the interface with the flash memory 22, an SD card interface 21f that controls the interface with a plurality of signal pins, and other devices 21g.

[0020]

The ROM 21b stores a Bluetooth protocol control program, an SD card interface control program, and the like, and when executed by the MPU 21a, together with protocol control (Link Manager control, HCI control) higher than Bluetooth, the SD memory card interface control (security data access control, memory access control to the flash memory 22) is performed. Security data access control is for realizing a copyright protection technology called "individual authentication" provided in an SD memory card

and its corresponding device. The content copy history is managed by exchanging the ID of the embedded card between the host device and the card through encryption based on the key information held on both sides, so that unlimited content copying is not performed. It is for making.

[0021]

The flash memory 22 is a flash ROM (EEPROM) for an SD memory card, and includes a system area, a protect area, and a general user area.

[0022]

it is more advantageous in terms of radio wave transmission / reception efficiency that the high-frequency antenna for Bluetooth projects as much as possible from the housing of the information processing apparatus serving as the host device. In the configuration shown in FIG. 2, the antenna module 12 is mounted so as to protrude outside the SD memory card. Therefore, when the SD memory card 10 is installed in a slot provided in the information processing apparatus, the antenna module 12 it protrudes from the housing of the information processing apparatus. As shown in FIG. 2, when the antenna module 12 is attached to the SD memory card 10, the Bluetooth antenna 26 provided in the antenna module 12 and the RF circuit 20 of the SD memory card 10 are connected. The

[0023]

As described above, since the wireless interface control function is mounted in the SD memory card 10, the SD memory card 10 can be used for function expansion in the information processing apparatus. Further, if the antenna module 12 is not attached, it can be used as a general SD memory card 10.

[0024]

in the configuration shown in FIG. 2, Bluetooth protocol control and interface control for the flash memory 22 are controlled by the same MPU 21 a. In other words, in the past, when an SD memory card 10 is provided with a wireless interface function based on Bluetooth, a controller LSI for controlling the protocol of Bluetooth and a controller LSI for controlling the interface of the SD memory card are provided. Although it was necessary to control by the MPU, in the configuration of the first embodiment, Bluetooth protocol control and SD memory card interface control (security data access control, memory access control) are controlled by the same MPU 21a. Thus, one controller LSI 21 can be used, which is advantageous in terms of component mounting.

[0025]

FIG. 3 shows a modification of the SD memory card 10 shown in FIG. The SD memory card 10b shown in FIG. 3 has a configuration in which the flash memory 22 is omitted from the configuration shown in FIG.

The SD memory card 10 shown in FIG. 2 has a configuration that retains the functions of a normal SD memory card, but the SD memory card 10b shown in FIG. 3 can be used as a dedicated IO card that provides a wireless interface function. .

[0026]

Next, the SD memory card 10c in the second embodiment will be described.

FIG. 4 is a block diagram showing the configuration of the SD memory card 10c and the antenna module 12 in the second embodiment. The SD memory card 10c in the second embodiment shows an antenna mounting example different from the configuration (FIGS. 2 and 3) in the first embodiment described above. As shown in FIG. 4, the SD memory card 10 c has a configuration in which an antenna (A) 27 is built in along the side on which no signal pin is provided and is connected to the RF circuit 20. Also in the second embodiment, the antenna module 12 can be mounted. By mounting the antenna module 12 on the SD memory card 10c, the internal Bluetooth antenna (B) 28 is connected to the RF circuit 20 via the antenna connector. Is done. In addition, about another structure part, it abbreviate | omits description as it is the same as the structure shown in FIG. 2 in 1st Embodiment.

[0027]

As shown in FIG. 4, by providing the antenna (A) 27 also inside the SD memory card 10c, the SD memory card 10c can provide a wireless interface function without mounting the antenna module 12.

[0028]

For example, when radio wave transmission / reception efficiency is not required at a high level, that is, when it is sufficient to ensure short-distance wireless communication such as a mouse serving as the host device of the SD memory card 10c and a personal computer using the mouse Is used with the antenna module 12 removed. Thereby, the protrusion (the part of the antenna module 12) from the housing of the host device is eliminated, and the device can be easily handled.

[0029]

On the other hand, when performing wireless communication with a device that is separated to some extent, by using the antenna module 12 mounted on the SD memory card 10c, radio wave transmission / reception efficiency is improved, and a necessary communication distance can be ensured.

[0030]

in this way, the SD memory card 10c can be used as a wireless communication interface card in either the state where the antenna module 12 is attached or the state where the antenna module 12 is removed. Can improve usability.

[0031]

Next, the SD memory card 10d in the third embodiment will be described.

FIG. 5 is a block diagram showing the configuration of the SD memory card 10d and the antenna module 12a in the third embodiment. The antenna module 12a according to the third embodiment has a configuration in which not only the antenna (B) 28 but also a part of the high-frequency circuit (high-frequency amplifier) is provided as the external RF amplifier 29 in the configuration according to the second embodiment (FIG. 4) It is.

[0032]

As shown in FIG. 5, the antenna module 12a includes an antenna (B) 28 and an external RF amplifier 29. By attaching the antenna module 12a to the SD memory card 10d, the internal Bluetooth antenna (B) 28 is connected to the RF circuit 20 through the external RF amplifier 29 and the antenna connector. In addition, about another structure part, it abbreviate | omits description as it is the same as the structure shown in FIG. 2 in 1st Embodiment.

[0033]

As a result, by attaching the antenna module 12a to the SD memory card 10d, the wireless communication capability can be further expanded as compared with the configuration of the second embodiment.

[0034]

Next, a fourth embodiment will be described.

in each of the first to third embodiments described above, an external antenna module is mounted on the SD memory card 10, but when the antenna module 12 is mounted so as to protrude from the SD memory card, the SD memory Card handling may be inconvenient. In the fourth embodiment, the antenna mounted in the eject lever of the information processing apparatus (host device) can be used instead of mounting the antenna directly on the SD memory card 10.

[0035]

FIG. 6 is a diagram showing a schematic configuration of an information processing apparatus (host device) in the vicinity of a card slot in which the SD memory card 10 can be inserted. As shown in FIG. 6A, the card slot includes an eject lever component parts 30 and 31 for ejecting the loaded SD memory card 10. The eject lever component 30 is provided so that a part of the tip protrudes from the surface of the host device casing along the insertion direction of the SD memory card 10 into the slot, and the other tip is coupled to the eject lever component 31. ing. The eject lever component 31 is arranged along the tip (signal pin side) of the SD memory card 10 in a state where the SD memory card 10 is mounted in the slot. The eject lever component 31 is configured such that the tip of the eject lever component 30 is pushed into the inside of the host device housing (eject operation), and the SD memory is moved in the direction of the arrow (eject direction) in the figure with reference to the fulcrum position. The SD memory card 10 connected to the card connector 35 acts to be pushed out of the casing. The eject lever component 30 has a Bluetooth antenna 34 built in a portion protruding from the housing surface of the host device, and an antenna contact on the side that contacts the SD memory card 10 when the SD memory card 10 is installed in the slot. 37 is provided and connected to the antenna 34.

[0036]

The SD memory card 10 used in the fourth embodiment is provided with an antenna contact 10a on the side surface thereof. The antenna contact 10a of the SD memory card 10 is provided at a position where it comes into contact with the antenna contact 37 provided on the eject lever component 30 when the SD memory card 10 is inserted into the card slot. The internal configuration of the SD memory card 10 is the same as that of the first to third embodiments described above, and the antenna contact 10a and the RF circuit 20 are connected internally.

[0037]

FIG. 6B shows a state in which the SD memory card 10 is mounted in a card slot provided in the host device housing 38. As shown in FIG. 6B, since the tip end portion of the eject lever component 30 incorporating the antenna 34 protrudes from the outside of the housing, the radio wave transmission / reception efficiency is improved. Further, since it is not necessary to directly attach the antenna module to the SD memory card 10, the handling of the SD memory card 10 can be facilitated. In addition, since the antenna 34 provided in advance on the host device side is used, the user does not need to be aware of the mounting of the antenna. In the card slot The wireless communication function can be expanded simply by installing the SD memory card 10.

[0038]

In the case of the configuration shown in FIG. 6B, if the handling of the host device becomes inconvenient with the eject lever component 30 protruding, as shown in FIG. You may comprise the front-end | tip part of the lever component 30. FIG. That is, in the configuration shown in FIG. 6C, when the SD memory card 10 is installed in the card slot, the antenna of the eject lever component 30 is built in as shown in the side sectional view shown in FIG. The tip portion is bent along the housing surface. Even in this configuration, the antenna 34 is exposed to the outside of the housing, so that radio wave transmission / reception efficiency is not significantly impaired.

[0039]

Next, a fifth embodiment will be described.

In the fourth embodiment described above, the antenna 34 used in the SD memory card 10 is provided inside the eject lever. In the fifth embodiment, a configuration example provided on the surface of the casing of the host device is shown.

[0040]

FIG. 7 is a diagram showing a schematic configuration of an information processing apparatus (host device) in the vicinity of a card slot in which the SD memory card 10 can be inserted. As shown in FIG. 7, a Bluetooth antenna 40 is mounted on a protrusion on the surface of the host device casing. On the contact surface of the card slot with the SD memory card 10, an antenna contact 42 is provided at a position where the SD memory card 10 comes into contact with the antenna 40 when the SD memory card 10 is inserted into the slot.

[0041]

Further, the SD memory card 10 used in the fifth embodiment is provided with an antenna contact 10a on the side surface thereof. The antenna contact 10a of the SD memory card 10 is provided at a position in contact with the antenna contact 42 provided on the contact surface of the card slot with the SD memory card 10 when the SD memory card 10 is inserted into the card slot. . The internal configuration of the SD memory card 10 is the same as that of the first to third embodiments described above, and the antenna contact 10a and the RF circuit 20 are connected internally.

[0042]

As shown in FIG. 7, since the antenna 40 is provided on the protruding portion on the surface of the host device casing, the radio wave transmission / reception efficiency is improved. Further, since it is not necessary to directly attach the antenna module to the SD memory card 10, the handling of the SD memory card 10 can be facilitated. In addition, since the antenna 40 provided in advance on the host device side is used, the user does not need to be conscious of wearing the antenna. In the card slot The wireless communication function can be expanded simply by installing the SD memory card 10.

[0043]

In the fourth and fifth embodiments described above, the SD memory card 10 is provided with the antenna contact 10a for connecting to the antenna. However, one of the signal pins provided on the SD memory card 10 is an antenna. If it can be used for connection, the SD memory card 10 may be connected to the antennas 34 and 40 provided on the host device side via the SD memory card connector 35

[0044]

Next, a sixth embodiment will be described.

The sixth embodiment is an example in which the SD memory card 10e contains only a normal SD memory card function, and the main components of the Bluetooth function are provided outside as the Bluetooth function expansion module 50. FIG. 8 shows a configuration of the SD memory card 10e and the Bluetooth function expansion module 50 in the sixth embodiment.

[0045]

The SD memory card 10e shown in FIG. 8 operates as a normal SD memory card when used alone, and includes a controller LSI 51 and a flash memory 52. The controller LSI 51 is provided with an MPU 51a, ROM 51b, SD-BT interface 51c, SRAM 51d, memory interface 51e, and SD card interface 51f. It should be noted that the controller LSI 51 has the same functions as the corresponding parts of the controller LSI 21 in FIG. 2 except that the controller LSI 51 is not provided with the SD-BT interface 51c and the communication interface function, and detailed description thereof is omitted. The SD-BT interface 51 c is an interface for connecting to the Bluetooth function expansion module 50 via the connector 54.

[0046]

The Bluetooth function expansion module 50 incorporates an RF circuit 20, a Bluetooth baseband LSI 56, and an antenna 58. The Bluetooth baseband LSI 56 performs Bluetooth baseband control, and is used as an MPU (RISC) 56a, a ROM 56b storing a baseband control program, a link controller 56c for controlling the lowest protocol of Bluetooth, and a work buffer memory. SRAM 56d, other device 56e, SD-BT interface 56f for controlling an interface with the SD memory card 10e, and the like. Note that the Bluetooth baseband LSI 56 has the same functions as the corresponding units of the controller LSI 21 in FIG. 2 except that the SD-BT interface 56f and the memory interface function are not provided, and detailed description thereof is omitted. The SD-BT interface 56f is an interface for connecting to the SD memory card 10e via the connector 54.

[0047]

The Bluetooth baseband LSI 56 is connected to the RF circuit 20 through the link controller 56c. The RF circuit 20 is connected to an antenna 58 built in the Bluetooth function expansion module 50.

[0048]

As described above, normally, the SD memory card 10e can be used as a general SD memory card device, and the Bluetooth function expansion module 50 including the antenna 58, the RF circuit 20, and the Bluetooth baseband LSI 56 is connected. The communication interface function can be expanded. This facilitates component mounting in the SD memory card 10e, and can be used by adding a wireless interface function by arbitrarily connecting the Bluetooth function expansion module 50 as necessary.

[0049]

Next, a connection destination setting method connected by the wireless interface function in the first to sixth embodiments will be described.

In wireless communication systems such as Bluetooth, it is often desirable to communicate only with a specific device among devices within a communicable range. In such a case, information for specifying a connected device to be connected is necessary. In the case of Bluetooth, for example, by registering in advance the own PIN code and the connection destination PIN code as connection destination setting information, it is possible to communicate only with a specific partner based on the registered information. Is possible.

[0050]

For example, in the configuration in each of the embodiments described above (except for the configuration shown in FIG. 3), the connection destination setting information is written in advance in the protected memory area of the SD memory card. In the case of the SD memory card 10 shown in FIG. 2, the connection destination

setting information written in the protected memory area of the flash memory 22 can be read by the controller LSI 21 that can execute the wireless interface control and the memory interface control. Can be used in the card as identification information. As a result, communication with a specific partner set in advance becomes possible. On the other hand, as a host device for the SD memory card 10, only a specific host device having dedicated key information can be accessed by the authentication means (security data access control) of the SD memory card.

[0051]

Usually, it is not preferable that the connection destination setting information be known or changed by others. Therefore, as described above, (1) by attaching the SD memory card 10 to an arbitrary host device (such as a personal computer), it is possible to communicate with a connection partner preset by the host device, and (2 On the other hand, it is possible to realize an operation in which connection destination change and connection destination setting information can be read only when a card is attached to a specific host device.

[0052]

As a result, it is possible to achieve both convenience as an SD memory card that can expand a wireless interface function that can specify a connection partner and protection of highly confidential connection destination setting information.

[0053]

In the above description, an SD memory card is used as an IC card having a wireless interface function. However, the present invention can be applied to a small IC card having another shape and function. Also, the wireless communication method is not limited to Bluetooth, and for example, a wireless LAN can be targeted.

[0054]

【The invention's effect】

As described above in detail, according to the present invention, since the wireless interface control function is mounted in the IC card (SD memory card), the IC card can be used for function expansion in the information processing apparatus. Further, if the antenna module is not attached, it can be used as a general IC card.

[Brief description of the drawings]

FIG. 1 is a diagram showing an external configuration of an IC card with built-in wireless interface function (SD memory card) according to the present embodiment.

FIG. 2 is a block diagram showing the configuration of the SD memory card 10 and the antenna module 12 shown in FIG. 1 in the first embodiment.

FIG. 3 is a view showing a modification of the SD memory card 10 shown in FIG. 2;

FIG. 4 is a block diagram showing a configuration of an SD memory card 10c and an antenna module 12 in a second embodiment.

FIG. 5 is a block diagram showing a configuration of an SD memory card 10d and an antenna module 12a in the third embodiment.

6 is a diagram showing a schematic configuration of an information processing apparatus (host device) in the vicinity of a card slot in which an SD memory card 10 can be mounted. FIG.

7 is a diagram showing a schematic configuration of an information processing apparatus (host device) in the vicinity of a card slot in which an SD memory card 10 can be mounted. FIG.

FIG. 8 is a diagram showing a configuration of an SD memory card 10e and a Bluetooth function expansion module 50 in a sixth embodiment.

[Explanation of symbols]

10, 10c, 10d, 10e ... SD memory card

12, 12a ... Antenna module

20 ... RF circuit

21 ... Controller LSI

21a ... MPU21a (RISC)

21b ... ROM

21c Link controller

21d ... SRAM

21e ... Memory interface

21f ... SD memory card interface

22, 52 ... Flash memory

26, 58 ... Antenna

27 ... Antenna (A)

28 ... Antenna (B)

29 ... External RF amplifier

30, 31 ... Ejector lever components

34, 40 ... Antenna

35 ... SD memory card connector

37 ... Antenna contact

38 ... Host device housing

50 ... Bluetooth function expansion module

51 ... Controller LSI

51c, 56f ... SD-BT interface

56 ... Bluetooth baseband LSI

Patent Citations (31)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US4105156A *	1976-09-06	1978-08-08	Dethloff Juergen	Identification system safeguarded against misuse
JP2872793B2	1990-10-01	1999-03-24	株式会社日立製作所	IC card
US6618013B1 *	1996-01-16	2003-09-09	3Com Corporation	Retractable antenna assembly
FR2693575B1	1992-07-09	1994-08-19	Gemplus Card Int	Mass memory card with input / output function.
JPH0682344A	1992-09-04	1994-03-22	Mitsubishi Electric Corp	Detector for detecting abnormality of vehicle

US5708833A *	1993-04-27	1998-01-13	Norand Corporation	Antenna cap, antenna connectors and telephone line connectors for computer devices utilizing radio and modem cards
US6295031B1 *	1993-12-23	2001-09-25	Symbol Technologies, Inc.	Memory card assembly having an integral antenna
AU6398208I2 *	1993-12-28	1998-04-09	Nec Corporation	IC card radio modem and communication system using the same
JPH07321726A *	1994-05-20	1995-12-08	Fujitsu Ltd	Ic card type radio communication equipment
JPH0816859A	1994-06-30	1996-01-19	Toshiba Corp	Portable radio information read/write device
JP2616455B2 *	1994-08-12	1997-06-04	日本電気株式会社	Wireless modem
JPH08101900A	1994-09-30	1996-04-16	Toshiba Corp	Ic card for radio communication and data processor mounted with the same
JPH08101751A	1994-09-30	1996-04-16	Mitsubishi Electric Corp	Pc card and pc card system
US5918163A *	1995-03-31	1999-06-29	Compaq Computer Corporation	Electronic card assembly having a retractable antenna
US5914980A *	1995-09-21	1999-06-22	Kabushiki Kaisha Toshiba	Wireless communication system and data storage medium
DE29607253U1 *	1996-04-22	1996-07-04	Stocko Metallwarenfab Henkels	Combi chip card reader
US5913174A *	1996-06-19	1999-06-15	Proxim, Inc.	Connectorized antenna for wireless LAN PCMCIA card radios
SG54559A1 *	1996-09-13	1998-11-16	Hitachi Ltd	Power transmission system ic card and information communication system using ic card
JPH10143570A *	1996-11-15	1998-05-29	Susumu Miyake	Electronic transfer method for individual information of credit card, and miniature ic card, adapter card, terminal adapter, slip issuing machine and portable terminal therefor
JPH10198776A	1997-01-14	1998-07-31	Dainippon Printing Co Ltd	Portable information recording medium, and its information writing and reading method
WO1998036546A1 *	1997-02-14	1998-08-20	Ntt Mobile Communications Network Inc.	Method for controlling activation of mobile station, and mobile station using the method
FI102927B1 *	1997-02-14	1999-03-15	Nokia Mobile Phones Ltd	Communication unit, antenna and method for connecting the antenna
US5999294A *	1997-03-13	1999-12-07	Aironet Wireless Communications, Inc.	Detachable antenna with optical port
DE69838364T2 *	1997-06-20	2008-05-29	Hitachi Kokusai Electric Inc.	Read / write device, power supply system and communication system
JPH1166248A *	1997-08-12	1999-03-09	Mitsubishi Electric Corp	Non-contact type ic card
US6073856A *	1997-09-05	2000-06-13	Dai Nippon Printing Co., Ltd.	Noncontact IC device
KR100540857B1	1997-10-22	2006-01-10	코닌클리케 필립스 일렉트로닉스 엔.브이.	Dual-mode data carrier and circuit for such a carrier with simplified data transfer means
JPH11272823A	1998-03-24	1999-10-08	Toshiba Corp	Composite ic card having contact and contactless interface
US6522299B2 *	1999-04-08	2003-02-18	Cypress Semiconductor Corp.	PC card retractable antenna
JP2001144634A	1999-11-12	2001-05-25	Sony Corp	Semiconductor memory device
TWI275976B *	2004-12-31	2007-03-11	Wistron Corp	Mini PCI module having antenna pin set for electrically connecting to an antenna set

* Cited by examiner, † Cited by third party

Cited By (128)

Publication number	Priority date	Publication date	Assignee	Title

Family To Family Citations

JP3699889B2 *	2000-08-01	2005-09-28	株式会社東芝	Information processing apparatus and communication function expansion method
US6873842B2 *	2001-03-30	2005-03-29	Xilinx, Inc.	Wireless programmable logic devices
JP2003061167A *	2001-08-16	2003-02-28	Sony Corp	Card type transmitter and remote control system
JP3799289B2 *	2002-04-18	2006-07-19	インターナショナル・ビジネス・マシーンズ・コーポレーション	Computer apparatus and wireless system setting method
TWI246064B *	2002-07-29	2005-12-21	Milsys Ltd	Data storage and processing device, electronic appliance, electronic system and method of operating an appliance that responds to a plurality of commands
JP2004133881A *	2002-08-14	2004-04-30	Ricoh Co Ltd	Interface circuit of card type memory, asic (application specified ic) mounted with its circuit and image forming apparatus mounted with its asic
FR2844078A1 *	2002-08-30	2004-03-05	St Microelectronics Sa	COMMUNICATION METHOD BY ANTENNA FOR CHIP CARD AND APPARATUS THEREOF
US7088107B2 *	2002-09-30	2006-08-01	Matsushita Electric Industrial Co., Ltd.	Memory card
JP3870888B2 *	2002-10-15	2007-01-24	ソニー株式会社	Wireless communication card
US7016603B2 *	2002-11-26	2006-03-21	Lab Partners Associates, Inc.	Wireless communication module
US7225357B2 *	2003-01-21	2007-05-29	Zentek Technology Japan, Inc.	SDIO card development system
US7219758B2 *	2003-01-21	2007-03-27	Zentek Technology Japan, Inc.	SDIO controller
US7108379B2 *	2003-02-03	2006-09-05	Hewlett-Packard Development Company, L.P.	Wearable electronic device
DE10317394A1 *	2003-04-15	2004-11-04	Power Data Communications Co., Ltd., Banchiau	Radio transmission memory card for handset mounted with flash memory card, has memory card controller, flash controller, radio control circuit and radio frequency interface in controller chip, built in flash memory card
US6961596B2	2003-04-21	2005-11-01	3Com Corporation	Modular RF antenna and filter system for dual radio WLAN access points
WO2005004342A1 *	2003-07-08	2005-01-13	Fujitsu Limited	Communication terminal device, power supply method, and power supply program
JP4412947B2 *	2003-09-08	2010-02-10	株式会社ルネサステクノロジ	Memory card
US20050054399A1 *	2003-09-10	2005-03-10	Buris Nicholas E.	Method and apparatus for providing improved antenna bandwidth
US7386304B2 *	2003-10-07	2008-04-29	Lenovo (Singapore) Pte. Ltd.	Cruable U-NII wireless radio with secure, integral antenna connection via SM BIOS in U-NII wireless ready device
US7072691B2 *	2003-10-07	2006-07-04	Lenovo (Singapore) Pte.Ltd.	Cruable-U-NII wireless radio with secure, integral antenna connection via validation registers in U-NII wireless ready device
US7117013B2 *	2003-10-07	2006-10-03	Lenovo (Singapore) Pte. Ltd.	Cruable dual mode ISM and U-NII wireless radio with secure, integral antenna connection
US8666508B2	2003-10-15	2014-03-04	Arthroscopic Surgery Associates Corporation	Method and apparatus for monitoring conditions
US8999175B2 *	2004-01-09	2015-04-07	Ecolab Usa Inc.	Methods for washing and processing fruits, vegetables, and other produce with medium chain peroxycarboxylic acid compositions
WO2005067377A2	2004-01-15	2005-07-28	M-Systems Flash Disk Pioneers Ltd.	Removable medium with bookmark
AT428986T *	2004-02-02	2009-05-15	Nokia Corp	METHOD AND DEVICE FOR SECURING THE OPERATING CONDITION OF A MOBILE ELECTRONIC END UNIT
EP1691943A3 *	2004-04-30	2008-03-26	BIOTRONIK CRM Patent AG	Sending and receiving device
JP2005322109A *	2004-05-11	2005-11-17	Renesas Technology Corp	ic card module
US20080098134A1 *	2004-09-06	2008-04-24	Koninklijke Philips Electronics, N.V.	Portable Storage Device and Method For Exchanging Data
KR100596410B1	2004-11-04	2006-07-03	한국전자통신연구원	SD memory card for extension of function

JP2006172122A *	2004-12-15	2006-06-29	Toshiba Corp	Card type storage device
JP2006172121A *	2004-12-15	2006-06-29	Toshiba Corp	Card type storage device, adapter for the same, and host device
US7464213B2 *	2004-12-24	2008-12-09	Sony Corporation	Memory adapter and unit including independent radio circuit and removable memory store
EP1677523A3 *	2004-12-28	2011-03-30	LG Electronics, Inc	Digital broadcasting transmitter-receiver for portable computer
GB0501170D0 *	2005-01-20	2005-03-02	Antenova Ltd	A two-module integrated antenna and radio
CN101111854B	2005-02-14	2012-07-18	松下电器产业株式会社	Semiconductor memory module having built-in antenna
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
US7881695B2 *	2005-04-13	2011-02-01	Sony Corporation	Fixed network master
JP2006301827A *	2005-04-19	2006-11-02	Aruze Corp	Non-contact ic card system and mounting object for non-contact ic card
JP4332133B2 *	2005-05-12	2009-09-16	パナソニック電工株式会社	Memory card socket
WO2007002034A2 *	2005-06-20	2007-01-04	Comcast Cable Holdings, Llc	Method and system of managing and allocating communication related resources
CA2616030A1	2005-07-20	2007-01-25	Lab Partners Associates, Inc.	Wireless photographic communication system and method
TWI284843B *	2005-07-22	2007-08-01	Ind Tech Res Inst	Radio frequency identification reader/writer and financial transaction method using the same
WO2007018353A1	2005-08-03	2007-02-08	Matsushita Electric Industrial Co., Ltd.	Storage medium with built-in antenna
US8885714B2	2005-09-14	2014-10-07	Sandisk Il Ltd.	Removable media player for mobile phones
JP4517998B2 *	2005-10-07	2010-08-04	パナソニック電工株式会社	Memory card socket
JP4534962B2 *	2005-11-16	2010-09-01	ソニー株式会社	Information recording apparatus, non-contact recording medium and recording method therefor
US7634363B2 *	2005-12-07	2009-12-15	Affymetrix, Inc.	Methods for high throughput genotyping
WO2007082900A1 *	2006-01-19	2007-07-26	Gemplus	Portable electronic device suitable for providing a dynamic content
CN101346838B	2006-01-20	2012-10-03	松下电器产业株式会社	Antenna built-in module, card type information device and methods for manufacturing them
US7382625B2 *	2006-01-23	2008-06-03	Sony Ericsson Mobile Communications Ab	Combination antenna and SIM card support structure
US7775446B2	2006-03-10	2010-08-17	Panasonic Corporation	Card type information device and method for manufacturing same
JP5022434B2 *	2006-03-16	2012-09-12	ケーティーフリーテル・カンパニー・リミテッド	IC chip supporting large capacity memory and supporting method
KR100736032B1	2006-03-24	2007-07-16	주식회사 케이티프리텔	Smart card of supporting large size memory and method thereof
WO2007116790A1	2006-04-03	2007-10-18	Panasonic Corporation	Semiconductor memory module incorporating antenna
US7437063B2	2006-04-07	2008-10-14	Lab Partners Associates, Inc.	Wireless camera flash synchronizer system and method
KR100738923B1	2006-04-24	2007-07-12	에스케이 텔레콤주식회사	Smart card having zigbee module in financial settlement module or subscriber identification module and mobile communication terminal having same
JP4730196B2 *	2006-05-08	2011-07-20	パナソニック株式会社	Card type information device
US7460076B2 *	2006-06-13	2008-12-02	Sony Ericsson Mobile Communications Ab	Mobile wireless communications terminals and wireless communications cards for use with an electronic device
US7733659B2 *	2006-08-18	2010-06-08	Delphi Technologies, Inc.	Lightweight audio system for automotive applications and method
CN101136008B	2006-09-01	2011-01-05	飞思卡尔半导体公司	Application processor circuit for realizing SD host slave equipment and electronic equipments thereof
US7991158B2 *	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
FR2910747B1 *	2006-12-20	2011-05-20	Smart Packaging Solutions Sps	LOCAL RADIO FREQUENCY COMMUNICATION INTERFACE BETWEEN A MOBILE TELEPHONE AND A CONTACTLESS READER.

KR100822769B1	2007-03-13	2008-04-17	주식회사 에이치엘테크	Electronic tag including the mode convertible function and base station device using the tag
US20080244208A1 *	2007-03-30	2008-10-02	Narendra Siva G	Memory card hidden command protocol
WO2008150902A1 *	2007-05-29	2008-12-11	Lab Partners Associates, Inc.	System and method for maintaining hot shoe communications between a camera and a wireless device
JP5082599B2 *	2007-06-05	2012-11-28	ＫｄｄｉＫｄｄｉ株式会社	Data transfer device
JP2010530704A *	2007-06-18	2010-09-09	テレフオンアクチーボラゲット エル エム エリクソン（パブル）	RF switch device
US7572152B2 *	2007-06-27	2009-08-11	Sandisk Il Ltd.	Memory interface card with SIM functions
JP2009042927A *	2007-08-07	2009-02-26	Toppan Forms Co Ltd	Information storage device and information management system
CN101779380A	2007-08-10	2010-07-14	松下电器产业株式会社	Portable wireless device
US8915447B2	2007-09-12	2014-12-23	Devicefidelity, Inc.	Amplifying radio frequency signals
US9311766B2 *	2007-09-12	2016-04-12	Devicefidelity, Inc.	Wireless communicating radio frequency signals
US8807057B2	2007-09-12	2011-12-06	Devicefidelity, Inc.	Switching between internal and external antennas
US20090070691A1 *	2007-09-12	2009-03-12	Devicefidelity, Inc.	Presenting web pages through mobile host devices
US9330455B2	2007-09-12	2016-04-05	Devicefidelity, Inc.	Magnetically coupling radio frequency antennas
CN100573568C *	2007-10-30	2009-12-23	国民技术股份有限公司	The radio-frequency (RF) IC card device that is used for mobile device
US8929805B2 *	2007-10-30	2015-01-06	Nationz Technologies Inc.	System, method, and device for radio frequency communication
US9741027B2 *	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
JP5169368B2 *	2008-03-25	2013-03-27	沖電気工業株式会社	SD memory communication system and SD memory communication system
US20110212777A1 *	2008-04-17	2011-09-01	Power Digital Communications Co., Ltd.	Game device enabling three-dimensional movement
JP4342596B1	2008-05-20	2009-10-14	株式会社東芝	Electronic device and content data providing method
JP4346670B1 *	2008-05-20	2009-10-21	株式会社東芝	Electronic device and content data providing method
WO2009145518A2 *	2008-05-26	2009-12-03	에스케이텔레콤 주식회사	Memory card supplemented with wireless communication module, terminal for using same, memory card including wpan communication module, and wpan communication method using same
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US7630203B1 *	2008-09-17	2009-12-08	Ardi Technology Corporation	IC card
DE202008012847U1	2008-09-26	2008-12-11	ARDI TECHNOLOGY CORPORATION, Tucheng City	IC card with replaceable battery
HK1130615A2	2008-10-31	2009-12-31	Maestro Wireless Solutions Ltd	Modular modem
JP5269625B2 *	2009-01-14	2013-08-21	株式会社東芝	Interface control device
US8326141B1	2009-02-12	2012-12-04	Lab Partners Associates, Inc.	Systems and methods for changing power states of a remote device using one or more camera body controls and a preset delay
JP2012517624A	2009-02-12	2012-08-02	ラブ・パートナーズ・アソシエイツ・インコーポレーテッド	Early photo synchronization system and method
US8326136B1	2009-02-12	2012-12-04	Lab Partners Associates, Inc.	Systems and methods for communicating with a device using one or more camera body controls
US8718461B2	2009-02-12	2014-05-06	Lab Partners Associates, Inc.	Photographic synchronization optimization system and method
US8614766B1	2009-02-12	2013-12-24	Lab Partners Associates, Inc.	Systems and methods for controlling a power state of a remote device using camera body backlighting control signaling

EP2401708A4 *	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
US20110010497A1 *	2009-07-09	2011-01-13	Sandisk Il Ltd.	A storage device receiving commands and data regardless of a host
JP5278210B2	2009-07-13	2013-09-04	ソニー株式会社	Wireless transmission system, electronic equipment
KR101135278B1 *	2009-07-31	2012-04-12	사단법인 금융결제원	Method for Processing Memory Card Remote-Abandonment and Memory Card
KR101016893B1	2009-07-31	2011-02-22	사단법인 금융결제원	Memory Card with Function of Wireless Communication by Using Single Antenna
JP5398463B2 *	2009-10-15	2014-01-29	ルネサスエレクトロニクス株式会社	Interface IC and memory card having the same
CN201570055U *	2009-11-06	2010-09-01	深圳市江波龙电子有限公司	Double interface Micro SD card
US9483651B2 *	2009-11-30	2016-11-01	Ncr Corporation	Methods and apparatus for transfer of content to a self contained wireless media device
CN101778174A *	2009-12-22	2010-07-14	中兴通讯股份有限公司	Method, system and external card for achieving function extension of mobile terminal
WO2010148971A1 *	2009-12-22	2010-12-29	中兴通讯股份有限公司	Method, system and external connected card for extending functions of mobile terminal
US20110234904A1 *	2010-03-26	2011-09-29	Robert Wang	Flash disk with a replaceable memory for receiving signals from the digital tv or the digital radio
CN101835282B *	2010-04-23	2012-11-07	华为终端有限公司	Wireless Internet access module, user terminal, secure digital card and wireless communication method
US8335670B2 *	2010-06-22	2012-12-18	At&T Mobility Ii Llc	Near field communication adapters
US8600224B2	2010-07-14	2013-12-03	Lab Partners Associates, Inc.	Photographic wireless communication protocol system and method
TWI421768 *	2010-07-22	2014-01-01		Wireless micro secure digital memory card and manufacturing method thereof
JP5830231B2 *	2010-08-27	2015-12-09	エヌ・シー・アール・コーポレイションＮｃｒ Ｃｏｒｐｏｒａｔｉｏｎ	Method and apparatus for transferring content to a built-in wireless media device
JP5613040B2	2010-12-24	2014-10-22	オリンパス株式会社	MEMORY, IMAGE GENERATION DEVICE, NETWORK SETTING METHOD, AND NETWORK SETTING INFORMATION RECORDING METHOD
JP5185361B2 *	2010-12-28	2013-04-17	株式会社東芝	COMMUNICATION DEVICE, HOST DEVICE, COMMUNICATION CONTROL METHOD, AND COMMUNICATION CONTROL PROGRAM
CN102176236B *	2011-02-14	2013-07-10	华为终端有限公司	Printed circuit board, secure digital card and method for manufacturing printed circuit board
JP2012168865A *	2011-02-16	2012-09-06	Toshiba Corp	Memory system
JP5398761B2 *	2011-02-28	2014-01-29	株式会社東芝	Memory system
JP5677219B2 *	2011-07-08	2015-02-25	株式会社東芝	Storage device, storage method, and device for storing storage device
JP5448205B2 *	2011-07-15	2014-03-19	エヌイーシーコンピュータテクノ株式会社	Peripheral device, access authentication server, access authentication method
US8671171B2 *	2011-12-01	2014-03-11	International Business Machines Corporation	Wireless configuration for a computing device
CN102545943B *	2011-12-02	2014-10-29	惠州Tcl移动通信有限公司	LTE (Long Term Evolution) communication card and system
KR101264562B1 *	2011-12-19	2013-05-14	에스케이씨앤씨 주식회사	Tray integrated smart card and mobile device using the same
US20130258576A1 *	2012-03-29	2013-10-03	Gadi Ben-Gad	Memory Card
JP2013218498A	2012-04-06	2013-10-24	Toshiba Corp	Memory system
CN102968652B *	2012-11-20	2015-10-07	北京海泰方圆科技有限公司	The access method of smart card and access means
CN105144201A *	2013-03-11	2015-12-09	外兹·赛克有限公司	Wireless signal generating cards and methods and system of using such cards
US20150026397A1 *	2013-07-20	2015-01-22	Samsung Electronics, Ltd.	Method and system for providing memory module intercommunication

US9690169B2	2013-11-04	2017-06-27	Lab Partners Associates, Inc.	Photographic lighting system and method
WO2016185868A1 *	2015-05-18	2016-11-24	ソニー株式会社	Storage device, reader-writer, access control system, and access control method
US10249934B2	2015-11-30	2019-04-02	Toshiba Memory Corporation	Wirelessly-communicable memory card

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
JP4053704B2	2008-02-27	IC card with built-in wireless interface function, antenna module, information processing device
US8262416B2	2012-09-11	Dual-personality extended USB plugs and receptacles using with PCBA and cable assembly
JP2004508621A	2004-03-18	Interconnection and operation of non-volatile memory cards and I / O cards
JP4242856B2	2009-03-25	SD memory card for function expansion
US7742741B2	2010-06-22	Portable wireless data storage device
US8297987B2	2012-10-30	Extended USB plug, USB PCBA, and USB flash drive with dual-personality for embedded application with mother boards
JP2005044375A	2005-02-17	Communication card with input/output function
JP2008210301A	2008-09-11	Storage medium, communication system, and control device
JP2005519358A	2005-06-30	Portable data conversion and processing device with standard data interface
JP2008524945A	2008-07-10	Data transmission module and peripheral device for holding the module
US8540164B2	2013-09-24	Answer to reset (ATR) pushing
JP4705353B2	2011-06-22	Connector integrated RFID reader / writer
US20070293267A1	2007-12-20	Multi-function wireless transmission device
EP2000955B1	2009-12-30	Caching an answer to reset (ATR)
JP4548473B2	2010-09-22	Information processing apparatus and information processing method
KR101238431B1	2013-02-28	Portable wierless data storage device
KR200217331Y1	2001-03-15	Ader for data processor having Bluetooth chip
JP2004343504A	2004-12-02	Radio communication apparatus
JP2005084964A	2005-03-31	Electronic device
WO2012079429A1	2012-06-21	Storage device and configuration method thereof

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
JP2000000486A	2000-01-05	2000-01-05	IC card with built-in wireless interface function, antenna module, information processing device

Applications Claiming Priority (4)

Application	Filing date	Title
JP2000000486A	2000-01-05	IC card with built-in wireless interface function, antenna module, information processing device
US09/748,857	2000-12-26	IC card with radio interface function, antenna module and data processing apparatus using the IC card
US10/911,523	2004-08-05	IC card with radio interface function, antenna module and data processing apparatus using the IC card
US11/706,994	2007-02-16	IC card with radio interface function, antenna module and data processing apparatus using the IC card

Legal Events

Date	Code	Title	Description
2005-02-16	A621	Written request for application examination	**Free format text:** JAPANESE INTERMEDIATE CODE: A621 **Effective date:** 20050215
2006-11-16	A977	Report on retrieval	**Free format text:** JAPANESE INTERMEDIATE CODE: A971007 **Effective date:** 20061116
2006-11-29	A131	Notification of reasons for refusal	**Free format text:** JAPANESE INTERMEDIATE CODE: A131 **Effective date:** 20061128
2007-01-30	A521	Written amendment	**Free format text:** JAPANESE INTERMEDIATE CODE: A523 **Effective date:** 20070129
2007-04-04	A131	Notification of reasons for refusal	**Free format text:** JAPANESE INTERMEDIATE CODE: A131 **Effective date:** 20070403
2007-05-31	A521	Written amendment	**Free format text:** JAPANESE INTERMEDIATE CODE: A523 **Effective date:** 20070530
2007-11-28	TRDD	Decision of grant or rejection written	
2007-12-05	A01	Written decision to grant a patent or to grant a registration (utility model)	**Free format text:** JAPANESE INTERMEDIATE CODE: A01 **Effective date:** 20071204
2007-12-13	A61	First payment of annual fees (during grant procedure)	**Free format text:** JAPANESE INTERMEDIATE CODE: A61 **Effective date:** 20071206
2007-12-14	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20101214 **Year of fee payment:** 3
2007-12-14	R151	Written notification of patent or utility model registration	**Ref document number:** 4053704 **Country of ref document:** JP **Free format text:** JAPANESE INTERMEDIATE CODE: R151
2007-12-17	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20101214 **Year of fee payment:** 3
2010-11-15	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20111214 **Year of fee payment:** 4
2011-11-15	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20121214 **Year of fee payment:** 5
2012-11-15	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20121214 **Year of fee payment:** 5
2012-11-20	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20131214 **Year of fee payment:** 6
2018-11-29	S111	Request for change of ownership or part of ownership	**Free format text:** JAPANESE INTERMEDIATE CODE: R313121 **Free format text:** JAPANESE INTERMEDIATE CODE: R313117
2019-01-30	R350	Written notification of registration of transfer	**Free format text:** JAPANESE INTERMEDIATE CODE: R350
2020-01-05	EXPY	Cancellation because of completion of term	

Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

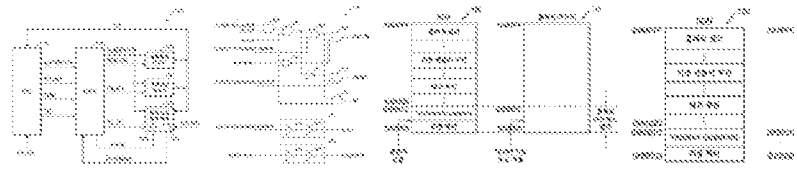
Patents KR100604877

Apparatus and method for controlling memory address mapping in embedded system

Abstract

Apparatus and methods for controlling the mapping of memory addresses in embedded systems are disclosed. An embedded system having a CPU for instructing and managing a program to decrypt and execute, comprises: a first nonvolatile memory that is electrically nonprogrammable; A second nonvolatile memory electrically programmable and erasable; A control signal generation circuit for generating a first control signal; And a decoder for transmitting the reset address to any one of the first nonvolatile memory and the second nonvolatile memory in response to the first control signal, a reset address output from the CPU, and at least one command signal. . The user can perform a reset routine according to the user's own code.
Flash memory

Images (6)



Classifications

- G06F12/02 Addressing or allocation; Relocation

View 3 more classifications

KR100604877B1
South Korea

Download PDF Find Prior Art Similar

Other languages: Korean

Inventor: 이형종

Worldwide applications

2004 KR 2005 US CN

Application KR1020040051801A events

2004-07-03 Application filed by 삼성전자주식회사
2004-07-03 Priority to KR1020040051801A
2005-06-30 Priority claimed from FR0506712A
2006-01-09 Publication of FR2866002A1
2006-07-31 Application granted
2006-07-31 Publication of KR100604877B1

Info: Patent citations (21), Non-patent citations (2), Cited by (19), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (23)

Hide Dependent

1. An embedded system having a CPU that instructs and manages a program to decrypt and execute,

   A first nonvolatile memory that cannot be electrically programmed and erased;

   A second nonvolatile memory electrically programmable and erasable;

   A control signal generation circuit for generating a first control signal Custom; And

   And a decoder for transmitting the reset address to any one of the first nonvolatile memory and the second nonvolatile memory in response to the first control signal, a reset address output from the CPU, and at least one command signal System characterized.

   2. The method of claim 1,

      The control signal generation circuit includes a third nonvolatile memory that can be electrically programmed and erased.

      When the decoder transmits the reset address to the first nonvolatile memory in response to the first control signal generated according to the initial state of the third volatile memory or the third volatile memory erase, the first nonvolatile memory Perform its own reset routine in response to the reset address,

      And when the decoder transmits the reset address to the second nonvolatile memory in response to the first control signal generated according to the third volatile memory program, the second nonvolatile memory performs its own reset routine. System.

   3. 3. The system of claim 2, wherein the third nonvolatile memory is programmed when the reset routine in the first nonvolatile memory ends.

   4. The method of claim 1,

      The decoder transmits the reset address to the first nonvolatile memory in response to the deactivated first control signal,

      And the decoder transmits the reset address to the second nonvolatile memory in response to the activated first control signal.

   5. The method of claim 1,

      And wherein the first nonvolatile memory is a ROM and the second nonvolatile memory is a flash memory.

   6. The method of claim 1, wherein the control signal generation circuit further generates a second control signal,

And the decoder blocks the CPU from accessing the first nonvolatile memory in response to the activated second control signal.

7. The system of claim 6, wherein the decoder outputs a signal to the CPU indicating that the CPU is blocked from accessing the first nonvolatile memory in response to the activated second control signal.

8. The method of claim 6,

The control signal generation circuit includes a third nonvolatile memory that can be electrically programmed and erased.

When the third nonvolatile memory is programmed, the control signal generation circuit generates the activated second control signal,

And when the third nonvolatile memory is erased, the control signal generating circuit generates the deactivated second control signal.

9. The method of claim 8,

The control signal generation circuit further generates a third control signal,

And the decoder permanently blocks the CPU from accessing the first nonvolatile memory in response to the activated third control signal.

10. The method of claim 1,

The control signal generation circuit further generates a second control signal, and wherein the decoder generates the selection signal for selecting only the second nonvolatile memory in response to the activated second control signal.

11. The method of claim 10,

The control signal generation circuit has a third nonvolatile memory which can be electrically programmed only.

And when the third nonvolatile memory is programmed, the control signal generation circuit generates an activated second control signal.

12. The system of claim 1, wherein the CPU outputs the reset address and the command signal to the decoder in response to a reset signal.

13. An embedded system having a CPU that instructs and manages a program to decrypt and execute,

A first nonvolatile memory that cannot be electrically programmed and erased;

A second nonvolatile memory electrically programmable and erasable;

A third nonvolatile memory electrically programmable and erasable; And

The reset address is generated in response to a first control signal generated according to any one of a program and an erase of the third nonvolatile memory, a reset address output from the CPU, and at least one command signal. And a decoder for outputting any one of the second nonvolatile memories.

14. The method of claim 13,

The system further includes a fourth nonvolatile memory that can be electrically programmed and erased.

And the decoder blocks the CPU from accessing the first nonvolatile memory in response to a second control signal generated as the fourth nonvolatile memory is programmed.

15. The method of claim 13,

The system further includes a fourth nonvolatile memory that can be electrically programmed and erased.

The decoder blocks the CPU from accessing the first nonvolatile memory in response to a second control signal generated as the fourth nonvolatile memory is programmed.

The decoder outputs the reset address to any one of the first nonvolatile memory and the second nonvolatile memory in response to a second control signal generated as the first control signal and the fourth nonvolatile memory are erased. System characterized in that.

16. The method of claim 15,

The system further includes a fifth nonvolatile memory that is electrically programmable only.

And the decoder permanently blocks the CPU from accessing the first nonvolatile memory in response to a third control signal generated as the fifth nonvolatile memory is programmed

17. The method of claim 13,

The system further includes a fourth nonvolatile memory that is electrically programmable only.

The decoder outputs an address associated with the reset address to the second nonvolatile memory regardless of the program or erase of the third nonvolatile memory in response to a second control signal generated as the fourth nonvolatile memory is programmed. System characterized in that.

18. 14. The system of claim 13, wherein the CPU outputs the reset address and the at least one control signal in response to a reset signal or a signal associated with a power up.

19. CPU for instructing and managing programs to decode and execute, first nonvolatile memory electrically nonprogrammable and erasable, second nonvolatile memory electrically programmable and erasable, third nonvolatile memory electrically programmable and erasable In the method for performing a reset routine in a system comprising:

In the first power-up or first reset, the decoder generates a first control signal generated by an initial state of the third nonvolatile memory or when the memory is erased, a reset address output from the CPU, and at least one command signal. in response to transmitting the reset address to the first nonvolatile memory;

Writing a program required by the second nonvolatile memory to the second nonvolatile memory while the first nonvolatile memory performs a reset routine based on the reset address;

Transmitting, by the decoder, the reset address to the second nonvolatile memory in response to the first control signal generated as the second nonvolatile memory is programmed when the second power-up or second reset is performed; And

And performing, by the second nonvolatile memory, performing a reset routine based on the reset address.

20. 20. The method of claim 19, wherein if the system further comprises a fourth nonvolatile memory that is electrically programmable and erasable,

And the decoder further blocks the CPU from accessing the first nonvolatile memory in response to a second control signal generated as the fourth nonvolatile memory is programmed. How to do it.

21. 20. The method of claim 19, wherein if the system further comprises a fourth nonvolatile memory that is electrically programmable and erasable,

The decoder blocks the CPU from accessing the first nonvolatile memory in response to a second control signal generated as the fourth nonvolatile memory is programmed;

The decoder transmits the reset address to any one of the first nonvolatile memory and the second nonvolatile memory in response to a second control signal generated as the first control signal and the fourth nonvolatile memory are erased. Further comprising the steps of: performing a reset routine.

22. The method of claim 21, wherein the system further comprises a fifth nonvolatile memory that is electrically programmable only.

And permanently blocking the CPU from accessing the first nonvolatile memory in response to a third control signal generated as the decoder is programmed with the fifth nonvolatile memory. How to.

23. 20. The method of claim 19, wherein the system further comprises a fourth nonvolatile memory that is electrically programmable only.

The decoder outputs an address associated with the reset address to the second nonvolatile memory regardless of the program or erase of the third nonvolatile memory in response to the second control signal generated as the fourth nonvolatile memory is programmed. Further comprising the step of: performing a reset routine.

Description

Apparatus and method for controlling memory address mapping in embedded system

The detailed description of each drawing is provided in order to provide a thorough understanding of the drawings cited in the detailed description of the invention.

1 illustrates a block diagram of an embedded system having a CPU that instructs and manages to decrypt and execute a program in accordance with an embodiment of the present invention.

FIG. 2 shows a circuit diagram of the decoder shown in FIG.

Fig. 3 shows a ROM before setting up a program required for the flash memory and a memory map of the flash memory.

Fig. 4 shows a ROM after setting up a program necessary for the flash memory and a memory map of the flash memory.

5 shows an operating timing diagram of the embedded system shown in FIG.

Figure 6 illustrates a block diagram of an embedded system having a CPU that instructs and manages to decrypt and execute a program according to another embodiment of the present invention.

The present invention relates to an embedded system (CPU), and more particularly to an apparatus and method for controlling the mapping of the memory address of the embedded system.

Recently, the rapid development of the embedded system has a processor therein and a memory for storing a program that defines the operation of the processor.

in general, since the embedded system performs a limited operation for a specific purpose unlike a general computer, once a program for the embedded system is developed, the program is fixed, and the fixed program is stored in a ROM embedded in the embedded system. . Such a program is called firmware.

Typically the firmware is stored in a ROM. Since the process of storing the firmware in the ROM is performed in the process of manufacturing the embedded system (called 'chip' when the embedded system is manufactured as one chip), the embedded system (or chip) After this is manufactured, there is a problem that the firmware cannot be modified.

in an embedded system with a CPU, when the embedded system is powered up or reset, typically the CPU indicates a value indicating the first address or last address of the memory. Is output as a reset address.

The chip starts all operations from the reset address. Since the instructions for executing the reset routine are stored in the memory area designated by the reset address, the CPU operates sequentially as described in the reset routine.

As is well known in the art, the reset routine performs tasks such as initializing the chip, starting a boot routine, and the like.

in an embedded system having a CPU, when the embedded system is powered up or reset, the reset address, which is the starting address for operating the CPU, is typically stored in a nonvolatile memory.

The reset routine including the boot routine must be maintained in the embedded system even after the power supplied to the embedded system is off to perform the same operation again when power is supplied to the embedded system again. If the reset routine is stored in the ROM, if the ROM must be changed every time the reset routine is different, that is, if the chip is to be remanufactured, it is time-consuming and economical.

In addition, from the standpoint of the manufacturer of the chip, if a customer wants to use different reset routines, there is a burden of masking using different ROM masks even if the chip is manufactured by the same manufacturing process.

Recently, a technology for storing firmware in EEPROM or flash memory has been developed. If the start address is in flash memory, the customer can change the reset routine to suit his intended use. Therefore, the manufacturer of the chip does not need to manufacture the chip that the customer wants for different customers.

However, the chip is delivered to the customer, and the customer must operate the chip in order to write his own unique reset routine into the flash memory. The flash memory is selected when the flash memory is selected by a start address of a CPU. Does not store any program code, the customer cannot operate the chip.

In general, since the start address of the CPU is made unique by the CPU manufacturer, the start address cannot be arbitrarily changed when making a system using the CPU. Therefore, a program code that enables writing of data to the flash memory is required. The program code is called a flash loader. Since the flash loader is code to help write data to the flash memory, the flash loader should be stored in a memory other than the flash memory.

The other memory should store the flash loader regardless of whether power is supplied. Therefore, a ROM is used as a memory for storing the flash loader.

Accordingly, the technical problem to be achieved by the present invention is that the firmware cannot be modified after the embedded system (or chip) is manufactured, and the ROM needs to be changed each time the reset routine is changed, and the user's needs are different. It provides a system and method to solve the problem of masking using a ROM mask.

An embedded system having a CPU for instructing and managing a program for decoding and executing a program for performing the technical problem comprises: a first nonvolatile memory which cannot be electrically programmed and erased; A second nonvolatile memory electrically programmable and erasable; A control signal generation circuit for generating a first control signal; And a decoder for transmitting the reset address to any one of the first nonvolatile memory and the second nonvolatile memory in response to the first control signal, a reset address output from the CPU, and at least one command signal IST_FET. It is provided.

The control signal generation circuit includes a third nonvolatile memory that can be electrically programmed and erased, and wherein the decoder is configured to control the first control signal generated according to the initial state of the third volatile memory or the third volatile memory erase. In response to transmitting the reset address to the first nonvolatile memory, the first nonvolatile memory performs its own reset routine in response to the reset address, and the decoder generates the reset routine according to the third volatile memory program. When the reset address is transmitted to the second nonvolatile memory in response to a first control signal, the second nonvolatile memory performs its own reset routine.

The third nonvolatile memory is programmed when the reset routine in the first nonvolatile memory ends.

The decoder transmits the reset address to the first nonvolatile memory in response to the deactivated first control signal, and the decoder transmits the reset address to the second nonvolatile memory in response to the activated first control signal. Send it.

The first nonvolatile memory is a ROM, and the second nonvolatile memory is a flash memory.

The control signal generation circuit further generates a second control signal, and the decoder blocks the CPU from accessing the first nonvolatile memory in response to the activated second control signal.

The decoder outputs a signal to the CPU indicating that the CPU is blocked from accessing the first nonvolatile memory in response to the activated second control signal.

The control signal generation circuit includes a third nonvolatile memory that can be electrically programmed and erased. When the third nonvolatile memory is programmed, the control signal generation circuit generates the activated second control signal, and When the third nonvolatile memory is erased, the control signal generation circuit generates the deactivated second control signal.

The control signal generation circuit further generates a third control signal, and the decoder permanently blocks the CPU from accessing the first nonvolatile memory in response to the activated third control signal.

The control signal generation circuit further generates a second control signal, and the decoder generates the selection signal for selecting only the second nonvolatile memory in response to the activated second control signal.

The control signal generation circuit includes a third nonvolatile memory that can be electrically programmed only, and when the third nonvolatile memory is programmed, the control signal generation circuit generates an activated second control signal.

The CPU outputs the reset address and the command signal to the decoder in response to a reset signal.

An embedded system having a CPU for instructing and managing to decode and execute a program for achieving the technical problem comprises: a first nonvolatile memory that is electrically programmable and non-erasable; A second nonvolatile memory electrically programmable and erasable; A third nonvolatile memory electrically programmable and erasable; And the reset address in response to a first control signal generated according to any one of a program and an erase of the third nonvolatile memory, a reset address output from the CPU, and at least one command signal. And a decoder configured to output any one of the second nonvolatile memories.

CPU for instructing and managing to decode and execute a program to achieve the above technical problem, a first nonvolatile memory that cannot be electrically programmed and erased, a second nonvolatile memory that can be electrically programmed and erased, and electrically programmed and erased. A method of performing a reset routine in a system having a third nonvolatile memory capable of performing the reset routine may occur when the decoder initializes the initial state of the third nonvolatile memory or when the memory is erased. Transmitting the reset address to the first nonvolatile memory in response to the first control signal, a reset address output from the CPU, and at least one command signal; Writing a program required by the second nonvolatile memory to the second nonvolatile memory while the first nonvolatile memory performs a reset routine based on the reset address; Transmitting, by the decoder, the reset address to the second nonvolatile memory in response to the first control signal generated as the second nonvolatile memory is programmed when the second power-up or second reset is performed; And performing, by the second nonvolatile memory, a reset routine based on the reset address.

In order to fully understand the present invention, the operational advantages of the present invention, and the objects achieved by the practice of the present invention, reference should be made to the accompanying drawings which illustrate preferred embodiments of the present invention and the contents described in the accompanying drawings.

Hereinafter, exemplary embodiments of the present invention will be described in detail with reference to the accompanying drawings. Like reference numerals in the drawings denote like elements.

1 illustrates a block diagram of an embedded system having a CPU according to an embodiment of the present invention. Referring to FIG. 1, the embedded system 100 according to the present invention includes a CPU 110, a first nonvolatile memory 120, a second nonvolatile memory 131, a control signal generation circuit 133, and a decoder (140).

The CPU 110 decodes a program used in an embedded system, instructs to execute the program, and comprehensively manages the embedded system or the program.

The first nonvolatile memory 120 is a memory which cannot be electrically programmed and erased, and may be implemented as a ROM. The second nonvolatile memory 131 is an electrically programmable and erased memory and may be implemented as a flash memory.

The control signal generation circuit 133 includes at least one nonvolatile memory 135 and 137.

The third nonvolatile memory 135 is an electrically programmable and eraseable memory and may be implemented as a flash memory. For example, the third nonvolatile memory 135 maintains a specific data value (eg, a logic 'high' or '1') through a process of programming predetermined data (hereinafter, referred to as a 'program'). The third nonvolatile memory 135 maintains a specific data value (eg, a logic 'low' or '0') through a process of erasing predetermined data (called 'erase'). Those skilled in the art are familiar with the program or erase process of the flash memory (cell), and thus a detailed description thereof will be omitted.

Accordingly, the third nonvolatile memory 135 generates a first control signal IniUser having a different state (eg, high or low) according to a program or an erase.

The control signal generation circuit 133 may further include a fourth nonvolatile memory 137, and the fourth nonvolatile memory 137 may be configured to have different states according to a program or an erase as described above. 2 Generate a control signal (RomHidden).

5 shows an operating timing diagram of the embedded system shown in FIG. 1 and 5, when the embedded system (or the chip 100) is first delivered to a customer or user, each of the first control signal IniUser and the second control signal RomHidden may be in an inactive state (eg, , Logic low).

When the power is supplied to the chip 100 by the user for the first time (this is called 'power up') and the external reset signal EXT_RST is in an active state (eg, logic high), the control is performed. The signal generation circuit 133-more precisely, the third nonvolatile memory 135 may receive a first control signal IniUser having a logic low in response to an external reset signal EXT_RST having a logic high or pulse shape. 140).

The control signal generation circuit 137-more precisely, the fourth nonvolatile memory 137 may further output the second control signal RomHidden to the decoder 140. The function of the second control signal RomHidden will be described later.

After a predetermined time elapses after the external reset signal EXT_RST becomes logic high, the internal reset signal INT_RST becomes logic high. Therefore, the CPU 110 outputs the reset address RST_ADD = C_ADD: n: 0> = 0x00000 to the decoder 140 in response to the internal reset signal INT_RST having a logic high.

In addition, the CPU 110 outputs a command signal IST_FET having a logic high for reading a command stored in a memory area corresponding to the reset address C_ADD: n: 0> = 0x00000 to the decoder 140.

The decoder 140 may respond to the reset address D_ADD <in response to a first control signal IniUser having a logic row, the reset address C_ADD <n: 0> = 0x00000, and at least one command signal IST_FET. m: 0> = 0x00000) to the first nonvolatile memory 120.

That is, the decoder 140 may transmit the first selection signal ROM_SEL having a logic high in response to the first control signal IniUser having a logic low and the command signal IST_FET having a logic high to the first nonvolatile memory 120.) And a reset address D_ADD <m: 0> = 0x00000 to the first nonvolatile memory 120. In this case, since the second selection signal FM_SEL maintains a logic low, the second nonvolatile memory 131 maintains a disabled state.

The first nonvolatile memory 120 is enabled in response to the first selection signal ROM_SEL having a logic high and is located in an area of the first nonvolatile memory 120 corresponding to the address 0x00000. The stored instructions are sent to the CPU 110 via the data bus 150.

When the CPU 110 interprets an instruction corresponding to the reset address (0x00000) and transmits an address (C_ADD <n: 0>) corresponding to the interpreted instruction to the decoder 140, the decoder 140 The address D_ADD <m: 0> corresponding to the address C_ADD <n: 0> is transmitted to the first nonvolatile memory 120. The first nonvolatile memory 120 performs initialization according to an instruction (eg, a reset handler routine) corresponding to the address D_ADD <m: 0>.

Thereafter, the first nonvolatile memory 120 is operated by an OS required for the second volatile memory 131 by a flash loader stored in the first nonvolatile memory 120 under the control of the CPU 110. A program including a system) is written (or stored) in the second volatile memory 131. The above process is called a 'reset routine according to the manufacturer code' or 'initialization mode'.

FIG. 2 shows a circuit diagram of the decoder shown in FIG. Referring to FIG. 2, the decoder 140 includes a plurality of logic circuits 201 to 227. The AND gate 201 logically multiplies the reset address C_ADD <n: 0> by the command signal IST_FET for drawing an instruction. The AND gate 203 logically multiplies the output signal of the AND gate 201 by the first control signal IniUser.

The OR gate 205 logically combines the output signal of the AND gate 203 with the address C_ADD <n: 0> = 0x80000 to 0x80FFF. The inverter 207 inverts the second control signal RomHidden, and the AND gate 209 ANDs the output signal of the OR gate 205 and the output signal of the inverter 207 and outputs the first selection signal ROM_SEL. do.

The inverter 211 inverts the output signal of the AND gate 203, and the AND gate 213 ANDs the output signal of the inverter 211 with the address C_ADD <n: 0> = 0x00000 to 0X7FFFFF and selects the second. Output the signal FM_SEL.

The buffer 217 is composed of a chain of a plurality of inverters 219 and 221 and buffers the addresses C_ADD <n: 0> = 0x90000 to 0X90FFF and outputs a selection signal FS_SEL. The buffer 223 consists of a chain of a plurality of inverters 225 and 227 and buffers the address C_ADD <m: 0> and outputs the address D_ADD <m: 0>.

Fig. 3 shows a ROM before setting up a program required for the flash memory and a memory map of the flash memory. Referring to FIG. 3, the first nonvolatile memory 120 may include various codes such as reset vectors, Vectored Exceptions, Exception routines, reset handler routines, flash loaders, and the like. Save the code. The second nonvolatile memory 131 does not store any code.

When the chip 100 is delivered to the customer for the first time, since there is no program (or code) in the second nonvolatile memory 131, the second nonvolatile memory 131 may be provided even when power is supplied to the chip 100. Does nothing. Therefore, when the program (or code) is not set in the second nonvolatile memory 131, a reset address (0x00000) is transmitted to the first nonvolatile memory 120 to operate the chip 100. Should be.

However, the first nonvolatile memory 120 and the second nonvolatile memory 131 have regions of overlapping addresses (for example, 0x00000 and 0x0001C). Therefore, the CPU 110 outputs the command signals IST_FET and DRW for distinguishing the address area of the first nonvolatile memory 120 from the address area of the second nonvolatile memory 131 to the decoder 140. .

The decoder 140 generates the first selection signal ROM_SEL having a logic high in response to the command signal IST_FET for command fetch and the first control signal IniUser having a logic low. May fetch an instruction stored in the first nonvolatile memory 120 and stored in a memory area corresponding to the reset address (0x00000) output from the CPU 110.

But. When the CPU 110 makes the command signal DRW for writing data or reading data to be logic high, the decoder 140 controls the command signal DRW having a logic high and the first control having a logic high. In response to the signal ROM_SEL, a second selection signal FM_SEL having a logic high is generated. Therefore, the CPU 110 may fetch an instruction stored in the second nonvolatile memory 120 and stored in the memory area corresponding to the reset address (0x00000) output from the CPU 110.

That is, when a manufacturer of the first nonvolatile memory 120 stores a predetermined code in the first nonvolatile memory 120 as shown in FIG. 3, power is first supplied or reset to the chip 100. In this case, the CPU 110 outputs a reset address (0x00000) and a command signal (IST_FET) for reading a command to the decoder 140 in response to the internal reset signal INT_RST, and the decoder 140 has a logic low. The first control signal ROM_SEL for enabling the first nonvolatile memory 120 is made logic high in response to the first control signal IniUser and the command signal IST_FET having a logic high.

Thus, the first nonvolatile memory 120 is initialized by a reset handler routine, after which the flash loader sets up all necessary programs (or code) including the user's own reset handler routine in the second nonvolatile memory 131. do. When the setup of the program (or code) is completed in the second nonvolatile memory 131, the third nonvolatile memory 133 is programmed.

That is, the first nonvolatile memory 120 performs a reset routine according to a manufacturer code under the control of the CPU 110 to write a predetermined code required for the second nonvolatile memory 131. After the initialization mode ends, the third nonvolatile memory 133 is programmed.

Thereafter, when the embedded system (or chip) is powered up or reset, the control signal generation circuit, that is, the third nonvolatile memory 135 has a logic high in response to an external reset signal EXT_RST. One control signal IniUser is output to the decoder 140.

When the internal reset signal INT_RST that is the reset signal of the CPU 110 becomes logic high, the CPU 110 outputs the reset address C_ADD <n: 0> = 0x00000 to the decoder 140. The command signal IST_FET for reading a command corresponding to the reset address C_ADD <n: 0> = 0x00000 is output to the decoder 140.

The decoder 140 generates a second selection signal FM_SEL having a logic high in response to the first control signal IniUser having a logic high and the command signal IST_FET having a logic high, and resets the reset address. The address D_ADD <m: 0> associated with the output is output. In this case, since the first selection signal ROM_SEL maintains a logic low, the first nonvolatile memory 120 maintains a disabled state.

However, the second nonvolatile memory 131 is enabled in response to the second selection signal FM_SEL having a logic high, and the second nonvolatile memory 131 corresponds to a reset address (0x00000). The command stored in the command (ie, a command set by the user) is output to the CPU 110 through the bus 150.

When the CPU 110 interprets an instruction set by a user and transmits an address C_ADD <n: 0> corresponding to the interpreted instruction to the decoder 140, the decoder 140 sends the address C_ADD < The address D_ADD <m: 0> corresponding to n: 0> is transmitted to the second nonvolatile memory 131.

The second nonvolatile memory 131 performs initialization according to an instruction corresponding to the address D_ADD <m: 0> (eg, a user specific reset handler routine of a user characteristic). Thereafter, the second nonvolatile memory 131 executes a user code set by a user under the control of the CPU 110. This is called 'reset routine according to user unique code' or 'user mode'.

Meanwhile, when various exceptions occur while the chip 100 operates in the initialization mode, control is transferred to a predetermined address in a CPU that supports vectored interrupts. Therefore, this vectored exception region should also be stored in the first nonvolatile memory 120.

Therefore, the address for the vectored exception region should be mapped to the first nonvolatile memory 120 in the initialization mode and to the second nonvolatile memory 131 in the user mode.

Fig. 4 shows a ROM after setting up a program necessary for the flash memory and a memory map of the flash memory. Referring to FIG. 4, when power is supplied to or reset from the chip 100 in a user mode, the decoder 140 may include a first control signal IniUser, a reset address 0x00000, and a command signal having a logic high. In response to IST_FET, a second select signal FM_SEL having a logic high is generated. Therefore, the chip 100 operates according to the reset routine according to the user unique code set up by the user.

In security-critical systems (or chips), such as smart cards, customers often have no confidence in the boot routine and / or flash loader provided by the chip manufacturer. This is because chip makers are concerned about making back doors such as Trojan horse codes.

In the embedded system (or chip) according to the present invention, after the customers store (or set) their own code in the second nonvolatile memory 131, the CPU 110 may transmit the first nonvolatile memory 120.) Can be disabled.

That is, a user wants to remove the first nonvolatile memory 120 because of concern that a program stored in the first nonvolatile memory 120 provided by a chip manufacturer is involved in the operation of the embedded system (or chip). In this case, the control signal generation circuit 133 of the embedded system 100 according to the present invention further includes a fourth nonvolatile memory 137 for generating the second control signal RomHidden.

When the control signal generation circuit 133 generates the first control signal IniUser having a logic low and the second control signal RomHidden having a logic high in response to an external reset signal EXT_RST, the CPU 110 Even if the first output the address for selecting the first nonvolatile memory 120, the decoder 140 is the CPU 110 in response to the second control signal (RomHidden) having a logic high is the first nonvolatile Access to the memory 120 is blocked, and a signal IVD indicating that access is blocked is output to the CPU 110.

Therefore, the CPU 110 may not execute a program (or code) stored in the first nonvolatile memory 120 and may not read desired data.

However, when the fourth nonvolatile memory 157 associated with generation of the second control signal RomHidden is erased, the fourth nonvolatile memory 137 has the second control signal RomHidden having a logic low. Occurs.

Accordingly, the decoder 140 may generate a first selection signal ROM_SEL having a logic high in response to the first control signal IniUser having a logic row and the second control signal RomHidden having a logic row. . That is, in the initialization mode, initialization is performed in the reset handler routine stored in the first nonvolatile memory 120.

Figure 6 illustrates a block diagram of an embedded system having a CPU that instructs and manages to decrypt and execute a program according to another embodiment of the present invention. Referring to FIG. 6, an embedded system 100 ' having a CPU includes a CPU 110, a first nonvolatile memory 120, a second nonvolatile memory 131, a control signal generation circuit 133 ', and A decoder 140 '.

The control signal generation circuit 133 ' includes at least two nonvolatile memories 135, 137, 139, and 141. The detailed inner block of the decoder 140 ' may be implemented with reference to FIG. 2.

The nonvolatile memory 135 generates a first control signal IniUser for selecting one of the first nonvolatile memory 120 and the second nonvolatile memory 131.

The nonvolatile memory 137 generates a second control signal (RomHidden), the nonvolatile memory 139 generates a third control signal (UserLock), and the nonvolatile memory 141 has a fourth control signal (RomHiddenLock). Occurs. The number of each control signal (IniUser, RomHidden, UserLock, and RomHiddenLock) is used arbitrarily for convenience of explanation.

The control signal generation circuit 133 includes a nonvolatile memory 139 which is electrically programmable only for generating a third control signal UserLock.

The third control signal UserLock having a logic high prevents the chip 100 from returning to the initialization mode permanently after the chip 100 is set to the user mode. That is, when the CPU 110 is prevented from accessing the first nonvolatile memory 120 by a second control signal (RomHidden) having a logic high, the user mode is changed to the initialization mode due to an unexpected wrong operation. The chip 100 can no longer be used.

Therefore, in order to prevent this, a third control signal UserLock having a logic high is required. That is, after programming the nonvolatile memory 135 generating the first control signal and the nonvolatile memory 137 generating the second control signal, the nonvolatile memory 139 generating the third control signal is programmed. When programming, the chip 100 cannot return to the initialization mode again.

for example. The initial state of the nonvolatile memory 139 is a logic low, and when the nonvolatile memory 139 is programmed, the nonvolatile memory 139 has a third logic having a logic high in response to an external reset signal EXT_RST. Generate a control signal (UserLock).

Once the nonvolatile memory 139 is programmed, the chip 100 is permanently used only in the user mode. That is, the CPU 100 may not permanently access the first nonvolatile memory 120.

In addition, the control signal generation circuit 133 includes a nonvolatile memory 141 which can be electrically programmed only to generate the fourth control signal RomHiddenLock.

An initial state of the nonvolatile memory 141 for generating the fourth control signal RomHiddenLock is logic low. Once the nonvolatile memory 141 is programmed, the nonvolatile memory 141 generates a fourth control signal RomHiddenLock having a logic high in response to an external reset signal EXT_RST.

Once the nonvolatile memory 141 is programmed, the chip 100 is permanently used only in the user mode. That is, the CPU 100 may not permanently access the first nonvolatile memory 120.

For example, when the fourth control signal RomHiddenLock is logic low, the nonvolatile memory 137 generating the second control signal RomHidden may be programmed or erased. However, when the fourth control signal RomHiddenLock becomes logic high, the nonvolatile memory 137 generating the second control signal RomHidden cannot be programmed or erased.

Although the present invention has been described with reference to one embodiment shown in the drawings, this is merely exemplary, and those skilled in the art will understand that various modifications and equivalent other embodiments are possible therefrom. Therefore, the true technical protection scope of the present invention will be defined by the technical spirit of the appended claims.

As described above, the system and method according to the present invention have the following advantages.

First, in the case where the reset routine including the boot routine is stored in the ROM, the ROM does not need to be changed every time the reset routine is changed.

Second, from the standpoint of the manufacturer of the chip, if the customer wants to use different reset routines, even if the chip is manufactured by the same manufacturing process, there is no need to mask using different ROM masks.

If the third start address is in flash memory, the customer can modify the reset routine to suit his intended use.

Fourth, the user can easily set the reset routine according to his own code.

Patent Citations (21)

Publication number	Priority date	Publication date	Assignee	Title
JPH1021085A	1996-07-05	1998-01-23	Nec Corp	Computer system
JPH10133958A	1996-10-31	1998-05-22	Nec Corp	Communication device control circuit
JP2000293376A	1999-04-05	2000-10-20	Nec Corp	Circuit and method for switching boot program
JP2000293375A *	1999-04-05	2000-10-20	Toshiba Information Systems (Japan) Corp	Object oriented computer system and computer readable storage medium with program stored therein
JP2004013719A	2002-06-10	2004-01-15	Fujitsu Ltd	Updating circuit, and updating method of multiplexed nonvolatile memory
KR20040017081A *	2002-08-20	2004-02-26	엘지전자 주식회사	Method for recording firmware in computer system
Family To Family Citations				
US5388267A	1991-05-29	1995-02-07	Dell Usa, L.P	Method and apparatus for updating and restoring system BIOS functions while maintaining BIOS integrity
US5634079A	1992-05-15	1997-05-27	Zenith Data Systems Corporation	System for providing for a parallel port with standard signals and a flash recovery mode with second predetermined signals redefining parallel port with alternate functions
US6182187B1 *	1993-04-07	2001-01-30	Compaq Computer Corporation	System ROM including a flash EPROM and a ROM for storing primary boot code replacing a block flash EPROM

US5805882A *	1996-07-19	1998-09-08	Compaq Computer Corporation	Computer system and method for replacing obsolete or corrupt boot code contained within reprogrammable memory with new boot code supplied from an external source through a data port
US5822243A *	1997-09-09	1998-10-13	Macronix International Co., Ltd.	Dual mode memory with embedded ROM
US5987605A *	1998-02-28	1999-11-16	Hewlett-Packard Co.	Methods and apparatus for dual-boot memory selection, update, and recovery in a programmable device
JP2000148594A *	1998-11-10	2000-05-30	Mitsubishi Electric Corp	Read protection circuit for rom data
JP3727485B2	1999-04-02	2005-12-14	シャープ株式会社	Microcomputer with built-in nonvolatile memory
US6601167B1 *	2000-01-14	2003-07-29	Advanced Micro Devices, Inc.	Computer system initialization with boot program stored in sequential access memory, controlled by a boot loader to control and execute the boot program
US6687154B2 *	2002-02-25	2004-02-03	Aplus Flash Technology, Inc.	Highly-integrated flash memory and mask ROM array architecture
US7111202B2 *	2002-06-28	2006-09-19	Hewlett-Packard Development Company, L.P.	Autonomous boot failure detection and recovery
JP2004038529A	2002-07-03	2004-02-05	Nec Corp	Information processor
CN1003371970	2002-10-14	2007-09-12	华为技术有限公司	Guide program recorder and method for guarantee of online upgrading thereof
US7272709B2 *	2002-12-26	2007-09-18	Micron Technology, Inc.	Using chip select to specify boot memory
US7206971B2 *	2003-04-07	2007-04-17	Lsi Logic Corporation	Selectable and updatable computer boot memory

* Cited by examiner, † Cited by third party

Non-Patent Citations (2)

Title
10021085
12293375

* Cited by examiner, † Cited by third party

Cited By (19)

Publication number	Priority date	Publication date	Assignee	Title
KR101094245B1 *	2010-05-25	2011-12-19	주식회사 씨앤엠마이크로	Main decoder chip structure for low power consumption and simplified pcb
Family To Family Citations				
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
KR100784866B1	2006-12-13	2007-12-14	삼성전자주식회사	Non-volatile memory device capable of reducing write time and memory card including the same
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US20090282419A1 *	2008-05-09	2009-11-12	International Business Machines Corporation	Ordered And Unordered Network-Addressed Message Control With Embedded DMA Commands For A Network On Chip
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US20100033310A1 *	2008-08-08	2010-02-11	Narendra Siva G	Power negotation for small rfid card
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
US10401961B2 *	2009-06-09	2019-09-03	Immersion Corporation	Method and apparatus for generating haptic effects using actuators
TWI497414B *	2009-06-23	2015-08-21	Phison Electronics Corp	File executing method and system
US8245024B2 *	2009-08-21	2012-08-14	Micron Technology, Inc.	Booting in systems having devices coupled in a chained configuration

US8429391B2	2010-04-16	2013-04-23	Micron Technology, Inc.	Boot partitions in memory devices and systems
GB2493340A *	2011-07-28	2013-02-06	St Microelectronics Res & Dev	Address mapping of boot transactions between dies in a system in package
CN103345456B *	2013-06-21	2015-12-02	烽火通信科技股份有限公司	Regulate circuit and the method for BootLoader enabling address
US10459735B2 *	2015-11-04	2019-10-29	Texas Instruments Incorporated	Scalable boot options for a processor/controller
US10979232B2 *	2018-05-31	2021-04-13	Motorola Solutions, Inc.	Method for provisioning device certificates for electronic processors in untrusted environments
US10430181B1 *	2018-08-20	2019-10-01	Quanta Computer Inc.	Retrieving updated firmware code
TWI690930B *	2019-01-09	2020-04-11	力晶積成電子製造股份有限公司	Method of compensating charge loss and source line bias in programing of non-volatile memory device

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
KR100604877B1	2006-07-31	Apparatus and method for controlling memory address mapping in embedded system
US5327531A	1994-07-05	Data processing system including corrupt flash ROM recovery
KR100375217B1	2003-03-07	Microcontroller incorporating an electrically rewritable non-volatile memory
US6505279B1	2003-01-07	Microcontroller system having security circuitry to selectively lock portions of a program memory address space
US6339815B1	2002-01-15	Microcontroller system having allocation circuitry to selectively allocate and/or hide portions of a program memory address space
KR100508087B1	2005-08-17	System boot using nand flash memory and method thereof
JP2004103219A	2004-04-02	Apparatus and system for setting write-protect region of memory block in non-volatile semiconductor memory device
JP2004118826A	2004-04-15	System unit booted using flash memory, and its booting method
US6115814A	2000-09-05	Memory paging scheme for 8051 class microcontrollers
JPH08278895A	1996-10-22	Data processor
US8607061B2	2013-12-10	Flash device security method utilizing a check register
JPH1050078A	1998-02-20	Erasing method and program protecting method and device for electrically erasable and programmable read only memory
US5950222A	1999-09-07	Microcomputer using a non-volatile memory
EP0858040B1	2005-10-26	Microcomputer containing flash EEPROM therein
US7310277B2	2007-12-18	Non-volatile semiconductor storage device with specific command enable/disable control signal
JP2005107608A	2005-04-21	Electronic device, nonvolatile memory, and method for rewriting data of nonvolatile memory
JP4958201B2	2012-06-20	Microcomputer
JP3197865B2	2001-08-13	Microcomputer
US9542113B2	2017-01-10	Apparatuses for securing program code stored in a non-volatile memory
CN110968254A	2020-04-07	Partition protection method and device for nonvolatile memory
KR20000033437A	2000-06-15	Apparatus for implementing function of bootstrap loader
JP3866269B2	2007-01-10	Microcomputer
JP2003044457A	2003-02-14	Data processor
JP3695931B2	2005-09-14	Microcomputer
JP4848126B2	2011-12-28	Microcomputer, data protection method for nonvolatile memory in microcomputer

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
KR1020040051801A	2004-07-03	2004-07-03	Apparatus and method for controlling memory address mapping in embedded system

Applications Claiming Priority (5)

Application	Filing date	Title
KR1020040051801A	2004-07-03	Apparatus and method for controlling memory address mapping in embedded system
US11/050,477	2005-02-03	Method and apparatus for executing the boot code of embedded systems
FR0506712A	2005-06-30	METHOD AND DEVICE FOR EXECUTING THE INTEGRATED SYSTEM INITIATION CODE
DE102005031530.5A	2005-07-01	Storage system, single-chip microcontroller and embedded system
CNB200510082149XA	2005-07-04	Method and apparatus for executing the boot code of embedded systems

Legal Events

Date	Code	Title	Description
2004-07-03	A201	Request for examination	
2006-01-12	E902	Notification of reason for refusal	
2006-06-19	E701	Decision to grant or registration of patent right	
2006-07-19	GRNT	Written decision to grant	
2013-07-01	FPAY	Annual fee payment	**Payment date**: 20130701 **Year of fee payment**: 8
2014-06-27	FPAY	Annual fee payment	**Payment date**: 20140630 **Year of fee payment**: 9
2015-06-29	FPAY	Annual fee payment	**Payment date**: 20150630 **Year of fee payment**: 10
2016-06-29	FPAY	Annual fee payment	**Payment date**: 20160630 **Year of fee payment**: 11
2017-06-29	FPAY	Annual fee payment	**Payment date**: 20170630 **Year of fee payment**: 12
2018-06-28	FPAY	Annual fee payment	**Payment date**: 20180629 **Year of fee payment**: 13

Data provided by IFI CLAIMS Patent Services

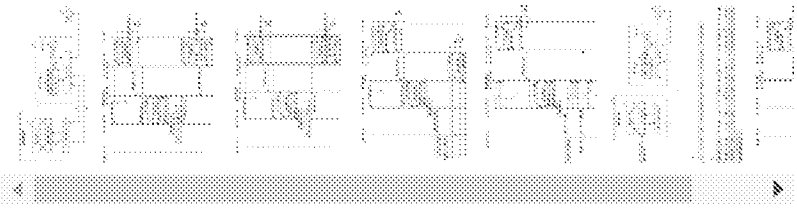
Patents JP2005202914

Secure device and information processor

Abstract

<P>PROBLEM TO BE SOLVED: To provide an IC card 20 that efficiently transmits information about card processing performed as instructed from an external R/W 30 to a cellular phone 10 according to international standards. <P>SOLUTION: The IC card 20 with a first communication means, a second communication means and a plurality of card applications 21 is provided with an information delivery means 22 that can be accessed from all the card applications. The card applications 21 create transfer information according to instructions received from the external R/W 30 through the first communication means, and write this information into the information delivery means 22. The transfer information is delivered to the cellular phone 10 according to the instructions received from the cellular phone 10 through the second communication means. The cellular phone 10 can obtain information about card processing by accessing the information delivery means 22 after card processing for the IC card 20 is complete. The IC card delivers the transfer information as instructed by the cellular phone and this process conforms to the international standards. <P>COPYRIGHT: (C)2005,JPO&NCIPI

Images (8)



Classifications

G06K19/07 Record carriers with conductive marks, printed circuits or semiconductor circuit elements, e g. credit or identity cards also with resonating or responding marks without active components with integrated circuit chips

View 4 more classifications

JP2005202914A

Japan

Download PDF Find Prior Art Similar

Other languages: Japanese

Inventor: Atsushi Minemura, 峰村 敦

Worldwide applications

2004 JP US CN EP

Application JP2004168282A events

2003-12-15 Priority to JP2003416380

2004-06-07 Application filed by Matsushita Electric Ind Co Ltd, 松下電器産業株式会社

2004-06-07 Priority to JP2004168282A

2005-07-28 Publication of JP2005202914A

Status Withdrawn

Info: Patent citations (10), Cited by (22), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (10)

Hide Dependent

1. A secure device comprising a first communication means, a second communication means, and one or more card function means,
An information transfer means that can be accessed from all the card function means is provided, and the card function means transfers the information for transmission generated based on an instruction from an external reader / writer received through the first communication means. The secure device, wherein the information delivery means delivers the transmission information to the information processing apparatus based on an instruction from the information processing apparatus received through the second communication means.

2. The secure device according to claim 1, wherein the first communication unit performs non-contact communication, and the second communication unit performs contact communication.

3. The secure device according to claim 1, wherein the transmission information includes information for specifying a processing unit of the information processing apparatus and information delivered to the processing unit.

4. 4. The secure device according to claim 3, wherein the transmission information further includes information for specifying the card function means.

5. An information processing apparatus that holds the secure device according to claim 1,
Middleware for accessing the information transfer means of the secure device through the second communication means of the secure device, and acquiring and interpreting the transmission information held in the information transfer means; An information processing apparatus that performs control so that a process for which information is requested is executed using resources of the information processing apparatus.

6. The information processing apparatus according to claim 5, wherein the middleware acquires the transmission information when a process start operation is performed.

7. An information processing apparatus that holds the secure device according to claim 1,
State monitoring means for monitoring the end of communication by the first communication means of the secure device;
When the state monitoring means detects the end of the communication, it accesses the information delivery means of the secure device through the second communication means of the secure device, and acquires the transmission information held by the information delivery means The information processing apparatus includes: middleware that interprets the information, and the middleware performs control so that the processing for which the transmission information is requested is executed using resources of the information processing apparatus.

8. An information processing apparatus that holds the secure device according to claim 1,
State monitoring means for monitoring detachment from the electromagnetic field at which communication by the first communication means of the secure device is impossible;
When the state monitoring unit detects separation from the electromagnetic field, the secure device accesses the information transfer unit of the secure device through the second communication unit of the secure device, and acquires the transmission information held by the information transfer unit Middleware that interprets the information, and the middleware performs control so that the processing requested by the transmission information is performed using the resources of the information processing device.

9. The information processing apparatus according to claim 5, wherein the secure device is attached in a detachable state.

10. The information processing apparatus according to claim 5, wherein the secure device is embedded integrally.

Description

The present invention relates to a secure device such as an IC card and an information processing apparatus such as a mobile phone equipped with the secure device, and the information processing apparatus efficiently grasps a result of processing performed between the secure device and an external reader / writer. In addition, the information processing apparatus can operate in conjunction with the processing.

In recent years, IC cards have been widely used for electronic payment cards, commuter passes, prepaid tickets with a deposit function, and the like. Recently, IC cards having a relatively large storage space have been made in combination with improvements in miniaturization technology, and such IC cards have a plurality of card applications (hereinafter, referred to as card services) that execute card services. The application is abbreviated as "application") and can be used as a multi-application card corresponding to a plurality of uses.
The IC card communication method includes contact communication for reading / writing recorded information by contacting the reader / writer with the electrical contact of the IC card, and physical communication with the reader / writer by exchanging information by wireless communication. There are two types of contactless communication that are not required.

International standards for IC cards include ISO 7816 for contact communication and ISO 14443 for non-contact communication. In this international standard, the exchange of data between the card application of the IC card and the terminal application on the reader / writer side is "command" sent from the terminal application to the card application, and "response" sent from the card application to the terminal application. And APDU (Application Protocol Data Unit) for specifying the command and response format is determined. Therefore, the IC card can only operate passively.

Recently, a chip-shaped IC card capable of both contact communication and non-contact communication is mounted on a mobile phone, and the mobile phone is used instead of an electronic wallet or commuter pass. For example, in the case where prepaid ticket information is recorded on an IC card, when the user operates the key of the mobile phone to instruct the balance display, the instruction is input to the IC card by contact communication from the mobile phone, and the IC card is read out and displayed on the screen of the mobile phone. In addition, when this mobile phone is put on an automatic ticket gate at a station, an instruction to read or rewrite information data is input to the IC card by contactless communication from the ticket gate, and the balance recorded on the IC card according to this instruction. Data is updated.

Patent Document 1 listed below discloses an apparatus for displaying that a card function has been normally operated using display means of a mobile phone when the non-contact communication processing by the IC card of the mobile phone is normally performed. Has been described. This IC card activates a card application specified by an external reader / writer from among a plurality of card applications, and performs card use communication (non-contact communication) according to the service to be used with the external reader / writer. If the card use communication ends normally, a notification signal indicating the fact and the application ID are transmitted to the control unit of the mobile phone. Upon receiving this, the control unit outputs notification information predetermined according to the application ID from the display unit of the mobile phone.
JP 2003-60748 A

Since mobile phones equipped with IC cards have keypads, displays, communication functions, application execution functions, etc., these mobile phone functions are linked to card processing in IC card non-contact communication. By using, services with higher convenience, operability and functionality can be realized. The device described in Patent Document 1 is also directed to display in conjunction with non-contact communication processing of an IC card using display means of a mobile phone.
However, an IC card that conforms to the international standard can only perform a passive operation that simply returns a response to a command transmitted from an external reader / writer via contactless communication. Like the described IC card, it is impossible to transmit a notification signal or application ID to the control unit of the mobile phone.

Accordingly, the inventors have taken measures to cause the mobile phone to perform an operation linked to the non-contact communication processing between the IC card and the external reader / writer even when the IC card satisfying the international standard is mounted on the mobile phone. Various investigations were made. For example, the following methods (1) and (2) can be considered.

(1) Pre-activation of terminal application When a mobile phone equipped with an IC card is placed over an external reader / writer, the card application specified by the external reader / writer is activated among the multiple card applications stored in the IC card. Then, contactless communication for use of the card is started between the IC card and the external reader / writer. However, in the case of an IC card conforming to the international standard, the IC card indicates that the contactless communication has ended. I cannot make calls to my mobile phone.
Therefore, the mobile phone continues to send a polling signal to the IC card by contact communication so that the end of the non-contact communication can be detected by the mobile phone. The IC card responds to the polling signal for monitoring the processing status if it is performing non-contact communication, and responds "not performing" if it is not performing non-contact communication. The end of communication can be detected.
The mobile phone that has detected the end of non-contact communication of the IC card sends a command instructing the card application that has executed the card use processing to respond to the card processing result. When the response data is obtained, the card processing result can be displayed on the mobile phone.

However, multiple card applications created by each service provider stored in a multi-application compatible IC card require authentication for access, and the authentication method differs for each service provider (card application). For maintenance purposes, the authentication method is not open to the public. Therefore, it is difficult for the mobile phone to send a command to the card application that has executed the card use process.

Therefore, in the method (1), the service provider creates a terminal application (an application accessible to the card application) that cooperates with the card application, and stores the terminal application in the mobile phone. Then, before placing the mobile phone on the external reader / writer, the user anticipates a card application designated by the external reader / writer and activates a corresponding terminal application in advance.
In this way, when the mobile phone detects the end of non-contact communication of the IC card, the terminal application activated in advance can obtain the card processing result from the card application that has executed the card use processing. The processed result can be displayed on the display of the mobile phone.

(2) Attempt to obtain information for all card applications When a mobile phone that monitors the processing status of an IC card detects the end of non-contact communication of an IC card, it obtains information on the card processing results for all card applications. Try. By doing so, information on the card processing result can be obtained from the card application that has actually executed the card use processing, and the information can be displayed on the display of the mobile phone.

However, the method "(1) Pre-starting terminal application" forces the user to start the terminal application, which increases the burden on the user and is not convenient. In addition, the user may not know the terminal application to be activated. Further, the method of "(2) Attempting to acquire information for all card applications" tries to acquire information for a card application that has not executed the card use process, and therefore the processing is slow. In addition, this method requires a separate measure against the difference in the authentication method of each card application.

The present invention solves such problems, and a secure device that can efficiently transmit information on processing performed in response to an instruction from an external reader / writer to an information processing device in accordance with international standards. An information processing apparatus capable of receiving information on the processing and an information processing apparatus capable of performing an operation linked to the processing of the secure device based on information obtained from the secure device are provided. The purpose is that.

Therefore, in the present invention, information transfer that can be accessed from all the card function means to a secure device including the first communication means, the second communication means, and one or more card function means (card application). The card function means writes the transmission information generated based on the instruction from the external reader / writer received through the first communication means to the information delivery means, and the information delivery means passes through the second communication means. Based on the received instruction from the information processing apparatus, this transmission information is delivered to the information processing apparatus.
Therefore, after the card processing by the first communication unit of the secure device is completed, the information processing apparatus can acquire information on the card processing by accessing the information transfer unit of the secure device. The secure device delivers information for transmission in response to an instruction from the information processing apparatus, and this processing conforms to international standards.

In the secure device of the present invention, the first communication means performs non-contact communication, and the second communication means performs contact communication.
In the present invention, the information for transmission that is handed over to the information processing device includes information for specifying the processing means (terminal application) of the information processing device, and information that is handed over to the processing means. The information that identifies is included.
Therefore, it is not necessary for the user to activate the terminal application in advance.

In the present invention, the information processing apparatus holding the secure device is accessed through the second communication means of the secure device to the information delivery means of the secure device, and the transmission information held by the information delivery means is acquired. The middleware controls the processing that the transmission information is requested to be executed using the resources of the information processing apparatus.
Further, the middleware acquires transmission information when a process start operation is performed.
This middleware can efficiently acquire the transmission information generated by each card function means without knowing the method of accessing each card function means (card application) stored in the secure device or the authentication method. it can.

In the present invention, the information processing apparatus holding the secure device monitors the end of communication by the first communication means of the secure device, or from an electromagnetic field that makes communication by the first communication means impossible. When the state monitoring means detects the end of the communication, the state monitoring means for monitoring the detachment of the device accesses the information delivery means of the secure device through the second communication means of the secure device and is held by the information delivery means Middleware for acquiring and interpreting transmission information is provided, and the middleware controls so that processing requested by the transmission information is executed using the resources of the information processing apparatus.
Therefore, an operation linked to the card processing of the secure device is performed using the resources of the information processing apparatus.

The secure device of the present invention is detachably attached to the information processing apparatus or is embedded in the information processing apparatus integrally.

The secure device of the present invention can efficiently transmit information of card processing performed by an instruction from an external reader / writer to the information processing apparatus in accordance with international standards, and the information processing apparatus of the present invention Can efficiently acquire the transmission information generated by each card function means without knowing the method of accessing each card function means (card application) stored in the secure device or the authentication method.

This information processing device is linked to the card processing of the secure device using information processing device resources, ie, keypad, display, communication function, terminal application, etc., based on information obtained from the secure device. Operation can be performed.
Therefore, the convenience, operability and functionality of the secure device are improved, and more advanced services can be realized with a general-purpose IC card conforming to international standards.

(First embodiment)
In the first embodiment of the present invention, a case will be described in which the secure device is an IC card having both contact communication and non-contact communication functions, and the information processing apparatus is a mobile phone. The IC card attached to the mobile phone exchanges information with the mobile phone by contact communication. Further, when the mobile phone is placed on the external reader / writer so that the IC card enters the communication range of the external reader / writer, the IC card exchanges information with the external reader / writer by non-contact communication.
Further, the IC card includes a dedicated card application (information passing card application) for transferring information to and from the mobile phone. Information can be written into this information delivery card application from any card application stored in the IC card. In the mobile phone, the middleware handles information exchange with the information exchange card application.

FIG. 1 schematically shows configurations of the mobile phone 10, the IC card 20, and the external reader / writer 30. The IC card 20 temporarily stores a plurality of card applications 21 that execute various services created by a service provider, an information transfer card application 22 that centrally transfers information to and from the mobile phone 10, and information to be transferred. An information storage unit 23 that stores data and a card OS 24 that executes communication processing and file management are provided. The mobile phone 10 includes a terminal application 11 that performs an operation linked to the processing of the card application 21, a middleware 12 that provides an information transfer service to the terminal application 11, and a device driver that controls the operation of the mobile phone 10. 13

All the card applications 21 of the IC card 20 can access the information delivery card application 22, and information sent from the external reader / writer 30 to the card application 21 is stored in the information storage unit 23 of the information delivery card application 22. Can be written on.
For example, a Java (registered trademark) card in which a card application is created in the Java (registered trademark) language can be used to realize the information passing card application 22 by using the Shared interface. In the IC card, the card applications are separated from each other by a firewall so that a plurality of card

applications can coexist safely. The Shared Interface is an interface that can access the card applications without being blocked by the firewall.
Further, if the middleware 12 of the mobile phone 10 performs mutual authentication with the information delivery card application 22, the information delivery card application 22 can be freely accessed thereafter.

In FIG. 1, the order of processing performed by the three parties of the mobile phone 10, the IC card 20, and the external reader / writer 30 is indicated by circled numbers. The user operates the mobile phone 10 to instruct the start of processing, and in response to this, the middleware 12 of the mobile phone 10 requests the device driver 13 to monitor the state of the IC card 20 by polling (1). When the user places the mobile phone 10 over the external reader / writer 30, the IC card 20 is activated, and the card application 21 designated by the external reader / writer 30 executes the processing instructed by the external reader / writer 30. (2). The card application 21 writes information that needs to be sent to the mobile phone 10 in accordance with this processing to the information delivery card application 22 (3).
This information includes the name of the terminal application (including middleware) to be activated, information to be transferred to the terminal application, the ID of the requested card application, and the like.

When the device driver 13 of the mobile phone 10 that continues to monitor the state of the IC card 20 detects the end of the non-contact communication of the IC card 20, it notifies the middleware 12 of a processing end notification (4). After performing mutual authentication with the information delivery card application 22, the middleware 12 accesses the information delivery card application 22 and acquires the information held therein (5). The middleware 12 activates the designated terminal application 11 based on the information acquired from the information delivery card application 22, and the terminal application 11 performs the designated processing. When the middleware 12 is designated, the middleware 12 itself performs the processing (6).

Thus, in this apparatus, since the IC card 20 is equipped with the information transfer card application 22, the middleware 12 of the mobile phone 10 receives this information transfer when the processing by the non-contact communication of the IC card 20 is completed. The card application 22 can be accessed and information associated with the processing can be acquired. For this reason, in this apparatus, the situation that the access destination is not known does not occur, and inefficient processing for accessing all of the card applications 21 is not necessary.

Further, the middleware 12 of the mobile phone 10 has only to authenticate with the information passing card application 22, and does not need to know the authentication method of each card application 21.
Further, since the information acquired from the information delivery card application 22 includes information on the terminal application to be activated, the terminal application can be identified from this information. Therefore, it is not necessary for the user to activate the terminal application in advance.
Further, when receiving an instruction from the middleware 12 of the mobile phone 10, the information passing card application 22 of the IC card 20 returns the held information to the middleware 12, and the operation of the IC card 20 is as follows. Complies with international standards.

Here, the device driver 13 of the mobile phone 10 detects the end of the non-contact communication of the IC card 20 and transmits it to the middleware 21. However, the external reader / writer 30 leaves the communication area. (In other words, a state in which contactless communication is impossible due to separation from an electromagnetic field capable of contactless communication) may be detected and transmitted to the middleware 21.
Also, the user can instruct polling processing to be started by an operation of pressing a specific key of the mobile phone 10 or an operation of shaking the mobile phone 10 by providing an acceleration sensor in the mobile phone 10.

FIG. 2 shows a processing flow when the mobile phone 10, the IC card 20 and the external reader / writer 30 of the payment terminal cooperate to ask the user to input a personal identification number (PIN) necessary for the credit payment processing. Is shown. The middleware 12 of the mobile phone 10 monitors the state of the IC card 10 (1). When the mobile phone 10 is placed in front of the external reader / writer 30, the external reader / writer 30 designates the card application 21 and instructs its activation (2). When the activation response is received from the card application 21, the external reader / writer 30 performs mutual authentication with the card application 21 (3), and then, together with information on the payment amount presented to the mobile phone 10, the personal authentication password. Request a number (4).

The card application 21 tries to read the personal authentication password from the information passing card application 22, but the information passing card application 22 does not hold the personal authentication password, so the information passing card application 22 writes the name of the terminal application to be activated (middleware 12 in this case), the personal identification number request, the payment amount information, and the card application ID of the request source (5), and the external reader / writer 30 NG is responded to the personal identification number request. Therefore, the settlement process 1 ends with failure.

When the middleware 12 of the mobile phone 10 detects the end of processing of the IC card 10 (6), it instructs the activation of the information passing card application 22 (7). When the activation OK response is received from the information delivery card application 22, the middleware 12 performs mutual authentication with the information delivery card application 22 (8), and then sends an information acquisition command to the information delivery card application 22 (9). Receiving this, the information delivery card application 22 returns a response using the stored information as response data to the middleware 12 (10). The middleware 12 interprets the acquired information (11), displays the payment amount on the display of the mobile phone 10, and displays a PIN input window (12) When the user operates the keypad of the mobile phone 10 and inputs the PIN, the middleware 12 writes the PIN in the information passing card application 22 (13).

When the user again places the mobile phone 10 in front of the external reader / writer 30, the external reader / writer 30 activates the card application 21 (14), performs mutual authentication (15), and then presents the payment amount. Then, a personal identification password is requested (16) The card application 21 accesses the information delivery card application 22, reads the PIN stored therein (17), includes the PIN information in the OK response to the personal authentication password request, and the external reader / writer 30. (18). This PIN verification is performed at a center connected to the external reader / writer 30, and when the verification is successful, a settlement process is executed, and a processing end notification is sent from the external reader / writer 30 to the card application 21 (19). Thus, the settlement process 2 is completed successfully.

The PIN writing (13) by the middleware 12 is directly performed on the requesting card application 21 as shown in FIG. 3 based on the requesting card application ID included in the information acquired from the information passing card application 22. You may make it do. In this case, the card application 21 immediately transmits a PIN to the external reader / writer 30 without accessing the information passing card application 22 in response to the personal identification number request (16) of the external reader / writer 30. (18).

FIG. 4 shows a processing flow in the case where the electronic value is charged from the external server to the IC card 20 in which the amount necessary for settlement is not accumulated. The middleware 12 of the mobile phone 10 monitors the state of the IC card 10 (20). When the mobile phone 10 is placed in front of the external reader / writer 30, the external reader / writer 30 designates the card application 21 and instructs its activation (21). When the activation response is received from the card application 21, the external reader / writer 30 performs mutual authentication with the card application 21 (22) and then presents the settlement amount (23). Since the amount necessary for the payment is not charged in the IC card 20, when the card application 21 responds NG, the external reader / writer 30 receives the terminal application (charge application) that performs the deposit process to the IC card 20. The activation is requested (24).
The card application 21 writes the terminal application name to be activated, the charge request, and the card application ID of the request source in the information passing card application 22 (25), and in response to the charge application activation request of the external reader / writer 30 Reply OK. In this way, the payment process ends in failure.

When the middleware 12 of the mobile phone 10 detects the end of the processing of the IC card 10 (26), it instructs the activation of the information passing card application 22 (27). When the activation OK response is received from the information delivery card application 22, the middleware 12 performs mutual authentication with the information delivery card application 22 (28), and then sends an information acquisition command to the information delivery card application 22 (29). Receiving this, the information delivery card application 22 returns a response using the stored information as response data to the middleware 12 (30). The middleware 12 interprets the acquired information (31), activates the designated terminal application (charge application) 11, and instructs charge processing to the requesting card application (32).
The activated terminal application 11 uses the communication function of the mobile phone 10 to connect to an external server that charges the IC card 10 and conveys necessary information (33). The external server instructs activation of the request source card application 21 of the IC card 20 (34). When there is a response of activation OK from the request source card application 21, the external server performs mutual authentication with the request source card application 21 (35), then writes an electronic value in the request source card application 21 (36), and remote charge The process ends.

In addition, when a mobile phone equipped with an IC card passes through an automatic ticket gate, the external reader / writer of the automatic ticket gate passes train delay information to the iC card, and this delay information is displayed on the mobile phone display. It can also be displayed on the screen.

In order to save the user's trouble of instructing the start of polling processing, card status monitoring polling for monitoring entry and exit from an electromagnetic field capable of non-contact communication may be constantly performed. FIG. 5 shows a processing flow when the middleware 12 always performs card status monitoring polling through the device driver 13. By constantly monitoring the card status, the middleware 12 can acquire and interpret information from the information delivery card application 22 as soon as the non-contact communication processing of the IC card 10 is completed.

Further, while the middleware 12 that has detected the end of the non-contact communication process reads out information from the information passing card application and executes interpretation, another card application 21 is activated from the external reader / writer 30. It is conceivable that processing is performed and information is written in the information delivery card application 22, or the same card application is activated again to perform processing and information is written in the information delivery card application 22. At this time, since the mobile phone 10 is reading the first information and is interpreting the information, confusion may occur. In order to avoid this, there are the following two measures (a) and (b).

(A) When there is one data input area (buffer) in the information storage unit 23, the information delivery card application 22 includes a flag indicating "middleware is processing", and the middleware 12 receives information from the information delivery card application 22. When reading, this flag is set. When this flag is set, the card application 21 that has requested information writing receives a notification of information writing failure from the information delivery card application 22.

(B) When a plurality of data input areas (buffers) of the information storage unit 23 are provided, the information delivery card application 22 includes an area indicating the data area number being processed by the middleware 12, and an information delivery card When the application 22 receives a request for writing information from the card application 21, the application 22 refers to this area and writes information in the area of the number next to the number of the area being processed by the middleware 12. On the other hand, the middleware 12 sequentially interprets and processes the information written in each area.

As described above, in this device, the convenience, operability and functionality of the IC card can be improved by using the terminal application installed in the mobile phone, the keypad, display, communication function, etc. of the mobile phone. A more advanced service can be realized with a general-purpose IC card conforming to international standards.
Although the case where the IC card is attached to the mobile phone has been described here, the present invention is not limited to this. Various information processing apparatuses such as a PDA (Personal Digital Assistant), a mail terminal, a small personal computer, and a game machine can be used instead of the mobile phone. In addition, any IC card can be used as long as it is a secure device capable of operating a card application in response to an APDU format command. The shape of the secure device may be a card shape or a chip shape, and may be embedded in the information processing apparatus.

(Second Embodiment)
In the second embodiment of the present invention, a case where the middleware reads out, displays, interprets, and processes the information written in the information delivery card application by the card application that has performed contactless communication processing when it is instructed by the user will be described. To do. Therefore, the user can check the information written in the information delivery card application at an arbitrary timing, and can omit the check if it is not necessary.

The configuration of the mobile phone and IC card in this case is shown in FIG. The structural blocks of the mobile phone 10 and the IC card 20 are the same as those in the first embodiment (FIG. 1).
In FIG. 6, the order of processing by the three parties of the mobile phone 10, the IC card 20, and the external reader / writer 30 is indicated by a circled number. When the user places the mobile phone 10 over the external reader / writer 30, the IC card 20 is activated, and the card application 21 designated by the external reader / writer 30 executes the processing instructed by the external reader / writer 30. (1). The card application 21 writes information necessary to be sent to the mobile phone 10 in accordance with this processing to the information delivery card application 22 (2).
This information includes the name of the terminal application (including middleware) to be activated, information to be transferred to the terminal application, the ID of the requested card application, and the like.

The user who wants to check the non-contact communication processing result performs an operation such as shaking the mobile phone 10 to instruct the start of processing at an arbitrary time (3). In response to this, the middleware 12 performs mutual authentication with the information delivery card application 22, and then accesses the information delivery card application 22 to obtain information held therein (4). The middleware 12 activates the designated terminal application 11 based on the information acquired from the information delivery card application 22, and the terminal application 11 performs the designated processing. When the middleware 12 is designated, the middleware 12 itself performs the process (5).

As shown in FIG. 7, the information storage unit 23 managed by the information transfer card application 22 of the IC card 20 has a single data input area (buffer) (a) and a plurality of data input areas (here, 3). (B). When (a) has one data input area (buffer), it is always overwritten and used. Therefore, only the latest contactless communication processing information is stored in the information storage unit 23, and when the user performs an operation to check the contactless communication processing result, the latest contactless communication processing result is displayed. The
When there are a plurality of data input areas (buffers) (b), the plurality of data input areas are used while being sequentially circulated, and the latest non-contact communication processing information is overwritten in order in these data input areas. In addition, a number indicating a data input area in which information on the latest contactless communication processing is written is stored.
Therefore, in this case, it is possible to display, interpret, and process the results from the latest non-contact communication process to the non-contact communication process that goes back by the past n (n is the number of data input areas). The display operation at this time goes back in time for each user instruction so that the latest processing result is displayed by the user's display instruction, and one past processing result is displayed by the next user's display instruction. Alternatively, all the processing results stored in the information storage unit 23 may be displayed at a time according to a user display instruction.

FIG. 8 shows the process of FIG. 4 in the first embodiment (the process in the case where electronic value is charged from an external server to the IC card 20 in which the amount required for payment is not accumulated) according to the second embodiment. Shows a processing flow in the case of the above. Here, the settlement

processing performed by placing the mobile phone 10 in front of the external reader / writer 30 and the subsequent processing are performed independently, and the subsequent processing is started in response to a user instruction

As described above, in the method of the second embodiment, the information written in the information storage unit 23 of the card application 22 for information transfer by the card application 21 is the middleware triggered by the user's instruction after the contactless communication process is completed. 12 is read, interpreted, and processed. The user can select whether to perform this process. Therefore, unlike the first embodiment, a prior state monitoring instruction by the user is unnecessary, and convenience is improved.

Further, in this case, the IC card 20 is provided with an information transfer card application 22, and the middleware 12 of the mobile phone 10 accesses the information transfer card application 22 and acquires information written by each card application 21. With this configuration, the middleware 12 can efficiently acquire information from each card application 21 without knowing the access method and authentication method for each card application 21.

The secure device and information processing apparatus of the present invention should be used in the field of using various card functions such as payment cards, transportation commuter pass and boarding tickets, theater admission tickets, medical cards, government-issued cards, etc. Can do.

The block diagram which shows the structure of the mobile telephone and IC card in the 1st Embodiment of this invention FIG. 6 is a sequence diagram showing a first cooperative operation of the mobile phone, IC card, and external reader / writer in the first embodiment of the present invention (when prompting the user to input a PIN) FIG. 7 is a sequence diagram showing a second cooperative operation of the mobile phone, IC card, and external reader / writer in the first embodiment of the present invention (when prompting the user to input a PIN) FIG. 6 is a sequence diagram showing a third cooperative operation of the mobile phone, IC card, and external reader / writer in the first embodiment of the present invention (when a charge application is activated). FIG. 3 is a sequence diagram showing a cooperative operation of a mobile phone, an IC card, and an external reader / writer in the first embodiment of the present invention (when state monitoring polling is always performed) The block diagram which shows the structure of the mobile telephone and IC card in the 2nd Embodiment of this invention The figure which shows the structure of the information storage part of the IC card in the 2nd Embodiment of this invention. The sequence diagram which shows the operation | movement of the mobile telephone in a 2nd Embodiment of this invention, an IC card, and an external reader / writer

Explanation of symbols

DESCRIPTION OF SYMBOLS 10 Mobile phone 11 Terminal application 12 Middleware 13 Device driver 20 IC card 21 Card application 22 Information passing card application 23 Information storage unit 24 Card OS
30 External reader / writer

Patent Citations (10)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
WO1995004328A1 *	1993-07-30	1995-02-09	Intellect Australia Pty. Ltd.	Device and method for ic cards
FI990710 *	1995-02-15	1997-09-25	Nokia Mobile Phones Ltd	Procedure for use of applications in a mobile telephone as well as a mobile telephone
CA2239985C *	1995-12-08	2002-05-14	Amsc Subsidiary Corporation	Mobile communications terminal for satellite communications system
US7181731B2 *	2000-09-01	2007-02-20	Op40, Inc.	Method, system, and structure for distributing and executing software and data on different network and computer devices, platforms, and environments
JP2003060748A *	2001-08-15	2003-02-28	Sony Corp	Portable terminal device and non-contact type ic card module
US7509487B2 *	2003-09-29	2009-03-24	Gemalto Inc	Secure networking using a resource-constrained device
US20050167512A1 *	2003-12-15	2005-08-04	Matsushita Electric Industrial Co., Ltd.	Secure device and information processing apparatus
JP4305847B2 *	2004-03-26	2009-07-29	富士通株式会社	Store settlement method, system and program
JP4628722B2 *	2004-08-19	2011-02-09	富士通株式会社	Collation system and program check method for collation system
US8700729B2 *	2005-01-21	2014-04-15	Robin Dua	Method and apparatus for managing credentials through a wireless network

* Cited by examiner, † Cited by third party

Cited By (22)

Publication number	Priority date	Publication date	Assignee	Title
CN101310254A *	2005-10-17	2008-11-19	法国电信公司	Method and device for managing applications of a mobile terminal
JP2010525620A *	2007-02-12	2010-07-22	オベルトゥル テクノロジ	Method and apparatus for controlling execution of at least one function in a short-range wireless communication module of a mobile telephone
JP2018046564A *	2017-10-18	2018-03-22	フェリカネットワー	Information processing device

			クス株式会社	

Family To Family Citations

US20050269401A1 *	2004-06-03	2005-12-08	Tyfone, Inc.	System and method for securing financial transactions
WO2005119607A2 *	2004-06-03	2005-12-15	Tyfone, Inc.	System and method for securing financial transactions
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
US20060226217A1 *	2005-04-07	2006-10-12	Tyfone, Inc.	Sleeve for electronic transaction card
JP4435076B2 *	2005-11-16	2010-03-17	フェリカネットワークス株式会社	Mobile terminal, data communication method, and computer program
US7991158B2	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
US20080244208A1 *	2007-03-30	2008-10-02	Narendra Siva G	Memory card hidden command protocol
WO2009038511A1 *	2007-09-21	2009-03-26	Telefonaktiebolaget Lm Ericsson (Publ)	All in one card
US9741027B2 *	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US8345122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
EP2401708A4 *	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
US20110076946A1 *	2009-08-20	2011-03-31	Deutsche Telekom Ag	Method, mobile terminal, transponder device and system for monitoring an object with respect to the mobile terminal
US9390256B2 *	2012-03-06	2016-07-12	Paypal, Inc.	System and methods for secure entry of a personal identification number (PIN)
US10888940B1	2019-12-20	2021-01-12	Capital One Services, Llc	Systems and methods for saw tooth milling to prevent chip fraud
US10817768B1	2019-12-20	2020-10-27	Capital One Services, Llc	Systems and methods for preventing chip fraud by inserts in chip pocket
US10977539B1	2019-12-20	2021-04-13	Capital One Services, Llc	Systems and methods for use of capacitive member to prevent chip fraud
US11049822B1	2019-12-20	2021-06-29	Capital One Services, Llc	Systems and methods for the use of fraud prevention fluid to prevent chip fraud
US10810475B1	2019-12-20	2020-10-20	Capital One Services, Llc	Systems and methods for overmolding a card to prevent chip fraud

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
JP2005202914A	2005-07-28	Secure device and information processor
US7340276B2	2008-03-04	System for downloading program to general-purpose subscriber identification module
JP4763332B2	2011-08-31	Mobile terminal device, contactless card function management system, and contactless card function acquisition system
EP2294834B1	2014-11-05	A method for application selection in a wireless mobile communication device in an nfc system and a corresponding wireless mobile communication device
EP2211480A1	2010-07-28	Wireless communication device for providing at least one near field communication service
EP1553530A1	2005-07-13	A secure device and information processing apparatus
JPWO2005059816A1	2007-07-12	Information display method, portable information device, and contactless communication device
US8700827B2	2014-04-15	Matching method, system and device for data exchange between a communication object and a processing unit
KR100971896B1	2010-07-23	Communication terminal, user data transferring system and user data transferring method
US20020016186A1	2002-02-07	Mobile phone
EP2620897A1	2013-07-31	Method, device and system for displaying radio frequency identification application information
WO2007026423A1	2007-03-08	Ic module and mobile communication terminal incorporating ic module

US11055696B2	2021-07-06	Portable terminal, terminal function management system, terminal function management method, terminal function management program, and computer-readable recording medium upon which said program has been recorded
JP2005346611A	2005-12-15	Secure device and information processor
EP1860605A1	2007-11-28	Electronic money system, information storage medium, and mobile terminal device
JP4764670B2	2011-09-07	Non-contact transmission / reception system and portable information terminal
JP2005174185A	2005-06-30	Security device and information processor
JP2005174215A	2005-06-30	Security device, information processor, and terminal device
JP6397208B2	2018-09-26	Management server, data processing method, and program
JP5724694B2	2015-05-27	COMMUNICATION DEVICE, COMMUNICATION METHOD, AND COMMUNICATION PROCESSING PROGRAM
US20070110014A1	2007-05-17	Data transfer apparatus, data transferring method, and data transfer program
TWI298851B	2008-07-11	
JP2012141754A	2012-07-26	Ic chip, processing method in ic chip, processing program for ic chip, and portable terminal
WO2013127868A1	2013-09-06	Method for exchanging data between two mobile devices
JP2012529090A	2012-11-15	RF identification device

Priority And Related Applications

Priority Applications (2)

Application	Priority date	Filing date	Title
JP2003416389		2003-12-15	
JP2004168282A	2003-12-15	2004-06-07	Secure device and information processor

Applications Claiming Priority (4)

Application	Filing date	Title
JP2004168282A	2004-06-07	Secure device and information processor
US11/011,641	2004-12-14	Secure device and information processing apparatus
CNA2004101021887A	2004-12-15	A secure device and information processing apparatus
EP04029715A	2004-12-15	A secure device and information processing apparatus

Legal Events

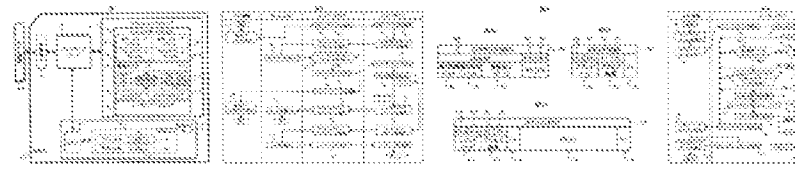
Date	Code	Title	Description
2006-12-15	A621	Written request for application examination	**Free format text**: JAPANESE INTERMEDIATE CODE: A621 **Effective date**: 20061214
2007-06-22	A761	Written withdrawal of application	**Free format text**: JAPANESE INTERMEDIATE CODE: A761 **Effective date**: 20070622

Data provided by IFI CLAIMS Patent Services

Patents JP4322021

Memory card

Images (6)



Classifications

G06F12/00 Accessing, addressing or allocating within memory systems or architectures

View 7 more classifications

JP4322021B2
Japan

Download PDF Find Prior Art Family

Other languages: Japanese

Inventor: 永雅 水島, 元泰 角田, 圀弘 片山

Worldwide applications

2003 JP KR 2004 US

Application JP2003050243A events

2003-02-06 Priority to JP2003028998
2003-02-27 Application filed by 株式会社ルネサステクノロジ
2003-02-27 Priority to JP2003050243A
2004-10-21 Publication of JP2004295160A
2009-08-26 Application granted
2009-08-26 Publication of JP4322021B2
Status Expired - Fee Related
2023-02-27 Anticipated expiration

Info: Patent citations (10), Cited by (50), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (22) Hide Dependent

1. An interface for connecting to an external host device;
Can store a plurality of application programs, and the IC card chip capable of executing the respective application programs,
A non-volatile memory that is divided into a plurality of blocks, and each of the blocks is assigned to each application program, and can store relational data related to each application program;
A controller connected to the interface, the IC card chip, and the nonvolatile memory;
In response to a specific command received from the host device via the interface, the controller sends a first IC card command for the IC card chip to start accessing the nonvolatile memory to the IC card chip. Send
In response to the first IC card command, the IC card chip includes an IC card response including or not including identification information for identifying the application program for the application program selected at that time. To the controller.
The controller includes the identification information when the identification information is included in the IC card response and the block allocated to the application program specified by the identification information exists in the nonvolatile memory. A second IC card command for transferring the relation data between the nonvolatile memory and the IC card chip corresponding to the application program specified by
When the identification information is not included in the IC card response or when the identification information is included in the IC card response and is assigned to the application program specified by the identification information in the nonvolatile memory A memory card that transmits the IC card response to the host device when the block is not present .

2. The memory card according to claim 1 ,
The nonvolatile memory is configured to transfer, for each block, the identification information of the application program assigned to the block, and a transfer command code for transferring the relational data between the nonvolatile memory and the IC card chip. memory card having a management area for storing in association with.

3. The memory card according to claim 2 ,
When storing at least one of said application program in the IC card chip, with respect to the management area of the previous St. nonvolatile memory, the locking function and additional or locking function of inhibiting the deletion of the identification information of the application program A memory card with an unlock function to release.

4. The memory card according to claim 2 or 3 ,
When the controller matches the identification information included in the IC card response from the IC card chip in the identification information stored in the management area of the nonvolatile memory, the IC A memory card that permits transfer of the relationship data between a card chip and the nonvolatile memory.

5. The memory card according to claim 2,
The management area is a memory card whose access is restricted by the controller so that the host device cannot directly read and write data.

6. The memory card according to claim 2,
The IC card chip, the identification information of the application program to be executed the IC card chip sends to the controller by the IC card response,
The controller specifies the transfer command code corresponding to the identification information from the IC card chip among the transfer command codes stored in the management area in the nonvolatile memory, and specifies the specified transfer command sends to the IC card chip to create the second IC card command based on the code,
in response to the second IC card command from the controller, the IC card chip instructs the controller by the IC card response the content of processing corresponding to the second IC card command ,
The controller is a memory card that executes the processing in response to an instruction from the IC card chip.

7. The memory card according to claim 6 ,
Said transfer command code is read out from said nonvolatile data to be written into said block of memory from the IC card chip first for transferring to said controller transfer command, said block of said nonvolatile memory And a second transfer command for transferring the transferred data from the controller to the IC card chip.

8. The memory card according to claim 7 ,
The transfer command code, a memory card different from the commands from the host device.

9. The memory card according to claim 6,
The IC card chip is a memory card that requests the controller to access data in the block in the nonvolatile memory by setting a predetermined value in the IC card response.

10. The memory card according to claim 7,
The IC card chip sets, in the IC card response, an access mode that specifies whether access to the nonvolatile memory is a data write to the block or a data read from the block ...
The controller uses the first transfer command or the second transfer command as the second IC card command based on the value of the access mode set in the IC card response from the IC card chip, Memory card to create.

11. The memory card according to claim 10, wherein
in response to the specific command from the host device, the IC card chip accesses the block in the nonvolatile memory based on the second IC card command created by the controller by the application program, A memory card that is performed multiple times.

12. The memory card according to claim 11,
The controller is a memory card that sets a result of a previous access to the block in the nonvolatile memory in the second IC card command.

13. The memory card according to claim 11,
The IC card chip sets the access mode for the next access to the block in the nonvolatile memory in the IC card response,
The controller determines the access mode that the controller recognizes at the next access from the IC card chip based on the access mode for the next access set in the IC card response from the IC card chip, Memory card to set.

14. The memory card according to claim 2,
Said controller, in response to a first command from said host device, by assigning the right to use of the blocks of the nonvolatile memory before each SL application program to said management area of said nonvolatile memory And adding the identification information of the assigned application program in association with the identifier of the block,
In response to the second command from the host device, the controller prohibits processing in response to the first command from an unlocked state in which processing in response to the first command can be executed Memory card to transition to.

15. The memory card according to claim 14 ,
The nonvolatile memory can store a flag for identifying whether the controller is in the locked state or the unlocked state ,
The controller is a memory card that changes the value of the flag when transitioning from the unlocked state to the locked state.

16. The memory card according to claim 14,
The controller is a memory card that does not permit access to the block in the nonvolatile memory by the application program in the IC card chip when the controller is in the unlocked state.

17. The memory card according to claim 14 ,
The controller is a memory card that makes a transition from the locked state to the unlocked state in response to a third command from the host device.

18. The memory card according to claim 17 ,
The nonvolatile memory can store a reference password for permitting processing in response to the third command,
In response to the second command, the controller sets the reference password in the nonvolatile memory when transitioning from the unlocked state to the locked state, and in response to the third command, when the transition from the locked state to the unlocked state, the transition from the locked state only when said password received from the host device and the reference password of the nonvolatile memory is matched to the unlocked state Memory card to allow .

19. The memory card according to claim 14 ,
in response to the fourth command from the host device, the controller releases the right to use the block allocated for the application program, and the management area in the nonvolatile memory A memory card for deleting the identification information of the application program corresponding to the identifier of the block .

20. The memory card according to claim 19,
When the controller deletes the identification information of the application program for the management area in the nonvolatile memory, the data remaining in the block in the nonvolatile memory allocated to the application program Erase memory card.

21. The memory card according to claim 14 ,
Wherein the nonvolatile memory includes a first area for storing data received from the host device, is divided into a plurality of blocks, and a second area where interest for rights allocated for the application program Having a memory card.

22. The memory card according to claim 21 , wherein
Wherein the controller, the transfer for transmitting said read data to be written into the second area of the nonvolatile memory from the received or the second area from the IC card chip data to the IC card chip A memory card that generates a command code for each application program.

Description

[0001]
BACKGROUND OF THE INVENTION
The present invention relates to a storage device having a security function, a host device into which the storage device can be inserted, and a host device having the storage device, and more particularly to a memory card having a flash memory chip, a controller chip, and an IC card chip.
[0002]
[Prior art]
Patent Document 1 describes a memory card on which an IC module and a large-capacity flash memory are mounted.
[0003]
In Patent Document 2, an execution requirement condition for each application program is stored in an IC card, and if an execution requirement condition is satisfied when a processing request is made, it can be executed, and if it is not satisfied, it is ineffective. It is described.
[0004]
Patent Document 3 describes that among memory areas in an IC card, area A is allocated for a bank and area B is allocated for a hospital.
[0005]
[Patent Document 1]
Japanese Patent Laid-Open No. 10-198776
[Patent Document 2]
JP 2000-66882 A
[Patent Document 3]
JP-A-6-222980
[0006]
[Problems to be solved by the invention]
However, none of the prior arts describe the allocation of divided storage areas for each application program (applet) of the IC card. Therefore, in the prior art, there is a concern that each application program illegally infringes data in each other's memory.
[0007]
An object of the present invention is to improve the safety of processing related to a specific application program by processing data related to the specific application program inside the memory device when executing processing related to the specific application program. A memory device is provided.
[0008]
An object of the present invention is to provide a storage medium capable of suppressing data interference between application programs of an IC card chip, that is, memory allocated to a certain application program is also accessed by other applets and data is not infringed. That is.
[0009]
[Means for Solving the Problems]
The present invention relates to relational data related to an application program between an IC card chip and a non-volatile memory (for example, a flash memory) in response to a specific command received by a controller via an interface (for example, an external terminal) from a host device. Transfer of data (for example, data to be processed by the application program) is executed, and transfer of related data to the host device via the interface is prohibited.
[0010]
In the present invention, the memory is divided into a plurality of blocks, and the right to use the blocks is assigned to each application program of the IC card chip. That is, the memory has a first storage area (for example, a normal data area) for storing data from the host device and a second storage area (for example, a secure data area) for storing data from the IC card chip. In addition, the second storage area is divided into a plurality of blocks, and each block is assigned to each application program.
[0011]
Further, according to the present invention, block usage rights are assigned, deallocated, assignment and deallocation prohibited, and allocation and deallocation prohibition are canceled by commands from the host device. That is, the present invention allocates the right to use a block of memory for each application program in response to a first command (for example, applet registration command) from the host device, and performs a second command (for example, management) from the host device. Transition from the unlocked state to the locked state in response to the table lock command). Further, in response to a third command (for example, management table unlock command) from the host device, the lock state is changed to the unlock state, and the fourth command (for example, applet registration cancellation command) from the host device is changed. In response, the right to use the block allocated for the application program is released.
[0012]
DETAILED DESCRIPTION OF THE INVENTION
Hereinafter, an embodiment of the present invention will be described.
[0013]
FIG. 1 is a simplified representation of the internal configuration of MultiMediaCard to which the present invention is applied (MultiMediaCard is a registered trademark of Infineon Technologies AG, hereinafter abbreviated as "MMC"). The MMC 110 preferably conforms to the MultiMediaCard specification. The MMC 110 has a storage function that allows the host device 160 connected to the outside to issue a memory card command that conforms to the MultiMediaCard protocol specifications, and a storage function that can read and write file data, as well as encryption necessary for confidential data protection and personal authentication. It has a security processing function that can perform calculations. The host device 160 corresponds to, for example, a mobile phone, a personal digital assistant (PDA), a personal computer, a music playback (and recording) device, a camera, a video camera, an automatic deposit deposit machine, a street corner terminal, a payment terminal, and the like. The MMC 110 has an MMC external terminal 140, a controller chip 120, a flash memory chip 130, and an IC card chip 150. The flash memory chip 130 is a large-capacity (for example, 64 megabyte) memory chip using a nonvolatile semiconductor memory as a storage medium, and data can be read and written by a flash memory command. The MMC external terminal 140 includes seven terminals and includes a power supply terminal, a clock input terminal, a command input / output terminal, a data input / output terminal, and a ground terminal for exchanging information with the external host device 160. The controller chip 120 is connected to other components (MMC external terminal 140, flash memory chip 130, IC card chip 150) inside the MMC 110, and is a microcomputer chip that controls them. The IC card chip 150 is a microcomputer chip that is embedded in a plastic substrate of the IC card, and its external terminals, electrical signal protocol, and commands are

compliant with ISO / IEC7816 standards. The external terminals of the IC card chip 150 include a power supply terminal, a clock input terminal, a reset input terminal, an I / O input / output terminal, and a ground terminal. With respect to the external terminals of the IC card chip 150, a power supply terminal, a clock input terminal, a reset input terminal, and an I / O input / output terminal are connected to the controller chip 120 except for the ground terminal. The controller chip 120 issues an IC card command from the external terminal of the IC card chip 150 to the IC card chip 150, thereby performing an operation necessary for security processing requested from the external host device 160. The IC card chip 150 includes a CPU 151 for performing arithmetic processing and an EEPROM (Electrically Erasable Programmable Read Only Memory) 152. On the other hand, the flash memory chip 130 includes a storage element, but does not include a microcomputer.

[0014]

The security processing is executed by the CPU 151 when data is written to the EEPROM 152 in the IC card chip 150 or when data is read from the EEPROM 152, for example. The detailed contents of the security processing are described by program codes stored in the EEPROM 152. The program code is configured as a plurality of functionally different modules so that it can be applied to various security processes. The CPU 151 can switch a module used for security processing as necessary. Hereinafter, this module unit is called an applet. For example, the EEPROM 152 stores an applet A153 and an applet B154. Each applet in the IC card owns its own application identifier (hereinafter referred to as AID (Application IDentifier)). In FIG. 1, the AID of applet A 153 is shown as 155 and the AID of applet B 154 is shown as 156. These AIDs are preferably values uniquely assigned internationally in order to identify the application program of the IC card. An internationally distributed AID numbering method is defined by ISO / IEC 7816-5 as an international standard. The storage capacity of the EEPROM 152 is, for example, 64 kilobytes, which is smaller than the storage capacity of the flash memory chip 130. However, when implementing the present invention, the storage capacity of the EEPROM 152 may be the same as or larger than the storage capacity of the flash memory chip 130.

[0015]

For the IC card chip 150, a product that has been certified by an evaluation / certification organization of ISO / IEC15408, which is an international standard for security evaluation standards, is used. Generally, when an IC card having a security processing function is used in an actual electronic payment service or the like, the IC card needs to be evaluated and certified by an ISO / IEC 15408 evaluation / certification organization. When the MMC 110 is realized by adding a security processing function to the MMC and used in an actual electronic payment service, etc., the MMC 110 also needs to be evaluated and certified by the ISO / IEC15408 evaluation / certification organization. is there. The MMC 110 has a built-in IC card chip 150 that has been authenticated by the evaluation / certification organization, and has a structure for performing security processing using the IC card chip 150, thereby obtaining a security processing function. Therefore, the MMC 110 can easily satisfy the security evaluation standard based on ISO / IEC15408, and the development period for adding the security processing function to the MMC can be shortened.

[0016]

The MMC 110 preferably has an external interface compliant with the MultiMediaCard specification. The MMC 110 accepts a command (hereinafter referred to as a secure write command) for executing security processing in addition to a standard memory card command conforming to the MultiMediaCard specification through one type of external interface. The secure write command is accompanied by input data. The controller chip 120 has a function of selecting a chip to be accessed and distributing command processing depending on whether the command received by the MMC 110 is a standard memory card command or a secure write command. When the standard memory card command is received, the flash memory chip 130 is selected and the flash memory command is issued to the host memory data. If a secure write command is received, the IC card chip 150 can be selected, and an IC card command can be issued to the security card to execute security processing. The IC card command issued here is embedded in data input by the secure write command (hereinafter referred to as secure write data). The IC card chip 150 returns an IC card response in response to this command, but the controller chip 120 caches it. Further, the MMC 110 also accepts a command (hereinafter referred to as a secure read command) for reading the result of security processing through one type of external interface. The secure read command is accompanied by output data. When the secure read command is received, the cached data including the IC card response (hereinafter referred to as secure read data) is output.

[0017]

FIG. 2 is a flowchart conceptually showing the operation of the MMC 110 to which the present invention is applied. The operation will be described below with reference to FIG. When the host device 160 transmits a secure write command to the MMC 110 (201), the controller chip 120 transmits an IC card command to the IC card chip 150 (202). When receiving the IC card command (203), the IC card chip 150 returns an IC card response including the AID of the applet selected at that time to the controller chip 120 (204). When the controller chip 120 receives the IC card response, a read command is transmitted to the flash memory chip 130 (205). As a result, the flash memory chip 130 reads the list of AIDs (assumed to be written in advance) (206) and outputs it to the controller chip 120. The controller chip 120 searches the list for a match with the AID from the IC card chip 150 (207). If a matching AID cannot be detected, a secure read command is received from the host device 160 and an IC card response is transmitted as secure read data (219), and the host device 160 receives it (220). On the other hand, if an AID is detected in step 207, the IC card response is prohibited from being output to the host device 160 and an IC card command is transmitted to the IC card chip 150 (208). When the IC card chip 150 receives this IC card command (209), since the selected applet transfers data between the IC card chip 150 and the flash memory chip 130, the IC card corresponding to the data transfer direction is used. Create a response. If it is desired to transfer from the IC card to the flash, an IC card response including the data to be written to the flash memory and its address is created and returned (211). If it is desired to transfer from the flash to the IC card, an IC card response including the address to be read from the flash memory is created and returned (214). After step 211, the controller chip 120 transmits a write command to the flash memory chip 130 (212). On the other hand, the flash memory chip 130 writes data to the designated address (213). Thereby, the data transfer from the IC card to the flash is completed. On the other hand, after step 214, the controller chip 120 transmits a read command to the flash memory chip 130 (215). On the other hand, the flash memory chip 130 reads data from the designated address (216) and outputs it to the controller chip 120. Controller chip 120. The read data is transmitted to the IC card chip 150 by an IC card command (217), and the IC card chip 150 receives this (218). Thereby, the data transfer from the flash to the IC card is completed. FIG. 6 shows an example of the format of secure write data and secure read data. This format is preferably applied when the contents of the security processing to be executed can be expressed by one IC card command and the result of the security processing can be expressed by one IC card response. As described above, both the IC card command transmitted to the IC card chip 150 and the IC card response received from the IC card chip 150 conform to the ISO / IEC7816-4 standard. According to this standard, a 4-byte header (class byte CLA, instruction byte INS, parameter bytes P1 and P2) is indispensable for the configuration of the IC card command. If necessary, the input data length instruction byte Lc, the input A data field DataIn and an output data length instruction byte Le follow. Further, the configuration of the IC card response requires the 2-byte status SW1 and SW2, and the output data field DataOut is placed in front of the status if necessary. The secure write data 601 in this format is obtained by adding an IC card command length Lca 604 before the IC card command 602 and padding dummy data 605 after the IC card command 602. The value of Lca 604 is a total value of the lengths of the components of the IC card command 602. On the other hand, the secure read data 611 is obtained by adding the IC card response length Lra 614 before the IC card response 612 and padding dummy data 615 after the IC card response 612. The value of Lra 614 is a total value of the lengths of the components of the IC card response 612. In this figure, an example of a format in which Lc, DataIn, and Le are included in the IC card command and DataOut is included in the IC card response is shown. In the specification of the data read / write command included in the standard memory card command for the MMC 110, it is fundamental to process data to be read / written in units of fixed length blocks. Therefore, it is preferable that the sizes of the secure write data 601 and the secure read data 611 also match the block size conforming to the standard memory card command specification of the MMC 110. The dummy data 605 and 615 are applied to make the sizes of the secure write data 601 and the secure read data 611 coincide with the block size. The value adopted as the block size is preferably the sector size (512 bytes) in the FAT method adopted by a general small memory card in the logical file system. The dummy data 605 and 615 to be padded may be all zero, random numbers, or a checksum for the controller chip 120 or the host device 160 to detect or correct a data error. The Lca 604 value is used by the controller chip 120 to remove the dummy data 605 from the secure write data 601 and extract the IC card command 602, and the Lra 614 value is used by the host device 160 to remove the dummy data 615 from the secure read data 611. And used to extract the IC card response 612.

[0018]

The controller chip 120 controls power supply and clock supply to the IC card chip 150 through a power supply terminal and a clock input terminal. When security processing is not requested from the host device 160, power supply and clock supply to the IC card chip 150 can be stopped, and power consumption of the MMC 110

can be reduced.

[0019]

In order to make the IC card chip 150 that is not supplied with power ready to receive an IC card command, it is first necessary to start supplying power to the IC card chip 150 and perform a reset process. The controller chip 120 has a function of starting power supply to the IC card chip 150 through the power supply terminal when the MMC 110 receives the secure write command from the host device 160. The controller chip 120 also has a function of resetting the IC card chip 150 through a reset input terminal when the MMC 110 receives a secure write command from the host device 160. The controller chip 120 can stop power supply to the IC card chip 150 until a secure write command is received. Therefore, the power consumption of the MMC 110 can be reduced.

[0020]

The controller chip 120 has a function of generating a clock signal to be supplied to the IC card chip 150 through the clock input terminal of the IC card chip 150 inside the MMC 110 and controlling the frequency, supply start timing, and supply stop timing. Since it can be made independent of the clock signal at the clock input terminal of the MMC external terminal 140, security is improved against attack methods called timing analysis, power difference analysis, and failure use analysis by the host device 160.

[0021]

The flash memory chip 130 includes a normal data area 131, a management area 132, and a secure data area 133.

[0022]

The normal data area 131 is an area where logical addresses are mapped in sector units, and is an area where the host device 160 can read and write data at logical addresses designated by using standard memory card commands.

[0023]

The secure data area 133 stores data to be handled when the CPU 151 executes an applet (for example, 153 or 154) stored in the EEPROM 152 in the IC card chip 150 (that is, when security processing is executed). This is an area where The secure data area 133 is divided into a plurality of blocks. This is called a secure data block. For example, the secure data area 133 is composed of four secure data blocks 133a, 133b, 133c, and 133d. The secure data block is a unit in which the controller chip 120 can assign the usage right for each applet. For example, applet A153 has the right to use secure data block c133c, and applet B154 has the right to use secure data block a133a. Each secure data block is divided into a plurality of fixed length data records. For example, the size of one record is 128 bytes and is composed of 8192 records per secure data block. At this time, the size of one secure data block is 1 megabyte, and the capacity of the secure data area 133 is 4 megabytes. Therefore, the applet stored in the EEPROM 152 can use non-volatile data exceeding the capacity of the EEPROM 152 by accessing the data stored in the secure data area 133. For example, when the applet A 153 in the IC card chip 150 is a program for security processing related to electronic payment, the payment log (payment amount, date and time) is stored in the secure data area 133, so that only the EEPROM 152 is used. In addition, many settlement logs can be stored, which increases the convenience for the user. Access (write or read) from the IC card chip 150 to the secure data area 133 is executed by the controller chip 120 based on a request from the IC card chip 150. The condition for generating the request is arbitrary for the IC card applet. . For example, the capacity of the EEPROM 152 has fallen below a certain threshold value (hence, it must be recorded outside the card), the data in the IC card chip does not meet some protection standard (thus, even if it is recorded outside the card) There is no problem), and the desired data is not found in the EEPROM 152 (hence, reading from the outside of the card) A detailed procedure for accessing the secure data area 133 from the IC card chip 150 will be described later.

[0024]

On the other hand, the management area 132 is an area for storing information for the controller chip 120 to manage the secure data area 133. The controller chip 120 stores or deletes information in this area when the MMC 110 receives a secure write command from the host device 160. The command will be described later. The management area 132 includes a lock flag 134, a password area 135, and a management table 136.

[0025]

The management table 136 is an area for registering applets having the right to use each secure data block constituting the secure data area 133. In order to identify the applet, it is desirable to register the applet by storing the AID in this area. By using the AID, an applet that uses the secure data area 133 can be reliably identified. The controller chip 120 prohibits storing a plurality of identical AIDs in the AID 137. In the block column of the management table 136, the head address value of the block is registered as a block identifier for identifying the secure data block. However, a unique number in the MMC may be registered as a block identifier instead of the head address value. Instead of the management table 136, AID may be registered directly in each secure data block).

[0026]

In the management table 136, not only the AID 137 but also a transfer command code 138 can be stored for each applet. This transfer command code 138 is preferably generated by the controller chip 120 when the controller chip 120 assigns the right to use the secure data block for the applet. The transfer command code is a value of 2 bytes × 2 set in the CLA byte and INS byte of the command APDU (Application Protocol Data Unit) of each of the "write transfer command" and the "read transfer command". Here, the "write transfer command" and the "read transfer command" refer to between the controller chip 120 and the IC card chip 150 before the record data is written to the secure data area 133 or after the record data is read therefrom. In order to transfer the record data, the controller chip 120 issues an IC card command format command to the IC card chip 150. In particular, a command for sending record data to the controller chip 120 is called a write transfer command, and a command for sending record data to the IC card chip 150 is called a read transfer command. Detailed description of these commands will be described later. The applet (153 or 154) having the right to use the secure data area 133 describes a processing program that handles record data when a write / read transfer command is received. The transfer command code 138 is individually determined for each applet. If the transfer command code is a fixed value common to all applets, a coding conflict occurs between the applet-specific command included in the secure write data from the host device 160 and the write / read transfer command. there is a possibility. According to the present invention, such coding competition can be prevented. Note that the INS code of the transfer command code 138 must conform to ISO / IEC7816-3 for the convenience of the transmission protocol.

[0027]

The lock flag 134 is an area for storing 1-byte data indicating whether or not the registration information stored in the management table 136 can be changed. Setting FFh in this area indicates that the change of information in the management table 136 is prohibited (locked). Also, setting 00h indicates that the change of information in the management table 136 is permitted (unlocked).

[0028]

The password area 135 is an area for storing a 255-byte password reference value for unlocking the information in the management table 136. When the information in the management table 136 is locked, a 255-byte password reference is set in this area by a secure write command from the host device 160. When the information in the management table 136 is set to the unlocked state, it is necessary to input the same password as the password reference set at the time of locking by the secure write command from the host device 160. The change of the information in the management table 136 can be unlocked by matching the input password with the password reference.

[0029]

The management area 132 is physically restricted by the controller chip 120 so that the host device 160 cannot illegally access and analyze the security processing. That is, since the management area 132 is not assigned a logical address by the controller chip 120, the host device 160 cannot directly read or write data. Therefore, the reliability and safety of the security processing of the MMC 110 are improved.

[0030]

Hereinafter, the command APDU and the response APDU of the write / read transfer command used in the record data write / read access to the secure data area 133 will be described in detail with reference to FIG.

[0031]

FIG. 2 a shows a response APDU output from the IC card chip 150. By setting special values in the first two bytes (hereinafter referred to as the first control byte 301 and the second control byte 302 in order from the beginning) of the DataOut 304 included in the response APDU 300, and the SW1 byte 305 and the SW2 byte 306. The IC card chip 150 can notify the controller chip 120 of an access request for the secure data area 133. Note that the subsequent output data 303 (a portion of the DataOut 304 excluding the first control byte 301 and the second control byte 302) is used for transmitting information necessary for the access request.

[0032]

Since the IC card chip 150 requests the controller chip 120 to access the secure data area 133, a dedicated status value of 90FFh must be set in the SW1 byte 305 and the SW2 byte 306. When the controller chip 120 constantly monitors the response APDU output from the IC card chip 150 and detects that the values of the SW1 byte 305 and the SW2 byte 306 are 90FFh, the first control byte 301 and the first control byte 301 of the DataOut 304 in front of the controller chip 120 are detected. 2 Control byte 302 First control byte The second control byte is examined, and the contents of the requested access are recognized. On the other hand, if it is not 90FFh, secure read data including the response APDU is output to the host device 160. However, even if the values of the SW1 byte 305 and the SW2 byte 306 are 90FFh, they may be output to the host device 160 as they are depending on conditions. Details thereof will be described later.

[0033]

When starting access to the secure data area 133, the controller chip 120 selects a secure data block to be activated from 133a to 133d depending on what applet is selected on the IC card chip 150. The secure data block to be accessed is selected immediately after an access start request is generated from the IC card chip 150. The specification of data set in DataOut 304 for the access start request is shown below. In the upper 4 bits of the first control byte 301, 0001 is set. In the lower 4 bits of the first control byte 301, a code indicating the access mode is set. There are two types of access modes that can be specified here: record data write and record data read. The code 0001 is a record data write, and the code 0010 is a record data read. Other codes are invalid. In the subsequent output data 303, the AID of the applet selected on the IC card chip 150 is set. For example, AID 155 is set when applet A153 is selected, and AID 156 is set when applet B154 is selected. In the second control byte 302, the length of the AID is set

[0034]

If the upper 4 bits of the first control byte are 0001, the controller chip 120 searches all the AIDs 137 in the management table 136 with the AID included in the subsequent output data 303 and determines the secure data block to be activated. If no matching AID is found, secure read data including the response APDU is output to the host device 160. After detecting the AID and determining the corresponding secure data block, the controller chip 120 recognizes that the write access is started if the lower 4 bits of the first control byte are 0001 and the read access is started if 0010. When the lower 4 bits of the first control byte are other than that, the secure read data including the response APDU is output to the host device 160.

[0035]

After the controller chip 120 recognizes the access mode (write or read), the record data to be written to the active secure data block or the read record data is issued by issuing a write / read transfer command according to the mode. Can be transferred between the IC card chip 150 and the controller chip 120. 3b and 3c show the command APDU of the write / read transfer command. FIG. 3b shows the case where there is no transfer data from the controller chip 120 to the IC card chip 150, and FIG. 3c shows the case where there is transfer data. As described above, the CLA byte 314 (or 326) and INS code 315 (or 327) of the command APDU 310 (or 320) of the write / read transfer command are set in advance for each applet. Therefore, 2 bytes × 2 transfer command codes 138 are read from the management table 136.

[0036]

In the command / APDU 310 (or 320) of the write / read transfer command, a special value is set in the P1 byte 316 (or 328) and the P2 byte 317 (or 329) in order to notify the IC card chip 150 of the result of the previous access. To do. 0000h means that there is no error in the previous access. 80XXh means that an error has occurred in the previous access. Note that XX is a hexadecimal code indicating the error content. In case of an error, no data access to the active secure data block is performed. Therefore, the contents of the record data of the secure data block are not changed.

[0037]

The IC card chip 150 transmits the record number and record data to be written or the record number to be read to the controller chip 120 using the subsequent output data 303 in the response APDU 300 of the write / read transfer command. In the write mode, concatenated data of a specified record number (4 bytes) and write data (128 bytes) is set, and in the read mode, a specified record number (4 bytes) is set. Thus, since the length of the subsequent output data 303 varies depending on the access mode, it is necessary to set a value corresponding to the access mode in the Le byte 313 (or 325) of the command APDU of the write / read transfer command. In the write mode, since the length of the subsequent output data 303 is 84h, the length of the DataOut 304 is 86h. Therefore, 86h is set in the Le byte 313 (or 325). In the read mode, the length of the subsequent output data 303 is 04h, so the length of the DataOut 304 is 06h. Therefore, 06h is set in the Le byte 313 (or 325).

[0038]

The command APDU of the write / read transfer command immediately after the start of access (that is, issued first) is in the format of FIG. 3b. At this time, 0000h is set in the P1 byte 316 and the P2 byte 317. In the Le byte 313, 86h is set in the write mode, and 06h is set in the read mode.

[0039]

The write / read transfer command response APDU takes the form of FIG. The applet selected on the IC card chip 150 can request the controller chip 120 to access (write / read) the active secure data block using the response APDU 300. Hereinafter, this is called an access execution request. The specification of data set in the first control byte 301 and the second control byte 302 is shown below. 0010 is set in the upper 4 bits of the first control byte 301. In the lower 4 bits of the first control byte 301, a code indicating the requested access is set. The code 0001 is a record data write, and the code 0010 is a record data read. Other codes are invalid. The access mode represented by this code must match the access mode allowed by the controller chip 120. Further, the next access mode (write / read) can be requested by the second control byte 302. The controller chip 120 refers to this and switches the access mode that it recognizes.

[0040]

If the upper 4 bits of the first control byte 301 are 0010, the controller chip 120 writes / reads the data of the designated record number to the active secure data block When the write / read processing is normally completed (the value of the access result 312 (or 322) is 0000h), the access mode recognized by itself is switched to the write mode if the second control byte 302 is 01h, and the read mode is switched if it is 02h. To do. If there is any error in the write / read process (the value of the access result 312 (or 322) is 80XXh), the access mode at the time when the error occurs is maintained without switching the access mode recognized by itself.

[0041]

The command / APDU of the write / read transfer command issued by the controller chip 120 for the second time or later may take the form of FIG. 3b or the form of FIG. 3c depending on the result of the previous access or the state transition of the access mode. The value of Le313 (or 325) also changes. Details are shown below.

[0042]

When the previous write access is normal and the next time the write mode is used, the format is as shown in FIG.

[0043]

When the immediately preceding write access is normal and the next time is in the read mode, the format is as shown in FIG.

[0044]

When the previous read access is normal and the next time in the read mode, the format is as shown in FIG. 3c, the access result 322 value is 0000h, the Lc323 value is 80h, and the read record data is set in the DataIn 324. The value is 06h.

[0045]

When the previous read access is normal and the next is the write mode, the format is as shown in FIG. 3c, the access result 322 value is 0000h, the Lc323 value is 80h, and the read record data is set in the DataIn 324. The value is 86h.

[0046]

When the previous write access is an error, it is in the format of FIG. 3b, the access result 312 value is 80XXh, and the Le 313 value is 86h.

[0047]
When the previous read access is an error, it is in the format of FIG. 3b, the value of the access result 312 is 80XXh, and the value of Le313 is 06h.
[0048]
An example of the code XX indicating the error content in 80XXh set in the access result 312 (or 322) at the time of an access error is shown below.
[0049]
XX = 01 means an error that the designated record number is outside the accessible range.
[0050]
XX = 02 means that the flash memory chip 130 cannot be used due to a failure or the like.
[0051]
XX = 03 means an error in which the lower 4 bits of the first control byte 301 do not match the current access mode.
[0052]
XX = 04 means an error in which the next access mode requested by the second control byte 302 is invalid.
[0053]
Referring to FIG. 4, the processing flow when the applet in the IC card chip 150 starts accessing the secure data area 133 and the processing flow when executing access to the secure data area 133 by the write / read transfer command are shown. explain.
[0054]
The host device 160 issues a secure write command to the MMC 110 (401) and inputs secure write data 601 (402). The controller chip 120 extracts the command APDU 602 of the IC card command from the secure write data 601 (403), and issues an IC card command to the IC card chip 150 using the command APDU (404).
[0055]
The IC card chip 150 receives the IC card command (405), creates an IC card response 300 for requesting access to the secure data area 133, and returns it (406). The controller chip 120 receives this response and checks whether the SW1 byte 305 and the SW2 byte 306 are 90FFh (407). If it is not 90FFh, the routine proceeds to step 408. If 90FFh, it is checked whether the upper 4 bits of the first control byte 301 are 0001 (access start request) (412). If not 0001, the process moves to step 420. If it is 0001, it is checked whether the management table 136 is locked (413). If unlocked, go to Step 408. If locked, the AID 137 on the management table 136 is searched with the AID included in the subsequent output data 303 (414). If a matching AID is detected (415), the controller chip 120 approves the access start request and proceeds to step 416. If not detected, the access start request is rejected, and the process proceeds to step 408. In step 416, the secure data block corresponding to the detected AID 137 is selected and activated. Further, the corresponding transfer command code 138 is acquired (417). Then, the lower 4 bits of the first control byte 301 are examined to obtain an access mode to be started (418), and a write / read transfer command as shown in FIG. 3b is created according to the access mode (419). Thereafter, the process returns to step 404 and issues a write / read transfer command to the IC card chip 150.
[0056]
in step 420, it is checked whether the upper 4 bits of the first control byte 301 are 0010 (access execution request). If not 0010, the process proceeds to step 408. If it is 0010, it is checked whether there is an active secure data block and whether the lower 4 bits of the first control byte 301 match the access mode recognized by the controller chip 120 (421). If any is false, the process proceeds to step 408. If both are true, the access execution is approved and the record number included in the subsequent output data 303 is acquired (422). Then, write / read is executed for the data indicated by the record number (423). At this time, in the write mode, the 128-byte data included in the subsequent output data 303 is written. Next, a code indicating the result of the access is set to 312 or 322 (424). Then, the lower 4 bits of the first control byte 301 are examined to obtain the next access mode (418), and a write / read transfer command as shown in FIG. 3b or FIG. 419). Thereafter, the process returns to step 404 and issues a write / read transfer command to the IC card chip 150.
[0057]
In step 408, secure read data 611 is created from the response APDU 612 returned by the IC card chip 150. By reaching step 408, access to the secure data area 133 is terminated. Thereafter, the host device 160 issues a secure read command (409), and the controller chip 120 outputs secure read data 611 (410). Then, the host device 160 receives the secure read data 611 (411).
[0058]
As described above, the applet in the IC card chip 150 can access the secure data area 133 any number of times while the MMC 110 processes a set of secure write / secure read commands from the host device 160
[0059]
Hereinafter, access related to the management area 132 will be described.
[0060]
The MMC 110 can respond to the following four management commands so that the host device 160 can access the information in the management area 132. That is, (1) applet registration command, (2) applet registration release command, (3) management table lock command, and (4) management table unlock command. (1) is a command for registering an applet that uses the secure data area 133 in the management table 136 and allocating a secure data block used by the applet. (2) is a command for deleting the registration information of the applet from the management table 136. A command for canceling allocation of data blocks, (3) is a command for prohibiting change of registration information on the management table 136, and (4) is a command for permitting change of registration information on the management table 136. These commands are executed by the protocol of the secure write command and the secure read command as in general security processing, and are processed by the controller chip 120. In addition, information necessary for each process (registration, deregistration, lock, unlock) is obtained by using secure write data input / output at that time and APDU (602 or 612 in FIG. 6) included in the secure read data. Exchange.
[0061]
An AID is set in Datain 606 in the applet registration command and applet registration cancellation command. An applet to be registered is designated by this AID. The controller chip 120 determines how the AID and the secure data block are associated with each other. The host device 160 cannot directly specify a secure data block.
[0062]
In the management table lock command, a 255-byte password is set in Datain 606. The password is set in the password area 135, and the lock flag 134 is set to FFh (locked state). As a result, the applet registration command and applet registration cancellation command become invalid. If the password is already locked, the password is not set in the password area 135, and the applet registration command and applet registration cancellation command remain valid.
[0063]
In the management table unlock command, a 255-byte password is set in Datain. The password is compared with the value set in the password area 135, and if it matches, the lock flag 134 becomes 00h (unlocked). As a result, the applet registration command and the applet registration cancellation command become valid. If it is already unlocked, the applet registration command and applet registration release command remain invalid.
[0064]
When the applet registration command and the applet registration cancellation command are valid (unlocked), the information in the management table 136 is illegally changed by the host device 160 that does not know the password, and secure data that can be accessed by an applet itself. Unauthorized accesses such as writing / reading secure data blocks other than blocks may occur. Therefore, when the value of the lock flag 134 is 00h (unlocked state), the controller chip 120 does not permit the applet selected in the IC card chip 150 to access the secure data area. The host device 160 must set the lock flag 134 to FFh by the management table lock command after setting / changing the registration information of the management table 136.
[0065]
With reference to FIG. 5, the process flow of the four management commands will be described.

[0066]
The host device 160 issues a secure write command to the MMC 110 (501) and inputs secure write data 601 (502). The controller chip 120 extracts the command APDU 602 of the IC card command from the secure write data 601 (503), and checks whether it is a management command (504). If it is a management command, the process proceeds to step 507. On the other hand, if it is not a management command, the IC card command is issued to the IC card chip 150 using the command APDU 602 (505), the response is received from the IC card chip 150 (506), and the process proceeds to step 527.
[0067]
In step 507, the controller chip 120 checks whether the command APDU 602 indicates an applet registration command. If it is an applet registration command, the process proceeds to step 511. Otherwise, it checks whether it indicates an applet deregistration command (508). If it is an applet registration cancellation command, the process proceeds to step 512. Otherwise, it is checked whether it indicates a management table lock command (509). If it is a management table lock command, the process proceeds to step 513. Otherwise, it is checked whether it indicates a management table unlock command (510). If it is a management table unlock command, the process proceeds to step 514. Otherwise, go to step 525.
[0068]
In step 511, the lock flag 134 is checked to determine whether the management table 136 is unlocked. If it is locked, the process proceeds to step 525. If it is unlocked, it is checked whether the same AID in DataIn 606 exists in the already registered AID 137 (515). If it exists, the process proceeds to step 525. If it does not exist, it is checked whether there is a space on the management table 136 (that is, whether there is a secure data block not yet allocated) (516). If there is no space, the process proceeds to step 525. If there is a free space, the AID and transfer command code included in DataIn 606 are set in the AID 137 and transfer command code 138 corresponding to the secure data block (517). As a result, the applet indicated by the AID acquires the right to use the secure data block. Then, the process proceeds to step 526.
[0069]
In step 512, the lock flag 134 is checked to determine whether the management table 136 is unlocked. If it is locked, the process proceeds to step 525. If it is in the unlocked state, all registered AIDs 137 are searched with the AID in DataIn 606 (518). If a matching AID is detected (519), the AID 137 and the corresponding transfer command code 138 are deleted from the management table 136 (520). If no matching AID is detected, the process proceeds to step 525. As a result, the applet indicated by AID loses the right to use the secure data block. Then, the process proceeds to step 526.
In step 513, the lock flag 134 is checked to determine whether the management table 136 is unlocked. If it is locked, the process proceeds to step 525. If unlocked, FFh is set in the lock flag 134 (521), and the management table 136 is locked. The password in DataIn 606 is set in the password area 135 (522). Then, the process proceeds to step 526
[0070]
In step 514, the lock flag 134 is checked to determine whether the management table 136 is unlocked. If unlocked, the process proceeds to step 525. If it is locked, it is checked whether the password in DataIn 606 matches that set in the password area 135 (523). If not, go to step 525. If they match, 00h is set in the lock flag 134 (524), and the management table 136 is unlocked. Then, the process proceeds to step 526.
[0071]
In step 525, in order to indicate to the host device 160 that an error has occurred in the processing of the management command, a response APDU 612 including a status code indicating the error content is created, and the process proceeds to step 527. In step 526, in order to indicate to the host device 160 that the processing of the management command has been completed normally, a response APDU 612 including a status code of normal termination (for example, 9000h) is created, and the process proceeds to step 527.
[0072]
In step 527, secure read data 611 is created from the response APDU 612. Thereafter, the host device 160 issues a secure read command (528), and the controller chip 120 outputs secure read data 611 (529). Then, the host device 160 receives the secure read data 611 (530).
[0073]
When applying the present invention, the IC card chip 150 sets a dedicated status value of 90FFh in the SW1 byte 305 and the SW2 byte 306 as means for requesting the controller chip 120 to access the secure data area 133. Although shown, this is only an example, and access may be requested by means other than this. For example, a status code other than 90FFh may be used, or a dedicated password or the like may be included in DataOut 304.
[0074]
When the present invention is applied, the MMC 110 may have a function capable of changing the size of the secure data area 133 in accordance with a new (or the above-mentioned) management command. Further, it may have a function capable of changing the number of divisions of the secure data block (in the above case, the number of divisions = 4) in accordance with a new (or the above-mentioned) management command. Further, it may have a function capable of individually changing the size of each secure data block in accordance with a new (or the above-mentioned) management command.
[0075]
When applying the present invention, the length of the password described above may not be 255 bytes. However, for security reasons, this password is preferably long.
[0076]
When applying the present invention, the secure data block released by the applet deregistration command contains confidential data related to the applet that has been using this block, and then obtained the right to use the block. There is a risk that some applets will retrieve the sensitive data. Therefore, for safety, it is preferable to delete data remaining after the registration is canceled. The deletion may be performed during the processing of the applet registration cancellation command described above, or may be performed by the MMC 110 in response to a new management command from the host device 160.
[0077]
The present invention is also applicable to storage devices other than the card format.
[0078]
【The invention's effect】
ADVANTAGE OF THE INVENTION According to this invention, when performing the process which concerns on a specific application program, the safety | security of the process which concerns on a specific application program can be improved by processing the data relevant to a specific application program inside a memory device There is an effect.
[0079]
According to the present invention, by assigning a different block of memory in a memory device to each application program to be executed by the memory device, data interference between application programs, that is, memory allocated to a certain application program is transferred to another applet. It is also possible to prevent data being breached by being accessed.
[Brief description of the drawings]
FIG. 1 is a diagram showing an internal configuration of an MMC to which the present invention is applied.
FIG. 2 is a flowchart conceptually showing an operation of the MMC to which the present invention is applied.
FIG. 3 is a diagram showing a structure of an IC card command and an IC card response between a controller chip and an IC card chip.
FIG. 4 is a flowchart for reading and writing data from / to a secure data area on a flash memory chip in response to a request from an IC card chip.
FIG. 5 is a flowchart for registering and releasing an applet with respect to a management area on a flash memory chip, and locking and unlocking registration information in response to a request from an IC card chip.
FIG. 6 is a configuration diagram of secure write data and secure read data.

[Explanation of symbols]

110 ... MMC, 120 .. controller chip, 136 .. management table, 140 .. MMC external terminal, 150 ... IC card chip, 160 .. host device.

Patent Citations (10)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
JP3536149B2	1993-01-27	2004-06-07	大日本印刷株式会社	Memory area management method
JPH10198776A	1997-01-14	1998-07-31	Dainippon Printing Co Ltd	Portable information recording medium, and its information writing and reading method
JPH11120300A *	1997-10-09	1999-04-30	Fujitsu Ltd	Portable card medium, memory space managing method for portable card medium, issuing method for portable card medium, program data writing method for portable card medium, and medium on which memory space managing program is recorded
JP2000066882A	1998-08-19	2000-03-03	Hitachi Ltd	Ic card, and program managing method for ic card
JP2000172808A *	1998-12-01	2000-06-23	Toshiba Corp	Ic card and application managing method
FR2790324B1 *	1999-02-25	2001-12-28	St Microelectronics Sa	SECURE ACCESS DEVICE TO APPLICATIONS FROM A CHIP CARD
JP2002312221A *	2001-04-17	2002-10-25	Matsushita Electric Ind Co Ltd	Memory device with access control function and faile access control program
US7185145B2 *	2001-06-04	2007-02-27	Renesas Technology Corp.	Memory card
US6745944B2 *	2001-06-20	2004-06-08	Capital One Financial Corporation	System and method for identifying applications loaded in a smart card
JP2003030596A *	2001-07-13	2003-01-31	Hitachi Ltd	Storage device provided with logic channel management function

* Cited by examiner, † Cited by third party

Cited By (50)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US7197583B2 *	2003-01-21	2007-03-27	Zentek Technology Japan, Inc.	SDIO controller
JP4624732B2 *	2003-07-16	2011-02-02	パナソニック株式会社	how to access
US7607177B2 *	2004-02-23	2009-10-20	Micron Technology, Inc.	Secure compact flash
JP4706220B2 *	2004-09-29	2011-06-22	ソニー株式会社	Information processing apparatus and method, recording medium, and program
FR2878677B1 *	2004-11-30	2007-02-02	Gemplus Sa	APPLICATION SERVICE COMMUNICATION FROM A MICROCONTROLLER CARD TO A TERMINAL
US20060129856A1 *	2004-12-10	2006-06-15	Main Kevin K	System and method for expansion card power limiting
WO2006075576A1 *	2005-01-11	2006-07-20	Matsushita Electric Industrial Co., Ltd.	Secure device and system for issuing ic cards
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
JP4400515B2 *	2005-06-13	2010-01-20	日本電気株式会社	Storage system, storage device, logical disk connection relation changing method and program
JP2007004522A	2005-06-24	2007-01-11	Renesas Technology Corp	Storage device
US8074288B2 *	2005-07-15	2011-12-06	Microsoft Corporation	Isolation of application-specific data within a user account
JP2007102559A *	2005-10-05	2007-04-19	Toshiba Corp	Portable electronic equipment
JP4634924B2 *	2005-12-16	2011-02-23	株式会社日立情報制御ソリューションズ	Authentication method, authentication program, authentication system, and memory card
US20070218837A1 *	2006-03-14	2007-09-20	Sony Ericsson Mobile Communications Ab	Data communication in an electronic device

JP2009537042A *	2006-05-12	2009-10-22	サムスン エレクトロニクス カンパニー リミテッド	Apparatus and method for managing security data
US20080022415A1 *	2006-06-20	2008-01-24	Yu-Chiun Kuo	Authority limit management method
US7775442B2 *	2006-07-12	2010-08-17	Nokia Corporation	Method for accessing after-operation information of secure element applications
JP2008112285A *	2006-10-30	2008-05-15	Toshiba Corp	Non-volatile memory system
US7762553B2 *	2006-11-25	2010-07-27	Harris Curtis J	Form-fitting electronic game controller cover
JP4943866B2 *	2007-01-18	2012-05-30	パナソニック株式会社	Network camera system
KR100843238B1 *	2007-02-16	2008-07-03	삼성전자주식회사	Memory card
KR100888261B1	2007-02-22	2009-03-11	삼성전자주식회사	Memory subsystem capable of using bank identification and method thereof
JP4264958B2 *	2007-03-23	2009-05-20	フェリカネットワークス株式会社	Portable information terminal
US20110271044A1 *	2007-03-30	2011-11-03	Tyfone, Inc.	Memory card having one or more secure elements accessed with hidden commands
FR2914459B1 *	2007-03-30	2009-07-03	Oberthur Card Syst Sa	MICROPROCESSOR CARD
JP4488891B2 *	2007-04-02	2010-06-16	フェリカネットワークス株式会社	information processing terminal, data movement method, and program
JP2009053970A *	2007-08-28	2009-03-12	Toshiba Corp	Semiconductor device
US20090070691A1 *	2007-09-12	2009-03-12	Devicefidelity, Inc.	Presenting web pages through mobile host devices
US9201790B2 *	2007-10-09	2015-12-01	Seagate Technology Llc	System and method of matching data rates
US8380711B2 *	2007-11-12	2013-02-19	Gemalto Sa	System and method for drive resizing and partition size exchange between a flash memory controller and a smart card
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
JP2010020513A *	2008-07-10	2010-01-28	Panasonic Corp	Sim card, portable terminal, and reader/writer device
US20100033310A1 *	2008-08-08	2010-02-11	Narendra Siva G	Power negotation for small rfid card
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
TWI380219B *	2009-01-20	2012-12-21	Phison Electronics Corp	Card reader with near field communication functions and near field communication device thereof
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
US9037824B2 *	2009-03-26	2015-05-19	Micron Technology, Inc.	Password accessible microelectronic memory
JP5454933B2 *	2009-09-11	2014-03-26	株式会社東芝	Portable electronic device, IC card, and control method for portable electronic device
KR101626884B1 *	2009-11-25	2016-06-01	삼성전자주식회사	Multi-chip memory system and data transfer method thereof
JP5566040B2 *	2010-03-30	2014-08-06	富士通株式会社	Storage device, data processing device, registration method, and computer program
US20110300526A1 *	2010-06-07	2011-12-08	Georgia State University Research Foundation	Systems And Methods For Facilitating Classroom Interaction
JP2012064045A	2010-09-16	2012-03-29	Toshiba Corp	Portable electronic device, non-contact ic card and command processing method for portable electronic device
KR101722159B1 *	2010-09-17	2017-04-03	주식회사 에스엘에이네트웍스	Secure memory card
US9311229B2 *	2011-03-29	2016-04-12	Blackberry Limited	System and method for managing flash memory
WO2013039451A1 *	2011-09-13	2013-03-21	T-Data Systems (S) Pte Ltd	A method for restricting access to data stored on a memory card and a memory card
CN105592038B *	2014-12-30	2018-12-25	中国银联股份有限公司	trusted service management system and method
US10332565B1 *	2016-07-29	2019-06-18	EMC IP Holding Company LLC	Application-aware control for data services

FR3062501B1 *	2017-02-02	2019-03-15	Idemia France	METHOD FOR SECURING ELECTRONIC OPERATION
US11194738B2 *	2019-07-29	2021-12-07	International Business Machines Corporation	Implementing management commands utilizing an in-band interface

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
JP4322021B2	2009-08-26	Memory card
JP2007004522A	2007-01-11	Storage device
US7185145B2	2007-02-27	Memory card
KR920007410B1	1992-08-31	Safe file system for a portable data carrier
US7607177B2	2009-10-20	Secure compact flash
US7653796B2	2010-01-26	Information recording medium and region management method for a plurality of recording regions each managed by independent file system
US20090182937A1	2009-07-16	Semiconductor memory card, and program for controlling the same
US20060236026A1	2006-10-19	Method and system for allocating, accessing and de-allocating storage space of a memory card
KR20080089586A	2008-10-07	Media card with command pass through mechanism
JP2005134953A	2005-05-26	Unset ic card, ic card issue system, and method for issuing ic card application
US7024532B2	2006-04-04	File management method, and memory card and terminal apparatus that make use of the method
JP4445718B2	2010-04-07	IC card and IC card program
GB2314948A	1998-01-14	Secure transfer of applications and/or data onto a chipcard
JP2003022216A	2003-01-24	Storage device
JP4057858B2	2008-03-05	File management method and memory card and terminal device using the same
KR20130139604A	2013-12-23	Memory device comprising a plurality of memory chips, authentication system and authentication method thereof
JP2011060136A	2011-03-24	Portable electronic apparatus, and data management method in the same
JP3017736B2	2000-03-13	Portable electronic devices
JP2005011171A	2005-01-13	ic card and ic card program
JP2007323140A	2007-12-13	Information processing apparatus, method and program
JPH1074243A	1998-03-17	ic card
JP2005025426A	2005-01-27	Semiconductor storage device and control method thereof
JP2019160191A	2019-09-19	Portable electronic device and IC card
JP2501050Y2	1996-06-12	IC card
KR101023100B1	2011-03-24	Device for USB Banking

Priority And Related Applications

Priority Applications (2)

Application	Priority date	Filing date	Title
JP2003028998		2003-02-06	
JP2003050243A	2003-02-06	2003-02-27	Memory card

Applications Claiming Priority (3)

Application	Filing date	Title

JP2003050243A	2003-02-27	Memory card
KR1020030099827A	2003-12-30	Memory card
US10/776,962	2004-02-10	Memory device storing data relating to specific application programs

Legal Events

Date	Code	Title	Description
2006-01-11	RD02	Notification of acceptance of power of attorney	**Free format text:** JAPANESE INTERMEDIATE CODE: A7422 **Effective date:** 20060110
2006-01-11	A621	Written request for application examination	**Free format text:** JAPANESE INTERMEDIATE CODE: A621 **Effective date:** 20060110
2008-06-27	A977	Report on retrieval	**Free format text:** JAPANESE INTERMEDIATE CODE: A971007 **Effective date:** 20080627
2008-07-23	A131	Notification of reasons for refusal	**Free format text:** JAPANESE INTERMEDIATE CODE: A131 **Effective date:** 20080722
2008-09-20	A521	Written amendment	**Free format text:** JAPANESE INTERMEDIATE CODE: A523 **Effective date:** 20080919
2009-05-13	TRDD	Decision of grant or rejection written	
2009-05-20	A01	Written decision to grant a patent or to grant a registration (utility model)	**Free format text:** JAPANESE INTERMEDIATE CODE: A01 **Effective date:** 20090519
2009-05-21	A01	Written decision to grant a patent or to grant a registration (utility model)	**Free format text:** JAPANESE INTERMEDIATE CODE: A01
2009-06-11	A61	First payment of annual fees (during grant procedure)	**Free format text:** JAPANESE INTERMEDIATE CODE: A61 **Effective date:** 20090602
2009-06-12	R150	Certificate of patent or registration of utility model	**Ref document number:** 4322021 **Country of ref document:** JP **Free format text:** JAPANESE INTERMEDIATE CODE: R150 **Free format text:** JAPANESE INTERMEDIATE CODE: R150
2009-06-15	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20120612 **Year of fee payment:** 3
2010-10-04	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20120612 **Year of fee payment:** 3
2010-10-04	S111	Request for change of ownership or part of ownership	**Free format text:** JAPANESE INTERMEDIATE CODE: R313111
2010-10-13	R350	Written notification of registration of transfer	**Free format text:** JAPANESE INTERMEDIATE CODE: R350
2010-10-13	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20120612 **Year of fee payment:** 3
2012-09-29	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20120612 **Year of fee payment:** 3
2012-04-03	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20130612 **Year of fee payment:** 4
2013-03-28	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20130612

			Year of fee payment: 4
2013-04-02	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20140612 Year of fee payment: 5
2015-09-15	S531	Written request for registration of change of domicile	Free format text: JAPANESE INTERMEDIATE CODE: R313531
2015-09-28	R350	Written notification of registration of transfer	Free format text: JAPANESE INTERMEDIATE CODE: R350
2019-06-12	LAPS	Cancellation because of no payment of annual fees	

Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

Patents 4831500

Authentication

Classifications

G01S5/14 Determining absolute distances from a plurality of spaced points of known location

View 12 more classifications

AU4831500A

Australia

Find Prior Art Similar

Inventor: Andrew L. Di Renzo

Current Assignee : ANDREW L DI RIENZO

Worldwide applications

2000 AU WO 2005 US 2014 US

Application AU48315/00A events

1999-05-10	Priority to US13349299P
1999-05-10	Priority to US60133492
2000-04-28	Priority to US56078400A
2000-04-28	Priority to US09560784
2000-05-09	Application filed by ANDREW L DI RIENZO
2000-05-09	Priority to PCT/US2000/012642
2000-11-21	Publication of AU4831500A
Status	Abandoned

Info: Patent citations (35), Cited by (32), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Patent Citations (35)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US4591823A *	1984-05-11	1986-05-27	Horvat George T	Traffic speed surveillance system
US4860352A *	1985-05-20	1989-08-22	Satellite Financial Systems Corporation	Satellite communication system and method with message authentication suitable for use in financial institutions
US4785291A *	1987-03-06	1988-11-15	Hawthorne Candy C	Distance monitor especially for child surveillance
US5243652A *	1992-09-30	1993-09-07	Gte Laboratories Incorporated	Location-sensitive remote database access control
US5777580A	1992-11-18	1998-07-07	Trimble Navigation Limited	Vehicle location system
US5327144A *	1993-05-07	1994-07-05	Associated Rt, Inc.	Cellular telephone location system
US5422814A *	1993-10-25	1995-06-06	Trimble Navigation Limited	Global position system receiver with map coordinate system outputs
US5568119A *	1993-12-21	1996-10-22	Trimble Navigation Limited	Arrestee monitoring with variable site boundaries
EP0710494B1 *	1994-02-24	2001-11-21	HYUGA, Makoto	Method for guiding golf course, device therefor, and golf course managing system
US5838277A	1994-05-20	1998-11-17	Trimble Navigation Limited	GPS-based controller module
US5461390A *	1994-05-27	1995-10-24	At&T Ipm Corp.	Locator device useful for house arrest and stalker detection
US5541845A	1994-08-02	1996-07-30	Trimble Navigation Limited	Monitoring of route and schedule adherence
US6072396A *	1994-12-30	2000-06-06	Advanced Business Sciences	Apparatus and method for continuous electronic monitoring and tracking of individuals

US5532690A *	1995-04-04	1996-07-02	Itt Corporation	Apparatus and method for monitoring and bounding the path of a ground vehicle
US5835061A *	1995-06-06	1998-11-10	Wayport, Inc.	Method and apparatus for geographic-based communications service
US5754657A *	1995-08-31	1998-05-19	Trimble Navigation Limited	Authentication of a message source
US5757916A *	1995-10-06	1998-05-26	International Series Research, Inc.	Method and apparatus for authenticating the location of remote users of networked computing systems
US5794174A	1995-10-18	1998-08-11	Trimble Navigation Limited	System for automatic vehicle location viewing via television
CA2190672C *	1995-12-27	2000-05-23	Mark Jeffrey Foladare	Communication system and method using two-way paging to provide call control
US6438380B1 *	1997-02-28	2002-08-20	Lucent Technologies Inc.	System for robust location of a mobile transmitter
US6091957A *	1997-06-12	2000-07-18	Northern Telecom Limited	System and method for providing a geographic location of a mobile telecommunications unit
US6148261A *	1997-06-20	2000-11-14	American Calcar, Inc.	Personal communication system to send and receive voice data positioning information
US6163701A	1997-07-25	2000-12-19	Motorola, Inc.	System and method for providing location information of a mobile station in a communication system
US6266582B1 *	1997-08-06	2001-07-24	Rockwell Collins, Inc.	GPS analytic redundancy for gyroscope failure detection
US6118977A	1997-09-11	2000-09-12	Lucent Technologies, Inc.	Telecommunications-assisted satellite positioning system
US6114991A	1997-09-11	2000-09-05	Lucent Technologies, Inc	Auxiliary system for assisting a wireless terminal in determining its position from signals transmitted from a navigation satellite
US6505046B1 *	1997-11-19	2003-01-07	Nortel Networks Limited	Method and apparatus for distributing location-based messages in a wireless communication network
US6647257B2 *	1998-01-21	2003-11-11	Leap Wireless International, Inc.	System and method for providing targeted messages based on wireless mobile location
JP3629935B2 *	1998-01-27	2005-03-16	オムロン株式会社	Speed measurement method for moving body and speed measurement device using the method
US7268700B1 *	1998-01-27	2007-09-11	Hoffberg Steven M	Mobile communication device
US6477543B1 *	1998-10-23	2002-11-05	International Business Machines Corporation	Method, apparatus and program storage device for a client and adaptive synchronization and transformation server
US20030060211A1 *	1999-01-26	2003-03-27	Vincent Chern	Location-based information retrieval system for wireless communication device
US6332127B1 *	1999-01-28	2001-12-18	International Business Machines Corporation	Systems, methods and computer program products for providing time and location specific advertising via the internet
US6360167B1 *	1999-01-29	2002-03-19	Magellan Dis, Inc.	Vehicle navigation system with location-based multi-media annotation
US9026780B2 *	2011-04-12	2015-05-05	Mobile Communication Technologies, Llc	Mobile communicator device including user attentiveness detector

* Cited by examiner, † Cited by third party

Cited By (32)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US8352582B2	2001-06-28	2013-01-08	Koninklijke Philips Electronics N.V.	Temporal proximity to verify physical proximity
US7240211B2	2001-10-09	2007-07-03	Activcard Ireland Limited	Method of providing an access request to a same server based on a unique identifier
US7069938B2 *	2002-03-01	2009-10-20	Enterasys Networks, Inc.	Verified device locations in a data network
US7042867B2 *	2002-07-29	2006-05-09	Meshnetworks, Inc.	System and method for determining physical location of a node in a wireless network during an authentication check of the node
EP1550284A1 *	2002-09-30	2005-07-06	Koninklijke Philips Electronics N.V	Secure proximity verification of a node on a network
US8239452B2 *	2004-05-01	2012-08-07	Microsoft Corporation	System and method for discovering and publishing of presence information on a network

US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
EP1868132A4 *	2005-03-23	2014-06-18	Ihc Corp	Authentication system
US8046459B2 *	2006-07-03	2011-10-25	A sigo Digital Technology Co , Ltd.	Method, device and system of obtaining network information using device as service credential
US20080276309A1 *	2006-07-06	2008-11-06	Edelman Lance F	System and Method for Securing Software Applications
US20080046579A1 *	2006-08-18	2008-02-21	Denis Brent Walton	Secure email recipient
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US20090320125A1 *	2008-05-08	2009-12-24	Eastman Chemical Company	Systems, methods, and computer readable media for computer security
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US20100033310A1 *	2008-08-08	2010-02-11	Narendra Siva G	Power negotation for small rfid card
US8451112B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
JP6098169B2 *	2012-02-01	2017-03-22	株式会社リコー	Information processing system, information processing apparatus, program, and authentication method
US9258287B2 *	2012-12-20	2016-02-09	Broadcom Corporation	Secure active networks
KR101416541B1 *	2012-12-27	2014-07-09	주식회사 로웸	Safety login system and the method and apparatus therefor
JP6427889B2 *	2014-02-06	2018-11-28	株式会社デンソー	Navigation message authentication system, receiving terminal, and authentication processing device
CN104980918B	2014-04-04	2019-09-17	阿里巴巴集团控股有限公司	Bootstrap information transmission provides the method and device of service based on beacon
US10356651B2	2014-07-17	2019-07-16	Cirrent, Inc.	Controlled connection of a wireless device to a network
US10834592B2 *	2014-07-17	2020-11-10	Cirrent, Inc.	Securing credential distribution
US10154409B2	2014-07-17	2018-12-11	Cirrent, Inc.	Binding an authenticated user with a wireless device
US9942756B2	2014-07-17	2018-04-10	Cirrent, Inc.	Securing credential distribution
FR3037423B1 *	2015-06-12	2018-05-25	Parkeon	METHOD FOR MANAGING THE ACCESS RIGHTS OF A USER IN A PLACE
US10348758B1 *	2016-06-30	2019-07-09	Symantec Corporation	Systems and methods for detecting network security deficiencies on endpoint devices
US10387677B2 *	2017-04-18	2019-08-20	International Business Machines Corporation	Deniable obfuscation of user locations
US10531287B2	2017-04-18	2020-01-07	International Business Machines Corporation	Plausible obfuscation of user location trajectories
US10404746B1 *	2017-08-09	2019-09-03	Robert B O'Dell	Rendering spoofed electronic mail harmless
US10989783B1 *	2020-10-26	2021-04-27	Listen Technologies Corporation	False positive immunity in beacon systems, and related systems, methods, and devices

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
AU4831500A	2000-11-21	Authentication
AU1173201A	2001-05-14	Skin-gripper
AU3092999A	2000-10-04	Digital-timeshare-exchange
AU7695400A	2001-04-17	Security arrangement
AU4115400A	2000-11-14	Short-circuiter
AU2804600A	2000-09-04	Arylaminoalkylamides
AU2023701A	2001-06-18	Sketcher

AU2237001A	2001-05-30	Nickel-iron-silica-alumina
AU2699800A	2000-09-04	Organoceramics
AU7514700A	2001-04-10	Cyanopiperidines
AU4568900A	2000-12-12	Improved can
AU4916900A	2000-12-05	Benzofuranylsulfonates
AU4561600A	2000-12-05	Benzofuranylaminoalcohols
AU1901801A	2001-05-30	Glucofuranoses
AU1183001A	2001-04-30	Deep-fryer
AU1915601A	2001-06-06	Periotome
AU7513400A	2001-04-30	Hydantoin-racemase
AU4435300A	2000-11-10	Hula-hoop
AU2582200A	2000-09-14	Windturbine
AU2197301A	2001-06-25	Microlamp
AU5416100A	2001-01-31	Retinoscopes
AU1737601A	2001-05-08	Collectalbum
AU3010501A	2001-07-03	3-nitro-dihydro-isoxazoles and -oxazines
AU1890101A	2001-06-25	Ikk4
AU2374501A	2001-06-18	Thermoroll

Priority And Related Applications

Priority Applications (5)

Application	Priority date	Filing date	Title
US13349299P	1999-05-10	1999-05-10	*US Provisional Application*
US60133492		1999-05-10	
US56078400A	2000-04-28	2000-04-28	*US Provisional Application*
US09560784		2000-04-28	
PCT/US2000/012642	1999-05-10	2000-05-09	Authentication

Legal Events

Date	Code	Title	Description
2002-03-21	MK6	Application lapsed section 142(2)(f)/reg. 8.3(3) - pct applic. not entering national phase	

Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

Patents 3180086

Mobile communication device, information transmission system and method, non-contact IC media usable in mobile communication device

Classifications

H02J50/10 Circuit arrangements or systems for wireless supply or distribution of electric power using inductive coupling

View 14 more classifications

JP3180086B2

Japan

Find Prior Art Similar

Other languages: Japanese

Inventor: [redacted]

Worldwide applications

1998 JP 1999 CN AU CN WO EP CN AT EP KR EP EP KR CN US DE 2004 US 2005 HK

Application JP24599598A events

1998-08-31	Application filed by [redacted]
1998-08-31	Priority to JP24599598A
2000-03-14	Publication of JP2000076399A
2000-04-19	Priority claimed from JP2000118571A
2001-06-25	Application granted
2001-06-25	Publication of JP3180086B2
2018-08-31	Anticipated expiration
Status	Expired - Fee Related

Info: Patent citations (53), Cited by (69), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (27)

Hide Dependent

(57) [Claims]

1. 1. A portable communication device equipped with a display, a medium carrier for exchangeably carrying a non-contact IC medium having an information recording area, and a wireless transmission / reception circuit including an antenna embedded in a device housing. When, through the wireless transceiver circuit, the read control and the write control of digital information with respect to both the recording area of the external contactless IC media in the region covering the non-contact IC medium which is carried on the media carrier antenna control circuit and performs the processing based on the read digital information, the non-contact IC media or the external contactless IC that is the supported through the control circuit along with displaying the result information of the information processing on the display to perform information processing means for recording in a recording area of the media. Communication device.

    2. Wherein said control circuit includes a plurality of external contactless I
    Selectively receives digital information transmitted from the C module, characterized by storing digital information received in the contactless IC media which is the supported, portable communication apparatus according to claim 1.

3. 3. A portable communication device equipped with a display and a sound generation mechanism, comprising: a non-contact IC medium in which sound source data and image data output in association with the sound source data are recorded in a recording area thereof; A medium carrier that exchangeably carries the plurality of non-contact IC media; a wireless transmission / reception circuit including a housing-embedded antenna; and a non-contact IC medium carried by the media carrier through the wireless transmission / reception circuit. Within the coverage area of the antenna
A control circuit from one of the recording area of the external contactless IC media reading out the sound source data and the image data that exist, the sound source controller and the read to reproduce the sound to the sound generation mechanism based on said read sound source data information processing means comprising a display controller for displaying an image on the display based on the output image data, and a mobile communication device.

    4. 4. The wireless communication device according to claim 1, wherein
    Exchange recorded information on non-contact IC media with other devices.
    Further comprising: The mobile communication device according to claim 1, 2 or 3.

    5. 5. A plurality of non-contact ICs provided on the medium carrier.
    Media are carried, and each non-contact IC media

Each configured to independently communicate with the control circuit.
Characterized by the fact that The mobile communication device according to claim 1.

6. 6. Non-contact carried on the medium carrier.
IC media is molded into a coin shape. The mobile communication device according to claim 5.

7. 7. A plurality of non-contact IC media are on the same plane.
6. The portable communication device according to claim 5, wherein the portable communication device is arranged side by side.
Place.

8. 8. A battery for supplying drive power to an apparatus main body.
A coil for receiving a power component from the outside in a non-contact manner, and a charging circuit for converting the power component received through the coil into a fixed value of charging power, and charging the battery using the converted charging power. further that Yusuke, portable communication apparatus according to one of claims 1 to 7.

9. Wherein said a mobile
 band communication apparatus according to one of claims 1 to 8, the digital information corresponding to a predetermined value information mobile
includes a media issuance device that band communication device issues recorded in the contactless IC media readable, wherein the media issuance device, a type of digital information to be recorded on the contactless IC media on the value information An information transmission system, which is configured to be selectable according to the information.

10. 10. The information transmission system according to claim 9 , wherein the media issuing device is configured to periodically update the digital information so as to correspond to the same value information.

11. 11. The information transmission system according to claim 10 , wherein said digital information is periodical article information including character data.

12. 12. of according to one of claims 1 to 8
A portable communication device, guidance information human visible is marked on the surface portion, the contents corresponding to the guide information to the
 internal recording area table to de l
 digital information is recorded including external non-contact IC media
The external non-contact IC media responds to the guidance information.
Responsive to and read by the portable communication device
An information transmission system characterized by being present .

13. Wherein said external contactless IC media, a plurality
13. The information transmission system according to claim 12 , wherein the guide information is embedded in the same guide panel on which the guide information is drawn.

14. 14. characterized in that said portable communication device is a mobile phone radio, communication system according to one of claims 9 to 13.

15. 15. A non-contact IC medium having an information recording area, and a portable communication medium according to claim 1.
An information transmission method performed using a communication device , comprising: transmitting information that can be visually recognized by a human on a surface portion of the non-contact IC medium or a medium carrying the non-contact IC medium; Recording digital information representing the content corresponding to the viewable information in a recording area and presenting the digital information to a holder of the portable communication device; Causing the portable communication device to read and perform required information processing.

16. 16. The non-contact IC medium is formed in a sheet shape, and mark information is written on a surface of the non-contact IC medium, and profile information is recorded in the recording area.
16. The information transmitting method according to claim 15, wherein the information transmission method is attached to a business card mount or a pamphlet and distributed .

17. 17. The non-contact IC medium is formed into a sheet.
None, record print target information on the non-contact IC media
And paste it on printed matter for distribution.
. The information transmission method according to claim 15.

18. 18. The non-contact IC medium is formed into a sheet.
None, write the information to be mailed on the contactless IC media.
Recorded, pasted on mail and distributed
And The information transmission method according to claim 15.

19. 19. The portable communication medium according to claim 1, wherein
Communication device and a fixed distance away from the
Contactless IC having information recording area inside communication device
Media and the mobile communication device
The digital data independently of the contact IC media
16. Transmission and reception of file information.
information transmission method.

20. 20. An information recording area in the portable communication device.
One or more non-contact IC media
A mechanism for holding the non-contact IC media
Use as a SIM (Subscriber Identity Module).
A coin-type non-contact IC media that can be used.
A predetermined service to be transmitted to each non-contact IC media
Record permission information for receiving service information
Characterized by The information transmission method according to claim 15.

21. 21. The portable communication device is a portable telephone radio set.
The method according to any one of claims 15 to 20, wherein
Information transmission method described in section.

22. 22. The method according to claim 1, wherein
Digital information read control and
A non-contact IC module having a recording area capable of both or one of writing control is embedded in a sheet-shaped medium having a predetermined shape, and at least one surface of the sheet-shaped medium has
Non-contact IC media, characterized in that there is a sticking member that cannot be peeled off after sticking.

23. 23. The method according to claim 1, wherein
Read control and the digital information I by the mobile communication apparatus
A non-contact IC module having a recording area capable of both or one of writing control is embedded in a sheet-shaped medium having a predetermined shape, and at least one surface of the sheet-shaped medium has
Non-contact IC media, characterized in that there is an attaching member that can be attached again after peeling.

24. 24. The non-contact IC on one sheet of medium.
Multiple non-contact ICs with multiple embedded modules
And wherein the region including the presence site of modules and the sticking member can be cut in a specific shape, the non-contact IC medium as claimed in claim 22 or 23.

25. 25. The method according to claim 1, wherein
Digital information read control and
A non-contact IC medium in which a non-contact IC module having a recording area capable of both or one of writing control is embedded in a sheet medium of a predetermined shape, wherein a human can visually recognize the surface of the sheet medium. Machine-readable digital information including the content corresponding to the information is recorded in the recording area, and a predetermined digital information reading device is provided on the back surface of the sheet-shaped medium. Non-contact IC media, characterized in that a sticking member for sticking itself is fixed at a position where the digital information can be read.

26. 26. The method according to claim 1, wherein
Digital information read control and
A non-contact IC medium characterized in that a non-contact IC module having a recording area capable of both or one of writing control is embedded in a stick-shaped medium that can be mounted on a stick-shaped casing.

27. 27. The portable communication device according to claim 1, which is a solid non-contact IC medium carried on a media carrier.
Read and write control of digital information
One or one has a solid-type module medium of a predetermined shape in which a non-contact IC module having a recording area capable of being embedded is embedded. A non-contact IC medium, wherein an engagement mechanism that allows engagement and disengagement is integrally formed.

Description

DETAILED DESCRIPTION OF THE INVENTION

[0001]

[0001] 1. Field of the Invention [0002] The present invention relates to a non-contact IC medium and a system using the non-contact IC medium. Here, "non-contact IC media" refers to, for example,
ISO (International Organization for Standadisat)
ion) IEC (International Electrotechnical comm)
ision) JTC1 (Joint Technical Committee 1) /
The SC (Sub-Committe) 17 is a core module based on the specifications of a contactless IC card ("Contactless IC Card"), which is being discussed in international standardization or international standardization deliberations. Point. As a specific example of a system to which the non-contact IC media is applied, the non-contact IC media is carried in a portable communication device, for example, an existing portable telephone radio or a portable computer device, and various applications are executed. Alternatively, the recorded information is read by holding the portable communication device over an external non-contact IC medium,
Execution of required processing and transmission of information through a non-contact IC medium or a non-contact reader / writer carrying the same can be cited.

[0002]

2. Description of the Related Art A contact-type IC card having electric contacts has been put into practical use as a card-type tool requiring security, such as an electronic payment card or an identification card in electric commerce. .
The contact-type IC card has a structure in which it is electrically connected directly to a reader / writer through a contact point, so that the operation is generally stable. However, insertion and removal of a card from a reader / writer involves physical contact, which may cause a problem such as poor contact. Therefore, recently, a non-contact IC card equipped with a non-contact IC medium capable of transmitting recorded information without physical contact has appeared, and is being studied for practical use.

[0003] A non-contact IC card is usually a non-contact IC comprising a radio transmitting / receiving circuit including an antenna (coil) and an IC section including a processor and a memory on a card medium.
It is configured by embedding media. Some ICs are configured as so-called memory cards that do not include a processor.

[0004] The connection of a non-contact IC card to a reader / writer is performed through a wireless transmission / reception circuit, and power and power required for operation are usually supplied from the reader / writer. For transmission of information including a power component and the like from the reader / writer, a signal obtained by ASK (Amplitude Shifting Keying) modulation of a wireless carrier of 13.56 [MHz] is used, while transmission of information from the card side is used. For example, 1
A subcarrier (8) obtained by combining a plurality of 3.56 [MHz] signals
47.5 / 423.7 [kHz]). Since a plurality of non-contact IC cards are expected to coexist near the same reader / writer, a technique called anti-collision has been established to prevent data collision between the cards. At present, it is possible to identify several cards by changing the modulation method at the time of reply from the card side

to the reader / writer or changing the return timing. The anti-collision technology is disclosed in Japanese Patent Application Laid-Open Nos. H5-217032 and H5-2. No. 66267 can be referred to.

In recent years, PHS (Personal Handyphi)
On the other hand, mobile phone radios such as mobile phones and mobile computer terminals, and mobile computer terminals have rapidly spread, and many people carry them. Therefore, attempts have been made to add various added values to mobile phone radios and the like using IC cards. For example, Japanese Patent Application Laid-Open No. 8-87655 discloses that an IC card in which information of a bank is recorded is inserted into a mobile phone radio, and the IC card owner (owner of the mobile phone radio) purchases or pays for an article. An information processing system is disclosed in which a device for providing goods or the like acquires information recorded on an IC card through a mobile phone wireless device when providing a service, and automatically performs electronic payment using the acquired recorded information. Have been. The IC card in this case is a contact-type IC card, and a contact-type reader / writer having electrical contacts is provided on the portable telephone radio side.

[0006]

As described above, since a non-contact IC card does not require an electrical contact, an IC module can be made smaller, thinner, and mass-produced than a contact-type IC card. Becomes possible. Further, even if a plurality of non-contact IC cards are mixed in the vicinity of the same reader / writer, these can be distinguished on the reader / writer side, so that the same usage form as the contact type IC card is possible. further,
A reader / writer for reading information recorded on a non-contact IC card can also be made smaller and lighter than a contact type IC card.

However, most of the conventional non-contact IC cards record information in card units. That is, the usage is determined for each card. For this reason, there is a trouble that the user has to carry a plurality of non-contact IC cards according to the purpose of use, and to find a corresponding one at the time of use.

Further, for example, in the above-mentioned information processing system, if a non-contact IC card is used instead of a contact IC card, the reader / writer can be reduced in size and the weight of the portable telephone radio itself can be reduced. Be expected. However, the conventional reader / writer for this type of application is only for exchanging information with the memory of a built-in contact type IC card (or non-contact type IC card) or an external non-contact type IC card. It is not assumed that information is exchanged between both a contact type IC card (or a non-contact type IC card) and an external non-contact type IC card.

As described above, conventionally, it is assumed that a non-contact IC medium is embedded in a card-shaped medium and used for each card. However, the non-contact IC media is not necessarily limited to the conventional use form. In addition, the use thereof is expected to be widely used not only in a specific field but also in various fields where information transmission is interposed.

An object of the present invention is to provide a non-contact IC medium having excellent versatility and an application system capable of adding more added value by using the non-contact IC medium.

[0011]

SUMMARY OF THE INVENTION The present invention provides a non-contact IC method.
Mobile communication that can increase added value using media
Provide equipment. This portable communication device has a display
Onboard mobile communication device, or display and sound generator
in a mobile communication device equipped with a
Exchanges single or multiple non-contact IC media
And a media carrier for carrying the media
A radio transmitting and receiving circuit including an embedded antenna, and
Through the receiving circuit, the non-
Contact IC media and external
Digital data for both recording areas of non-contact IC media
A control circuit for performing read control and write control of file information;
Performs information processing based on the read digital information,
Displaying the result information of the information processing on the display
And the carried non-contact through the control circuit
Recording on IC media or the external non-contact IC media
Information processing means for recording in the area.
I do. Preferably, the control circuit includes a plurality of external non-contact
Selective digital information transmitted from IC module
And the received digital information is
It is configured to accumulate on the contact IC media.

[0012] Another portable communication device of the present invention is a display device.
in a portable communication device equipped with a
For exchangeably carrying non-contact IC media
The media carrier and the antenna embedded in the device housing
Including a wireless transmitting and receiving circuit, and through this wireless transmitting and receiving circuit,
A non-contact IC medium carried on the medium carrier;
External non-contact IC media in the area covered by the antenna
Control of reading digital information from both recording areas
Control circuit for controlling read and write, and said read digital
Information processing based on the file information, and the result of the information processing
Displaying information on the display and controlling
The carried non-contact IC media through the circuit or
Information to be recorded in the recording area of the external non-contact IC media
Report processing means.

[0013] Another portable communication device of the present invention is a display device.
A portable communication device equipped with a
Source data and images output in conjunction with this sound source data
Non-contact IC media with data recorded in its recording area

And exchange the single or multiple non-contact IC media
The media carrier that is carried on the
Wireless transmission and reception circuit including
The non-contact IC media carried on the media carrier.
And the external non-contact IC
Source data and image data from any of the
A control circuit for reading image data, and the read sound source
A sound source for causing the sound generation mechanism to reproduce sound based on data
Based on the controller and the read image data
Display control for displaying an image on the display
And information processing means comprising:
You.

In each of the above portable communication devices, preferably
is a non-contact IC in its own device through the wireless transmission / reception circuit.
There is a means for exchanging recording information of media with other devices.
That multiple non-contact IC media are controlled independently
Configuration that can communicate with non-contact IC media
Being shaped like a coin, multiple non-contact IC
That they are supported side by side on the same plane
Providing any or all of them allows for further applications.
It is desirable.

The portable communication device of the present invention is driven by the device main body.
Non-contact with power supply battery and external power components
And a coil for receiving power through the coil.
The converted power component is converted to a fixed value of charging power, and the converted charging
And a charging circuit for charging the battery using electric power.
May be provided.

The present invention further relates to a non-contact IC medium.
Various information transmission systems. The first information biography
is equipped with the contactless reader / writer of the present invention, for example.
Mobile communication device and a directory corresponding to predetermined value information.
Digital information on non-contact IC media
And a media issuing device.
The type of digital information to be recorded depends on the value information.
The feature is that it can be arbitrarily selected
You. The media publishing device is configured to
Periodical articles that contain digital information, such as textual data
It is configured to update information periodically. Images and sounds
Contactless IC media including digital content
May be recorded and issued.

The second information transmission system has a human surface on the surface.
The guide information that can be visually recognized is written in the internal recording area.
Machine-readable digital information representing the content corresponding to the information
-Contact IC media on which information is recorded and this non-contact IC
Means for reproducing digital information read from the medium
The portable communication device of the present invention provided with the non-contact IC
It is noted that the media are scattered in multiple
It is a sign. A plurality of said non-contact IC media
Is embedded in the same guide panel on which the guide information is drawn
It may be something.

[0018] The third information transmission system may be single or plural.
Non-contact IC media and non-contact reader / writer of the present invention
Each comprising a plurality of mobile communication devices having
Exchanges the recorded information of the non-contact IC media of the own device.
It is configured to be exchangeable.

The present invention also relates to a non- volatile memory having an information recording area.
Contact IC media and recording area of the non-contact IC media
Means for reading information from the server and information based on the read information.
Information transmission using a portable communication device provided with
The contactless IC medium or the contactless IC medium.
Humans approve the surface of the media carrying the tactile IC media
information that can be transmitted, and
Recording area corresponding to the visible information in the recording area.
Record digital information and present it to the holder of the portable communication device
And recording on the presented non-contact IC media
Read digital information into the portable communication device.
And perform the necessary information processing.
You. This is a non-contact IC media sheet-like surface
Write the mark information on the

Record information and paste it on business card mount or pamphlet
And non-contact IC media in sheet form
The information to be printed is recorded on the non-contact IC media and
Method of pasting and distributing on printed matter, non-contact IC media
To be mailed to non-contact IC media
Those who record information and paste it on mail to distribute
Method, non-contact IC media only a certain distance from the mobile communication device
Place the information storage area inside the portable communication device at a remote location.
Accommodating internal non-contact IC media with
The portable communication device can communicate with each non-contact IC media.
For transmitting and receiving the digital information independently of the mobile phone
One or more non-contact devices having an information recording area in the communication device
A mechanism is provided for supporting IC media in a replaceable manner.
Non-contact IC media can be used as SIM
Coin-type non-contact IC media and individual non-contact IC media
Predetermined service information to be transmitted to contact IC media
To record permission information for receiving
The communication device may be a mobile phone radio.

Further, the non-contact method according to the present invention for solving the above-mentioned problems.
IC media is computer-readable digital information.
-Contact IC module having a recording area for recording information
Tool embedded in a sheet-like medium of a predetermined shape.
Non-peelable sticking part on at least one surface of the sheet-like medium
There is a sticking member that can be attached again after the material or peeling
It is characterized by the following. The sheet shape makes it easy to carry
And paste it on business cards or postcards.
Business card information including data or encrypted sealed information
Can also be recorded.

It is to be noted that one non-contact medium is provided for one seed medium.
Not only the structure with embedded IC module but also
Embedded multiple non-contact IC modules in
There are various non-contact IC modules and the attaching member
Make the area including the part cut out in a specific shape.
May be. Non-contact IC media with such a structure is
industrialization is possible, and significant cost reduction is expected
is done. It also makes it easier for users to carry
It is profitable.

From the viewpoint of the convenience of possession, the non-contact
It has a structure that allows the IC module to be
It can be embedded in a stick medium
You.

According to the present invention, there is provided a solid-state medium supported by a medium carrier.
It also provides non-contact IC media in the form of a body. This non-contact I
C media is a non-contact IC module having a recording area
Has a solid-type module medium with a predetermined shape embedded with
You. Modular media is only displaced by its own position.
An engagement mechanism that allows engagement and disengagement with the media carrier
Integrally formed, easily detached from media carrier
It is characterized in that it cannot be done.

Compatibility in use with existing contact-type IC cards
When it is necessary to maintain the electrical connection,
Table of the non-contact IC module for the conductive member for making
On the surface, and has a recess of the same shape as the media carrier.
Contact type when carried in the recess of the card medium
An IC card is formed.

[0025]

[0026]

[0027]

[0028]

[0029]

[0030]

Next, embodiments of the present invention will be described in detail with reference to the drawings.

1. Embodiment of Non-Contact IC Media First, an embodiment of a non-contact IC medium of the present invention will be described. (1) Sheet-shaped non-contact IC medium FIG. 1A is a front view of a sheet 1a on which a plurality of circular non-contact IC media 11 are formed, and FIG. FIG. 5 is a front view of a plurality of formed sheets 1b. The sheets 1a and 1b have cutouts 11 along the outer periphery of each of the non-contact IC media 11 and 12, respectively.

a, 12a are formed so that the non-contact IC media 11, 12 can be cut out one by one at the time of use. Individual non-contact IC media 11, 12
For example, a non-contact IC module is embedded in a sheet medium made of a thin resin, for example, and a sticking member is attached to the entire back surface or a part thereof. The sheet medium is subjected to surface processing so that printing or the like can be performed, and waterproof processing or the like is performed as necessary. The sticking member is stuck to a card medium by using a non-peelable resin adhesive when the sticking member is used for a purpose that needs to maintain security, for example, by sticking it to a finance card or the like. For applications where security is not always required, contactless I
After the C media 11 and 12 are peeled off from the pasted portion, the material can be re-attached to another portion. The latter attachment member can be realized more simply by using a slow-drying adhesive. A structure may be employed in which a magnetic agent is attached to the non-contact IC module through a shield member that performs magnetic shield.

As the non-contact IC module, a known module having a radio transmitting / receiving circuit including an antenna and an IC unit can be used. The IC unit is provided with at least a recording area for digital information and a control circuit for controlling writing and reading of data between the radio transmitting / receiving circuit and the recording area. The recording of digital information in the recording area
This may be performed afterward through a non-contact reader / writer, which will be described later, or may be performed in advance when generating a module. When the above control circuit can be replaced by a reader / writer, the control circuit of the IC unit may be omitted.

The non-contact IC media 11 and 12 having such a structure can be attached to an arbitrary position where the non-contact reader / writer can read digital information from its recording area. For example, non-contact IC media 11 and 12
Can be used by attaching to a non-contact reader / writer body, or can be used by attaching to an electronic device equipped with a non-contact reader / writer.

The non-contact IC media 11 and 12
Record personal and company profiles, addresses, telephone numbers, etc. in the form of textual information and image information, paste them on the back of business cards or pamphlets, and distribute them to the other party, and print information to be printed on non-contact IC media. Record on 11 and 12,
A non-contact IC which pastes this on printed matter, records information to be mailed on non-contact IC media 11 and 12 and pastes it on postal matter, or records company advertising information composed of multimedia data A usage form in which the media 11 and 12 are pasted and distributed on a reelet of "company information" becomes possible. If you want to paste it on the back of a business card,
By printing a company logo or the like on the surface of the non-contact IC media 11 and 12 and attaching it to a predetermined position on the backing paper, an "electronic business card" that does not seem uncomfortable with a normal business card
Can be realized. The advantages of realizing an electronic business card are as follows. -It becomes unnecessary to manually input data when editing and managing business card information with an electronic device. The business card information can be used as it is for a device that performs automatic telephone dialing based on telephone number information or a device that sets a destination for navigation based on address information. -Information such as company information, product catalogs, business information, announcements, and contracts other than the information printed on the mount surface can also be recorded. -Voice information is recorded as digital data together with business card information, so that multifaceted expression of personal information and company information becomes possible. -When going to the customer, it is sufficient to bring one electronic business card and have it read by the reader / writer at the customer, and it is not necessary to bind a pamphlet or carry it. -A non-contact IC medium whose recording information is changed depending on the use can be arbitrarily selected. For example, in a case where only the name, address, telephone number, and the like need to be distributed, it is sufficient to prepare a small-capacity electronic business card, and it is not necessary to always distribute an expensive electronic business card having a large memory capacity for recording all information.

Further, digital content including periodical article information such as newspapers and magazines, and sound data such as photographic images, graphic images, voices, BGM, bird voices, etc. is transmitted to a plurality of non-contact IC media 11 and 12. It is also possible to record at the same time and sell them one by one. On the side receiving such non-contact IC media 11, 12,
For example, digital information is read from the recording area through a non-contact reader / writer described later or a normal non-contact reader / writer, and necessary information processing, display processing on a display device, and the like are performed. In addition, the non-contact IC media of the present invention uses the sheet 1
In addition to the form of embedding in a and 1b, a form in which a single non-contact IC module is embedded in a sheet medium is possible. For example, it is possible to embed a non-contact IC module in a postcard to obtain an "IC postcard", or to embed a non-contact IC module in the above-mentioned business card mount to obtain an "IC business card mount".

(2) Stick-shaped non-contact IC medium FIG. 2 is an external view showing an example of a stick-shaped non-contact IC medium. This non-contact IC medium 13 is a stick-shaped medium 1 provided with a recess 1d having the same shape as the upper end of a stick-shaped casing, for example, a pen-shaped casing such as a writing instrument.
A non-contact IC module is embedded in c.
In the non-contact IC medium 13 having such a structure, the recorded information can be read out or digital information can be recorded simply by bringing the upper end of the pen-shaped housing close to a non-contact type reader / writer (not shown). Can be. IC
A unit in which only a data recording area is formed without a processor in the unit can be used, for example, for purposes of recording data for the time being or recording of digital information dedicated to reproduction. In the case where a processor and an application program recording area are formed in the IC unit in addition to the data recording area, more advanced information processing, for example, the result of execution of the application program by the processor is transmitted to the reader / writer, or Can be temporarily stored in the data recording area.

(3) Solid Non-Contact IC Media The non-contact IC media of the present invention is not limited to sheets and sticks, and can be embodied as solid media of a certain shape. Here, an example of a coin-type medium is shown as an example. This coin-type media is provided in a media holder (media carrier) provided in a portable audio device, a notebook personal computer, a portable game machine, a digital camera, a cellular phone radio, a portable terminal (PDA), a watch, a card medium, and the like. It is supported and used in a replaceable state.

The coin-type medium is formed by embedding a known non-contact IC module in a coin-shaped module medium. The coin-shaped module medium basically has a simple structure that can be carried by the media holder, but when used in a state exposed on the media holder, for example, make sure that the module medium does not come off during use. Therefore, it is necessary to devise its shape and structure. In this embodiment,
An engagement mechanism that allows engagement and disengagement with the media holder only by displacing its own position is integrally formed.

This engagement mechanism corresponds to the media engagement mechanism 31 on the media holder side illustrated in FIG. 3 (a), and its specific structure is, for example, as shown in the upper part of FIG. 3 (b). Become. That is, the coin-shaped module medium 10
is integrally formed with the projection 10a which can be engaged with the media engagement mechanism 31. In use, as shown in FIG. 3C, the module medium 10 is inserted into the medium engaging mechanism 31 and rotated to engage. To disengage, rotate in the direction opposite to the direction of engagement.

It is to be noted that, instead of the structure shown, a hinge body whose thickness changes in a tapered shape in the engagement direction is integrally formed on a part of the outer peripheral portion of the module medium, and the medium engagement mechanism is provided with a hinge. If the structure is such that the module medium can be engaged when the thickness of the body reaches the end of the taper, the shapes and structures of the module medium and the media holder can be further

simplified. Also, the above description is an example of a coin-type medium, but a plug-type medium and other types of solid-type media are also formed with a similar engagement mechanism so as not to be easily detached from the media holder. be able to Needless to say, even if the sheet-shaped non-contact IC medium 11 of FIG 1A is pasted on a coin-shaped module medium, it can be used as the above-mentioned coin-type medium.

When the media holder is a card medium having the same shape as that of a general-purpose IC card, and it is desired to use the solid-type medium as a contact-type IC card in addition to a non-contact IC card in a state where the medium is exchangeably supported. If non-contact I
A conductive member is deposited or adhered on the surface of the C medium. This conductive member is for conducting to a contact of an external electronic circuit, and is normally connected in parallel with a contact portion between the wireless transmitting / receiving circuit and the IC unit. The conductive member is a sheet-shaped non-contact IC shown in FIGS. 1 (a) and 1 (b).
It may be deposited or adhered to the surfaces of the media 11 and 12.

2. Non-contact reader / writer Next, for using the non-contact IC media of the present invention,
Or contactless IC using with noncontact IC media
An embodiment of a non-contact reader / writer for realizing the same function as a function given to a medium will be described. Here, an example in which a coin-type medium 20 without the above-described engagement mechanism 10a is used as the non-contact IC medium will be described. The above-mentioned sheet-shaped non-contact IC medium 11 can also be used as a coin-type medium 20 by sticking it on a coin-shaped module medium.

(1) First Embodiment FIG. 4 is a configuration diagram of a first embodiment of a non-contact reader / writer, which is a basic configuration of another non-contact reader / writer. The non-contact reader / writer 40 has an antenna 42 interposed between a media holder 41 for holding an internal coin-type medium 20b and another external coin-type medium 20a. This antenna 42
is usually embedded in the housing lid of the non-contact reader / writer. A transmission / reception circuit 43 is connected to the antenna 42, and a control unit 44, a power supply unit 47, and a clock supply unit 48 are connected to the transmission / reception circuit 43. The power supply unit 47 outputs a power component superimposed on a carrier wave in the transmission / reception circuit 43.
Reference numeral 8 similarly outputs a clock component having a predetermined period to be superimposed on a carrier wave. The control unit 44 controls reading of recorded information from the memory (M) 45, control of writing to the memory 45, timing control of transmission / reception waves in the transmission / reception circuit 43, and an external electronic circuit through an external interface (I / F) 46. Control of information exchange between the server and the server. In addition, it also has a function of preventing congestion between a plurality of coin-type media using a known anti-collision method.

Each of the coin-type media 20a and 20b includes at least an antenna 21, a transmission / reception circuit 22, and a control circuit 2.
3 and a memory 24. Control circuit 23
Generates a power supply clock and a clock based on the power component and the clock component received from the non-contact reader / writer 40 through the antenna 21 and the transmission / reception circuit 22, and prepares the operating environment of the non-contact module. Further, while controlling data writing ("data IN") to the memory 24 and data reading ("data OUT") from the memory 24, the read data and commands are transmitted through the transmission / reception circuit 22 and the antenna 21 in a non-contact manner. It is transmitted to the reader / writer 40 side. In the memory 24, identification data for identifying the coin-type medium, user-specific data, simple application programs, data, digital contents, and the like are recorded as necessary.

When used for applications requiring security, the coin-type medium 20b is provided with a processor as one of information processing means, and the memory 24 is provided with an encryption key and a decryption key readable by the processor. And the encryption algorithm. This enables the non-contact reader / writer 40 to realize the same function as the function given to the coin-type medium 20b, that is, the encryption function and the decryption function. Similarly, when an application program in an executable format is recorded in the memory 24 of the coin-type medium 20b, the application program can be executed by the non-contact reader / writer 40. Also, The execution result of the application program can be recorded in the memory 24 of the coin-type medium 20b.

Transmission and reception of information between the non-contact reader / writer 40 and the coin-type media 20a and 20b can be realized in the same operating environment as a normal non-contact reader / writer and non-contact IC card. For example, when transmitting information from the non-contact reader / writer 40 to the coin-type media 20a and 20b, a wireless carrier of 13 56 [MHz] is transmitted using ASK.
13.56 for transmitting the modulated signal and information from the coin-type media 20a and 20b to the non-contact reader / writer 40.
[MHz] subcarriers (847.5)
/423.7 [kHz]) can be used. A clock component and a power component are sent from the non-contact reader / writer 40 to the coin-type media 20a and 20b in addition to the data component, similarly to the case of the conventional non-contact IC card.

The non-contact reader / writer 40 configured as described above is controlled by the
0b and the external coin-type media 20a in the area covered by the antenna 42 can be controlled to read and write information. This point is a function that does not exist in the conventional contactless reader / writer. Even if two coin-type media 20a and 20b are present at the same time,
In addition to the above-described anti-collision function, the identification data recorded in the memory 24 of each of the coin-type media 20a and 20b and the user's unique data can be easily identified by decoding the identification data. Absent.

(2) Second Embodiment FIG. 5 is a configuration diagram of a non-contact reader / writer as a modification of the first embodiment. For convenience, elements having the same functions as in FIG. I have. This non-contact reader / writer 50 is provided with two wireless transmission / reception systems including an antenna and operates independently.

That is, the antenna 42a and the transmission / reception circuit 43 communicate with the coin-type medium 20a existing outside.
a, the power supply unit 47a, and the clock supply unit 48a are operated. On the other hand, the antenna 42b and the transmission / reception circuit 43
b, the power supply unit 47b, and the clock supply unit 48b. The control unit 44 grasps the operating conditions of both, and selectively performs read control and write control of digital information with respect to the recording area of the external coin-type medium 20a and / or the carried coin-type medium 20b. .

The non-contact reader / writer 50 having the above configuration
In this case, data transmission and reception are performed between the external coin-type media 20a and the internal coin-type media 20b through wireless transmission / reception systems that are independent of each other, so that the problem of congestion is less likely to occur. (3) Third embodiment

FIGS. 6 and 7 are configuration diagrams of non-contact reader / writers 55 and 56 capable of simultaneously supporting a plurality of coin-type media 20 on the media holder 51. For convenience, components having the same functions as those in FIG. Are denoted by the same reference numerals. FIG. 6 shows a case where one antenna 42 is used, and FIG.
This is an example in which two antennas 42a and 42b are used.

In the case of the non-contact reader / writer 55 shown in FIG. 6, the control unit 44 performs data read control or data write control with a plurality of coin-type media 20 at different timings, or executes different commands. Data read control or data write control is performed only on the one for which the response is returned after transmission. By doing so, it becomes possible to selectively execute a plurality of application programs while simultaneously carrying the coin-type media 20.

in the case of the non-contact reader / writer 56 shown in FIG.
Performs read control or write control of data under one of the antennas 42a and the other antenna 42b under different conditions depending on the application. For example, high-speed data reading is performed using the antenna 42a in applications requiring real-time performance, and low-speed and high-quality data reading is performed using the antenna 42b in applications requiring higher quality than time. In this way, multipurpose data processing according to the application can be performed. Although not described, data read control or data write control can be performed with an external coin-type medium through the antennas 42 and 42a, respectively.

(4) Fourth Embodiment FIG. 8 shows a media holder 52 capable of carrying a plurality of coin-shaped media 20 arranged on the same plane, and one antenna 42 between the coin-shaped media 20.
FIG. 2 is a configuration diagram of a non-contact reader / writer 57 that performs data read control or data write control through the controller. For convenience, elements having the same functions as those in FIG. 4 are denoted by the same reference numerals. Antenna 42
is embedded in the case lid, for example, in parallel with each coin-type medium 20. The basic operation is the same as that of the non-contact reader / writer 55 shown in FIG. FIG.
FIG. 9 is a configuration diagram of a non-contact reader / writer 58 in which the same number of antennas 42 as the coin-shaped media 20 arranged in the media holder 52 shown in FIG. 8 are arranged. Each antenna 42
It is embedded in the housing lid in parallel with the coin-type media 20. The basic operation is the same as that of the non-contact reader / writer 56 shown in FIG. 7, but the individual antennas 42 and the coin-shaped media 20 can be brought into close contact with each other, and the occurrence of interference and the like can be reduced. 8 has the advantage that it can be reduced

(5) Fifth Embodiment FIGS. 10A to 10D show the structure of a non-contact reader / writer that selects a specific one of a plurality of coin-type media and reads and writes data. FIG. This non-contact reader / writer is configured to house a movable media holder having a displacement mechanism in a housing and a wireless transmission / reception system including a contact antenna. The movable media holder is shown in FIG.
As shown in (a), a plurality of hollow portions 62 having the same shape as the coin-shaped media 20 are formed in an annular plate 61 having substantially the same thickness as that of the coin-shaped media 20, and the same hollow portion 62 is provided at the center thereof. Displacement mechanism 6 for rotating on a plane
3 is fixed. FIG. 10B is an internal structural view showing the positional relationship of the movable media holder in the housing 64, FIG. 10C is a top view of the housing 64, and FIG. It is a side sectional view. Reference numeral 61a
is a housing window for accommodating the coin-type medium 20 in the hollow portion 62 and detaching it, and 65 is a close-contact type antenna

A non-contact reader / writer 60 having such a structure
In this example, a plurality of coin-type media 20 storing different digital information, for example, application programs and security data, are housed in the hollow portion 62, and the user displaces the displacement mechanism 63 to bring the desired coin-type media 20 into close contact. It approaches the type antenna 65. The digital information read through the contact antenna 65 is transmitted to an external electronic device through a transmission / reception circuit 66 and an external interface circuit (not shown). In this manner, the corresponding coin-type media 20 can be properly used depending on the application.

It is needless to say that the annular plate 61 is merely an example, and that other shapes can be used. For example, there is also a structure in which a plurality of hollow portions are arranged in a rectangular plate or a fan-shaped plate, and these are reversibly slid on the same plane using a displacement mechanism such as gears to approach a close contact antenna . Within the scope of the present invention. Further, an antenna having directivity can be used instead of the close contact antenna.

(6) Sixth Embodiment FIGS. 11A to 11C show the structure of another non-contact reader / writer which selects a specific one of a plurality of coin-type media and reads and writes data. FIG. This non-contact reader / writer is configured by housing a fixed type media holder and a movable type reading / writing mechanism carrier having a media reading / writing mechanism including an antenna and a wireless transmission / reception system in a housing.

As shown in FIG. 11A, a plurality of hollow portions 72 for accommodating the coin-shaped media 20 are formed on an annular plate 71 having a thickness substantially equal to the thickness of the coin-shaped media 20, as shown in FIG. After the coin-type medium 20 is carried, the non-contact reader / writer is mounted at a predetermined position in the housing. Reference numeral 73 is a hole formed in the center of the annular plate 71.

FIG. 11B is a structural view of the reading / writing mechanism carrier. Here, an example in which an antenna, a wireless transmission / reception circuit, and a module subsequent thereto are modularized as a mechanism for reading / writing digital information from / to the coin-type medium 20 will be described. The reading / writing mechanism carrier fixes, for example, a support having a displacement mechanism 76 formed at the center of an annular plate 75 having substantially the same diameter as the annular plate 71, and slidably inserts this support into a hole 73 of the annular plate 71. A module 74 including an antenna is embedded in an intermediate portion of the annular plate 75 while being inserted. The module 74 is embedded at a position where its antenna comes into close contact with each of the plurality of coin-shaped media 20 by the rotation of the annular plate 75.

The non-contact reader / writer 70 having such a structure
Can be used in the same manner as in the fifth embodiment except that the module 74 including an antenna is displaced. In other words, when the user operates the displacement mechanism ring 76, the annular plate 75 rotates around the hole 73 as a fulcrum, and as shown in FIG. It can be closer to the media 20. It is needless to say that the annular plate 75 can be replaced with another shape like the media holder. Further, instead of the module 74, only the antenna and the radio transmission / reception circuit are embedded in the annular plate 75, and for the subsequent circuit, the non-contact reader / writer 70 is connected through electrical contacts provided along the rotation path of the annular plate 75. It may be configured to be connected to an internal circuit of an electronic device mounted.

(7) Seventh Embodiment FIG. 12A shows an electronic device operated by a battery.
FIG. 3 is a configuration diagram of a main part of a non-contact reader / writer mounted on, for example, a mobile phone wireless device or a PDA. The non-contact reader / writer 80 includes at least the antenna 42 embedded in the housing lid and the transmitting / receiving circuit 4 connected to the antenna 42.
3 and a charging circuit 81 connected to the output side of the transmission / reception circuit 43. The charging circuit 81 includes a constant voltage circuit 811 that supplies a constant voltage to a subsequent component of the reader / writer function and supplies a constant value of power to a charging terminal of the battery B stably. .

FIG. 12B is a configuration diagram of a main part of a non-contact reader / writer 85 mounted on a charging device for charging an electronic device. The non-contact reader / writer 85 includes an antenna 42 embedded in the housing lid, a transmission / reception circuit 43 connected to the antenna 42, and a power conversion circuit 86 for converting commercial power into charging power. This power conversion circuit 86 includes the power supply unit 47 shown in FIGS.
47a and 47b. The antenna 42 and the transmission / reception circuit 43 function as an electromagnetic induction coil that induces electric power on the electronic device side by electromagnetic induction when the charging device and the electronic device are brought close to each other. In use, as shown in FIG. 12C, the electronic device D1 is set near the charging device J1, and charging power is transmitted from the charging device J1 to the electronic device D1 through the non-contact reader / writer 85. In the non-contact reader / writer 80 on the electronic device D1 side, the electric power induced by the antenna 42 and the transmission / reception circuit 43 is input to the charging circuit 81. The charging circuit 81 stabilizes the induced power at a constant voltage circuit 811 to a constant value higher than the rated voltage of the battery B, and supplies this power to the charging terminal 82 of the battery B. Thereby, the battery B of the electronic device D1
is charged.

Usually, a dedicated charging device is prepared for the electronic device D1, and charging can be performed by setting the electronic device at a predetermined position of the charging device and bringing the contacts into contact with each other. Therefore, if the models and shapes are different, the charging device cannot be used. However, in the present embodiment, the battery can be charged regardless of the model and shape.

(8) Eighth Embodiment The non-contact reader / writer of the present invention can also be used by mounting it on a card medium such as a PC card. For example, a PC card 90 whose appearance is shown in FIG.
Has a medium holder 92 for accommodating a non-contact reader / writer 91 inside a housing and supporting the coin-type medium 20 in a detachable manner on a surface portion thereof. As shown in FIG. 13B, a non-contact reader / writer 95 having a media holder 96 for holding a plurality of coin-type media 20 may be mounted in the internal space 93 of the PC card 94. The coin-type medium 20 records application programs and data.

As shown in FIG. 13C, the PC cards 90 and 94 are used by being mounted on a card slot 97 of a personal computer or the like. Depends on the type. For example, the coin-type medium 20 is used as a removable recording device of a personal computer PC, used as a recording medium of a program code read and executed by the personal computer PC, or a transmission medium of electronic data read from an external electronic device. Can be used as in the case of a PC card having a communication function, a usage form in which communication environment data is stored in the coin-type media 20 is possible.

As shown in FIG. 14, the digital camera DC can be used as an image recording card. That is, the coin-shaped medium 20 is inserted into the card-shaped media holder 98, and the photographing data is recorded on the coin-shaped medium 20. After that, the image recording card 98 is inserted into the card slot 99 of the digital camera DC to store image data. By presenting the image recording card 98 to a photo lab or the like, it is possible to output a recorded image to photographic paper or to a high-resolution printer.

(9) Ninth Embodiment The non-contact IC reader / writer of the present invention is capable of reading and writing digital information (program code, data, etc.) to and from the coin-shaped media 20, 20a, 20b. May be configured to execute information processing based on the information. Specifically, it includes a processor for reading and executing digital information and a memory for recording required programs and the like. The processor and the memory are preferably formed as an IC chip and housed in a housing. The result of the information processing by the processor is output to a display or the like of an electronic device equipped with the non-contact IC reader / writer, and is recorded at a source from which digital information is read. Since the non-contact IC reader / writer configured as described above can perform information processing only by the processor inside, it is possible to reduce the range of design changes on the electronic device side on which the non-contact IC reader / writer is mounted. Further, it becomes easy to realize the same function as the function given to the coin-type medium based on the digital information recorded on the coin-type medium.

3. Portable Communication Device Next, an embodiment of a portable communication device equipped with the non-contact reader / writer will be described. Here, an example of a mobile phone wireless device will be described, but the present invention is not limited to this example.
In addition, a mobile phone radio is a mobile phone in a narrow sense,
S, portable transceivers, car phones, etc.

First, the non-contact reader / writers 40, 5
A mobile phone radio equipped with 0, 55, 56, 57, 58 will be described. These non-contact reader / writers may be incorporated in a mobile phone radio as it is, but here, an example of a mobile phone radio integrated therein will be described.

FIG. 15 is an external perspective view of a portable telephone radio 110 in which the non-contact reader / writer 40/50 shown in FIG. 4 or 5 is integrally mounted in a housing. A media holder 111 for holding the coin-type media 20 and a lid 112 thereof are formed in a lower rear portion of the mobile phone wireless device 110. The antenna 42 is embedded in the lid 112 of the housing, and is parallel to the coin-type medium 20 when the lid 112 is closed.

The portable telephone radio 11 constructed as described above
0, the coin-type media 20 is stored in a SIM (Subscr
iber Identity Module).
The subscriber ID is recorded in the SIM. Thus, when replacing the mobile phone radio 110 with another one or using the mobile phone radio 110 properly depending on the application, it is only necessary to replace the SIM. In addition, by replacing the SIM, it becomes possible to receive the same service through various mobile phone radios. That is, it becomes possible to use the portable telephone radio as a public telephone.

As shown in FIG. 16, in addition to the coin-shaped media 20b carried by the media holder 111,
Non-contact IC card ICC, coin-type media 20a, and other shapes of non-contact IC media 20 existing outside
Since digital information can be read from and written to both recording areas b ', the external non-contact IC card ICC, the coin-type medium 20 and the like can be read using the security information recorded on the internal coin-type medium 20. Embodiments that access the system are also possible. As in the ninth embodiment, when a non-contact reader / writer is provided with a processor or the like to read out security information or a program code recorded on an internal coin-type medium and execute required information processing, the processing result is obtained. It can also be recorded on the coin type media 20. For example, a form is possible in which electronic payment processing is performed by holding the mobile phone wireless device 110 over a POS terminal, a vending machine, a mobile payment terminal, or the like, and the result is recorded on a coin-type medium.

As other applications that can be realized by the portable telephone radio set 110, there can be cited ones for prepaid cards such as gift cards, novelty cards, ticket cards, and telephone cards. In addition, it is also possible to apply the present invention to electronic payment by taking the prepaid value inside by holding the mobile phone wireless device 110 over the prepaid card. Mobile phone radio 11
0 itself, the name in the memory area of the coin-type medium 20,
The address can be written and the coin-type medium 20 can be used as an electronic business card. Further, by merely holding the mobile phone wireless device 110 over the electronic business card of the other party, it is possible to read and write data from and to the electronic business card, thereby improving convenience. Further, the identification data and key information of the owner of the car are recorded on one of the coin-type media, and the mobile phone wireless device 110 is used as an electronic key. It can also be used for analysis of flight history.

Further, as shown in FIG. 17, the portable telephone radios 110 are brought close to each other, and
0b can be exchanged.

The coin-type media 20 can carry not only one, but a plurality of them at the same time. FIG. 18 is a cross-sectional view of a mobile phone radio 120 having a media holder 121 on which a plurality of coin-type media 20 can be stacked. The antenna 42 is embedded in the lid 122. This portable telephone radio 120 has the non-contact reader / writer 55 shown in FIG. 6 integrally mounted thereon. FIG.
FIG. 8 is a cross-sectional view of the mobile phone wireless device 130 in which the non-contact reader / writer 56 shown in FIG.
2 a is embedded in the housing lid 132, and the antenna 42 b is embedded in the bottom 133 of the media holder 131. FIG. 20 shows FIG.
FIG. 21 is a cross-sectional view of a mobile phone wireless device 140 integrally mounted with the non-contact reader / writer 57 shown in FIG. 21. FIG. 21 is a mobile phone wireless device 1 integrally mounted with the non-contact reader / writer 58 shown in FIG.

It is sectional drawing of 50. The antenna 42 is embedded in the lids 142 and 152 corresponding to the media holders 141 and 151, and when closed, the coin-shaped media 2
It adheres in parallel with 0. The non-contact reader / writer 60 having the structure shown in FIG. 10 or FIG.
It is also possible to provide 70 integrally in the mobile phone radio.

The mobile phone radios 110 to 150 usually have a display and a sound generation mechanism. Therefore, the chip including the processor and the like described in the ninth embodiment is mounted so that required information processing can be executed based on digital information read from a plurality of coin-type media 20.

The processor forms a sound source controller that reproduces sound based on the sound source data by executing the program code stored in the memory, and a display controller that displays an image on a display based on the image data. Sound source data is recorded on one of the coin-shaped media 20, and image data output in cooperation with the sound source data is recorded on the other coin-shaped media 20. Then, the sound source data is read out, and the sound source controller causes the sound generation mechanism to reproduce sound, and an image is displayed on the display based on the image data read out in synchronization with the sound source data. The mobile phone wireless devices 110 to 150 configured as described above can display character data on a display by appropriately replacing and using the coin-type media 20, and can use a sound or BGM (background / voice) corresponding to the character data. Music) can be heard with a receiver or earphone. For example, a mobile phone radio can be used as a "portable karaoke machine". That is, it is also possible to display the lyrics on a display, sing a song while listening to the melody with an earphone, and record the sung content. An embodiment in which only character data is displayed or only sound is generated based on sound source data is also possible. The above description is about a mobile phone radio,
The present invention can be similarly applied to a personal computer, a portable terminal (PDA), a portable audio device, and the like.

4. Next, an embodiment of an information transmission system to which the present invention is applied will be described. Here, an example in which information is transmitted using the above-described non-contact IC media and a portable communication device will be described.
As the mobile communication device, for example, a mobile phone wireless device 110 is used. The mobile phone wireless device 110 is equipped with a non-contact reader / writer incorporating the above-described processor and the like. When a non-contact reader / writer is used, a corresponding function is assigned to one of the operation buttons of the mobile phone wireless device 110.

(1) Periodical article publishing system This is a system in which articles such as newspapers, weekly magazines, and monthly magazines are converted into digital information while being periodically updated and provided to the user. FIG. FIG. The digital information referred to here is character data, image data, digital content, and the like, and includes sound source data as necessary. Non-contact IC for recording this digital information
As the medium, for the sake of convenience, the coin-type medium 2 described above is used.
Although 0 is used, it goes without saying that a sheet-shaped medium may be used.

This periodic publication article issuing system 200
It comprises a mobile phone radio 210 that carries the coin-shaped media 20 in an exchangeable manner, and a media issuing device 220. The media issuing device 220 is connected to the display 22
1, a data input device 222, a money input mechanism 223, an input / output interface 224, an article database DB, a media issuing mechanism 229, and a menu display section formed by reading and executing a predetermined program code by an internal processor. 225, article identification unit 22
6, a functional block of a database management unit 227 and an information recording unit 228.

The menu display section 225 causes the display 221 to display a menu screen for guiding published articles handled by the apparatus itself through the input / output interface 224. The data input device 222 is for inputting selection information of a published article. The article specifying unit 226, when receiving selection information of a specific article from the data input device 222 and money input information (value information) from the money input mechanism 223, manages information for specifying the published article in a database. Notify section 227. Database management unit 227
Reads digital information from the article database DB based on this information, and passes it to the information recording unit 228. The information recording unit 228 records this digital information on the coin-type medium 20 and issues it.

On the menu screen, guide information of a published article of a type and content corresponding to the amount is displayed, and the user can arbitrarily select the information through the data input device 222. The contents of the article database DB are periodically updated by the database management unit 227 based on, for example, data sent from an external system. Published articles to be updated are updated daily for newspapers, weekly for weekly magazines, and monthly for monthly magazines. The user purchases the coin-type media 20 on which digital information is recorded from the media issuing device 220, puts it into the media holder of the mobile phone radio 210, presses an operation button, and displays the recorded information on the display 211. Coin type media 2
If the sound source data is also recorded in 0, the content is heard with a receiver or earphone. In addition, the information transmission system of the present invention can be applied to a system that issues digital contents regularly or irregularly, in addition to periodical article information.

(2) Information guide system Address, postal code, map and map code, area guide, facility guide, timetable, business guide, etc. are converted into digital information and recorded on a non-contact IC medium. Embed it in the appropriate place and attach or paste it. Then, the relevant information is read from the plate using a portable communication device equipped with the non-contact reader / writer of the present invention having at least an image controller, for example, a portable telephone radio, and displayed on a display. The installation location of the plate, for example,
"Address etc." is a building or telephone pole, "Map and map code" is an address display board, "Regional information" is the building outer wall, "Facility information" is the entrance of the facility, "Timetable" is the wall of the station platform, "Sales" The "information" shall be the entrance to the store or office.

The user presses the corresponding operation button and holds the portable telephone radio over these plates. As a result, the reader / writer function of the mobile phone radio operates to read out digital information, visualize it, and display it on the display.

It is to be noted that a plurality of non-contact IC media can be embedded or attached to the same guide panel on which guide information is drawn. In addition, it is possible to provide a service for distributing venue guidance information simply by placing a gate having a built-in non-contact reader / writer at the gate of a concert or sports venue and allowing the user to hold the portable telephone radio over the gate.

[0086]

As is apparent from the above description, according to the present invention, a non-contact IC medium having excellent versatility can be obtained. Further, it is possible to provide an application system that can add more added value by using the non-contact IC media.

[Brief description of the drawings]

FIG. 1A is a front view of a sheet on which a plurality of circular non-contact IC media are formed, and FIG. 1B is a front view of a sheet on which a plurality of plug-type non-contact IC media are formed.

FIG. 2 is an external perspective view of a stick-type non-contact IC medium.

FIG. 3 is an explanatory diagram of an engagement mechanism that allows engagement and disengagement with a media holder only by displacing its own position; (A) is a front view of the media engaging mechanism on the media holder side, (b) is an explanatory diagram of the engaging mechanism on the module media side, (C) is an explanatory view showing a use state.

FIG. 4 is a configuration diagram of a first embodiment of a non-contact reader / writer.

FIG. 5 is a configuration diagram of a second embodiment of a non-contact reader / writer.

FIG. 6 is a configuration diagram of a non-contact reader / writer according to a third embodiment, which is an example in the case of one antenna.

FIG. 7 is a configuration diagram of a third embodiment of a non-contact reader / writer, which is an example in a case where there are two antennas

FIG. 8 is a configuration diagram of a fourth embodiment of a non-contact reader / writer, which is an example in the case of one antenna.

FIG. 9 is a configuration diagram of a fourth embodiment of a non-contact reader / writer, in which the number of antennas is the same as that of coin-type media.

FIGS. 10A to 10D are configuration diagrams of a non-contact reader / writer according to a fifth embodiment. FIGS. 10A to 10D illustrate non-contact non-contact reader / writers that select a specific one of a plurality of coin-type media and read and write data. FIG. 3 is a diagram illustrating a structure of a reader / writer.

FIGS. 11A to 11C are configuration diagrams of a non-contact reader / writer according to a sixth embodiment. FIGS. 11A to 11C illustrate non-contact non-contact reader / writers that select a specific one of a plurality of coin-type media and read and write data. FIG. 3 is a diagram illustrating a structure of a reader / writer.

12A and 12B are configuration diagrams of a non-contact reader / writer according to a seventh embodiment, in which FIG. 12A is a configuration diagram of a main part of a non-contact reader / writer mounted on a mobile phone wireless device operated by a battery,
(B) is a main part configuration diagram of a non-contact reader / writer mounted on the charging device, and (c) is a use state explanatory diagram at the time of charging.

FIGS. 13A and 13B are configuration diagrams of a non-contact reader / writer according to an eighth embodiment, in which FIGS. 13A and 13B illustrate a structure of a PC card on which the non-contact reader / writer is mounted, and FIG. P
it is explanatory drawing of the usage form of a C card.

FIG. 14 is an explanatory diagram illustrating a use state of an image recording card of a digital camera equipped with a non-contact reader / writer.

FIG. 15 is an external perspective view of a mobile phone wireless device in which the non-contact reader / writer shown in FIG. 4 or 5 is integrally mounted.

FIG. 16 is a conceptual explanatory diagram showing an example of a usage mode of a mobile phone wireless device.

FIG. 17 is a conceptual explanatory view showing another usage pattern of the mobile phone radio.

FIG. 18 is a cross-sectional view of a portable telephone radio equipped with a non-contact reader / writer capable of stacking a plurality of coin-type media.

FIG. 19 is a cross-sectional view of a mobile phone wireless device on which a plurality of coin-type media can be stacked and a non-contact reader / writer equipped with a plurality of antennas is mounted.

FIG. 20 is an external perspective view of a mobile phone wireless device in which a plurality of coin-type media can be arranged in parallel and a non-contact reader / writer with one antenna is mounted.

FIG. 21 is an external perspective view of a mobile phone wireless device in which a plurality of coin-type media can be arranged in parallel and the antenna has the same number of non-contact reader / writers as the coin-type media.

FIG. 22 is a configuration diagram of a system that converts articles such as newspapers, weekly magazines, and monthly magazines into digital information while periodically updating them, and provides the digital information to users.

[Explanation of symbols]

1a, 1b Sheet embedded with non-contact IC module 1c Stick medium embedded with non-contact IC module 10, 11, 12, 13, 20, 20, 20a, 20b Non-contact IC media 10 Engagement mechanism on media side 31 Media carrier side Media engagement mechanism 21, 42, 42a, 42b, 65 Antenna 22, 43, 43a, 43b, 66 Transmission / reception circuit 23 Control circuit 24, 45 Memory 40, 50, 55 to 58, 60, 70, 80, 85, 9
1,95,98 Non-contact reader / writer 41,51,52,61,71 Media carrier 44 Control unit 46 External interface circuit 47,47a, 47b Power supply unit 48,48a, 48b Clock supply unit 63,76 Displacement mechanism 81 Charging circuit 110-150, 210 Mobile phone radio 200 Periodical article issuing system 220 Media issuing device 223 Money input mechanism 224 Input / output interface 225 Menu display section 226 Article specifying section 227 Database management section 228 Information recording section 229 Media issuing mechanism D8 Article database ICC non-contact IC card D1 Electronic device equipped with non-contact reader / writer J1 Charger for electronic device

----------続き Continuation of the front page (51) Int.Cl. [7] identification code FI H04B 7/26 109H
(56) References JP-A-1-190496 (JP, A) JP-A-61-277495 (JP, A) JP-A-4-145593 (JP, A) JP-A-8-230367 (JP, A) JP-A-8-118860 (JP, A) JP-A-5-124384 (JP, A) JP-A-1-111363 (JP, U) JP-A 61-180758 (JP, U) JP-A 1-59670 (JP, U) JP-A 1-123269 (JP, U) (58) Fields surveyed (Int. Cl. [7]) G06K 19/00-19/07 G06K 17/00 H04B 5/02 H04Q 7/38

Patent Citations (53)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US4277837A	1977-12-30	1981-07-07	International	Personal portable terminal for financial transactions

			Business Machines Corporation	
JPS61180758A	1985-02-07	1986-08-13	Showa Roodeia Kagaku Kk	Production of aminobenzonitrile compound
JPS61277495A	1985-06-04	1986-12-08	Nec Corp	Electronic business card
JPS63246292A	1987-04-01	1988-10-13	Toshiba Corp	ic card
CH673744A5	1987-05-22	1990-03-30	Durgo Ag	
JPS6459670A	1987-08-31	1989-03-07	Canon Kk	information signal recorder
JPH01111360A	1987-10-26	1989-04-28	Nec Corp	Manufacture of semiconductor device
JPH01190496A	1988-01-26	1989-07-31	Kazumasa Sasaki	Electronic name card and processor
JPH0262295A	1988-08-29	1990-03-02	Matsushita Electric Ind Co Ltd	information medium, conveying body therefor and reader thereof
US5049728A *	1990-04-04	1991-09-17	Rovin George H	IC card system with removable IC modules
JPH04145593A	1990-10-05	1992-05-19	Koatsu Gas Kogyo Co Ltd	Physical distribution management system
JPH04178689A *	1990-11-14	1992-06-25	Hitachi Ltd	information providing device and information reader
JPH07120473B2	1991-08-12	1995-12-20	リズム時計工業株式会社	Information vending machine
JPH04321190A	1991-04-22	1992-11-11	Mitsubishi Electric Corp	Antenna circuit and its production for non-contact type portable storage
DE4132720A1	1991-10-01	1993-04-08	Gao Ges Automation Org	CHIP CARD AND METHOD FOR THE PRODUCTION THEREOF
CA2079517A1	1991-10-01	1993-04-02	Michael C. Ryan	Method for identifying a penetrable member
JPH0530874U	1991-10-02	1993-04-23	三菱重工業株式会社	Flexible IC tag
JPH0583866U	1992-04-15	1993-11-12	日廣電工株式会社	ID tag
JPH06119552A *	1992-10-02	1994-04-28	Sony Corp	Information providing system
US6003779A *	1992-10-06	1999-12-21	Interdigital Technology Corporation	Wireless telephone debit card system and method
DE4313049C2	1993-04-21	1996-05-15	Michael L Hoeffgen	Shipping container
US5581065A *	1993-08-02	1996-12-03	Dai Nippon Printing Co., Ltd.	Sheet-framed IC carrier, method for producing the same, and IC carrier case
JPH07239922A	1994-02-25	1995-09-12	Dainippon Printing Co Ltd	ic module for ic card
JPH07325895A *	1994-05-31	1995-12-12	Toshiba Corp	Radio medium processor
DE9411619U1	1994-07-18	1994-09-22	Koehler Juergen	Reusable phone card
DE4431754C1 *	1994-09-06	1995-11-23	Siemens Ag	Carrier element for ic module of chip card
JPH08129630A	1994-09-09	1996-05-21	Hitachi Maxell Ltd	Portable information storage device and reader writer therefor
GB9422803D0 *	1994-11-11	1995-01-04	At & T Global Inf Solution	A card reader
JPH08186513A *	1994-12-27	1996-07-16	Toshiba Corp	Radio card communication equipment
SE506506C2 *	1995-04-11	1997-12-22	Au System	Electronic transaction terminal, telecommunication system including an electronic transaction terminal, smart card as electronic transaction terminal and method of transferring electronic credits
DE19517818C2 *	1995-05-18	1997-12-18	Angewandte Digital Elektronik	Method for issuing individual chip cards to a plurality of individual chip card users using a neutral chip card dispensing station
JPH0922449A	1995-07-05	1997-01-21	Tokai Rika Co Ltd	Transmission-reception system
US5640002A *	1995-08-15	1997-06-17	Ruppert; Jonathan	Portable RF ID tag and barcode reader

			Paul	
CN1183584A *	1995-09-29	1998-06-03	伸神鉄	Method and apparatus for control of production process
JPH09104189A *	1995-10-09	1997-04-22	Denso Corp	Information recording medium, method and device for its production
US6036099A *	1995-10-17	2000-03-14	Leighton, Keith	Hot lamination process for the manufacture of a combination contact/contactless smart card and product resulting therefrom
DE19539851C2	1995-10-26	1999-01-07	Daimler Benz Ag	Key vehicle communication device for controlling an immobilizer and a remote-controlled function
FR2743649B1 *	1996-01-17	1998-04-03	Gemplus Card Int	CONTACTLESS ELECTRONIC MODULE, ELECTRONIC LABEL CARD INCORPORATING THE SAME, AND METHODS OF MAKING SAME
EP0788069A3	1996-02-01	2000-01-19	Kaba Schliessysteme AG	Wearable identification carrier
FR2745103B1 *	1996-02-15	1998-04-03	Bourgogne Grasset	STORAGE DEVICE FOR GAME TOKENS
JPH09244567A	1996-03-06	1997-09-19	Masayuki Oguri	Guiding information device
US5850187A *	1996-03-27	1998-12-15	Amtech Corporation	Integrated electronic tag reader and wireless communication link
JPH09312076A	1996-05-23	1997-12-02	Nippon Columbia Co Ltd	Container for housing recording media and recording/ reproducing device
JPH1092673A	1996-07-26	1998-04-10	Tdk Corp	Non-contact power transmission device
SG54559A1 *	1996-09-13	1998-11-16	Hitachi Ltd	Power transmission system ic card and information communication system using ic card
JPH1097599A *	1996-09-24	1998-04-14	Hitachi Ltd	Portable terminal equipment for ic card
DE19640304C2 *	1996-09-30	2000-10-12	Siemens Ag	Chip module in particular for implantation in a chip card body
EP0845755B1 *	1996-12-02	2004-03-10	Swisscom Mobile AG	IC-card and program for IC-cards
DE19701167A1 *	1997-01-15	1998-07-23	Siemens Ag	Smart card
US6329213B1 *	1997-05-01	2001-12-11	Micron Technology, Inc.	Methods for forming integrated circuits within substrates
JPH11205334A *	1998-01-16	1999-07-30	Mitsubishi Electric Corp	Recognition system and recognition method for contactless ic card
US6173899B1 *	1998-04-03	2001-01-16	Alexander Rozin	Method and system for contactless energy transmission and data exchange between a terminal and IC card
US6062887A *	1998-08-31	2000-05-16	Motorola, Inc.	Electronic device with dual card reader employing a drawer

* Cited by examiner, † Cited by third party

Cited By (69)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US5834871A	1996-08-05	1998-11-10	Puskas, William L.	Apparatus and methods for cleaning and/or processing delicate parts
JP4541465B2 *	1998-09-10	2010-09-08	ミルストーントラン スファーエージー、エル、エル、シー、	Electronic tag, electronic tag identification system
US7181429B1	1999-04-27	2007-02-20	Booil Mobil Telecomm. Corp.	Apparatus and method for storing electronic money
JP2001160105A	1999-09-22	2001-06-12	Sony Corp	Information processing system, portable telephone set, and information processing method
MY133933A	2000-05-24	2007-11-30	Ericsson Telefon Ab L M	Method and apparatus for buyer identification
DE10035152A1 *	2000-07-19	2002-01-31	Siemens Ag	Electronic business card

JP4494607B2 *	2000-08-17	2010-06-30	日本信号株式会社	Logistics management device
JP2002083250A *	2000-09-11	2002-03-22	Dainippon Printing Co Ltd	Commodity information system and portable information terminal used therefor
JP4686024B2 *	2000-11-28	2011-05-18	大日本印刷株式会社	Poster with RF-ID tag
KR100825199B1	2000-12-20	2008-04-24	엘렉스피 비 브이	Processing device for the contactless communication with a data carrier which is detachably connected to the processing device
JP2001327747A *	2000-12-20	2001-11-27	Omron Corp	Ic coin-processing device for game machine, and inter- machine unit
JP5028708B2 *	2001-01-16	2012-09-19	大日本印刷株式会社	Showcase for sale or display with RF-ID tag
JP4788042B2 *	2001-01-16	2011-10-05	大日本印刷株式会社	Advertising billboard and display medium with RF-ID tag
JP4745515B2 *	2001-02-27	2011-08-10	トッパン・フォームズ株式会社	Information recording medium
RU2178922C1 *	2001-03-28	2002-01-27	Ровнер Яков Шоел-Берович	Mobile karaoke system
KR20020042748A *	2001-06-20	2002-06-07	김윤	Portable telephone having smartcard which non-contact interface is transferred into break contact point
JP2003058839A *	2001-08-10	2003-02-28	Ricoh Co Ltd	Medium, method and device for providing input information
KR20030014455A *	2001-08-11	2003-02-19	지식정보기술 주식회사	RF ID Coin and Game apparatus
US6843413B2	2001-09-07	2005-01-18	Mitsubishi Denki Kabushiki Kaisha	Information providing method and information providing device
JP3617491B2	2001-10-31	2005-02-02	ソニー株式会社	IC chip and information processing terminal
JP4232474B2 *	2002-09-27	2009-03-04	ソニー株式会社	Electronic equipment with communication function
JP2004126096A *	2002-10-01	2004-04-22	Fuji Photo Film Co Ltd	Information card and device of system utilizing the same
GB0229141D0 *	2002-12-16	2003-01-15	Splashpower Ltd	Improvements relating to contact-less power transfer
GB0230196D0 *	2002-12-24	2003-02-05	Esselte Nv	Identifying compatible combination for a thermal printer
JP3993108B2	2003-01-17	2007-10-17	ソニー・エリクソン・モバイルコミュニケーションズ株式会社	Wireless communication method and wireless communication terminal
JP4334247B2	2003-03-07	2009-09-30	ビットワレット株式会社	Portable terminal device and electronic money server
US7694883B2 *	2003-05-01	2010-04-13	Brother Kogyo Kabushiki Kaisha	RFID label, method for producing the RFID label, device for producing the RFID label, sheet member (tag sheet) used for the RFID label, and cartridge attached to the device for producing the RFID label
US7184756B2 *	2003-06-12	2007-02-27	Motorola Inc.	Wireless communication device with tamper resistant configuration settings
AU2003261934A1 *	2003-09-04	2005-03-29	Fujitsu Frontech Limited	Ic card
JP4066929B2 *	2003-10-08	2008-03-26	株式会社日立製作所	Electronic device and manufacturing method thereof
US20080027842A1 *	2003-12-24	2008-01-31	Junko Suginaka	Personal Information Storage Device And Mobile Terminal
KR20070026813A *	2004-06-14	2007-03-08	코닌클리즈케 필립스 일렉트로닉스 엔.브이.	A telecommunication device and a baseband processor for this device
JP4266504B2 *	2004-08-09	2009-05-20	日本電気株式会社	Mobile terminal device
TWI244315B *	2004-09-02	2005-11-21	Inventec Appliances Corp	Apparatus for showing remaining balance value of electronic ticket card on portable electronic device and wirelessly adding value to the electronic ticket card by means of the portable electronic device and method therefor
CN101099165A *	2005-01-11	2008-01-02	富士通株式会社	IC tag storing case
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
US20060226217A1 *	2005-04-07	2006-10-12	Tyfone, Inc.	Sleeve for electronic transaction card

EP1912282B1	2005-08-02	2010-03-17	Panasonic Corporation	Antenna unit for noncontact communication and mobile communication device provided with such antenna unit
WO2007015353A1 *	2005-08-03	2007-02-08	Matsushita Electric Industrial Co., Ltd.	Storage medium with built-in antenna
DE102005043585A1 *	2005-09-12	2007-04-12	Combots Product Gmbh & Co. Kg	Personal contact- and visiting card for internet-supported communication system, has card and/or support body with data and/or information carriers having contact data, and including receiver to receive one of carriers against other carrier
JP4155408B2 *	2005-09-29	2008-09-24	ソニー・エリクソン・モバイルコミュニケーションズ株式会社	Charging device and charging system
JP4110167B2 *	2005-09-29	2008-07-02	三菱電機株式会社	Electronic key device for vehicles
JP5103741B2 *	2006-01-20	2012-12-19	大日本印刷株式会社	Non-contact data carrier device
JP2007274551A *	2006-03-31	2007-10-18	Fujitsu Ltd	Wireless communications equipment
US7991158B2	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
EP1936541B1 *	2006-12-22	2017-08-30	EM Microelectronic-Marin SA	On/off battery charger with power supply protection for monolithic integrated circuits using the energy from the antenna
JP2009048488A *	2007-08-21	2009-03-05	Sony Corp	Electronic wallet device, and method and program for using electronic value
JP5018339B2	2007-08-23	2012-09-05	ソニー株式会社	Signal processing apparatus, signal processing method, and program
JP4400433B2	2007-08-23	2010-01-27	ソニー株式会社	Electronic wallet device, communication method and program
JP5286714B2	2007-08-23	2013-09-11	ソニー株式会社	Electronic wallet device, electronic value utilization method and program
US8074027B2	2007-12-14	2011-08-22	Tyfone, Inc.	Memory card based contactless devices
WO2009089283A1	2008-01-07	2009-07-16	Access Business Group International Llc	Wireless power adapter for computer
JP5109720B2 *	2008-02-29	2012-12-26	オムロン株式会社	RFID reader / writer and its definition information management method
JP5486686B2	2008-03-31	2014-05-07	パナソニック株式会社	Electronic device, charger, and electronic device charging system
JP5398160B2	2008-03-31	2014-01-29	パナソニック株式会社	Electronic device, charger, and electronic device charging system
JP2008217836A *	2008-06-16	2008-09-18	Sony Corp	Value information control system
KR101472937B1 *	2008-07-23	2014-12-15	삼성전자 주식회사	Multi-usage memory card with a display unit
KR20100015206A *	2008-08-04	2010-02-12	삼성전자주식회사	A wireless testing interface device, a semiconductor device and a semiconductor package including thereof, and a testing method using thereof
US8348122B2	2008-08-06	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
JP2010073066A *	2008-09-19	2010-04-02	Toshiba Tec Corp	Mobile terminal device and rfid system
EP2401708A4	2009-02-24	2012-08-15	Tyfone inc	Contactless device with miniaturized antenna
JP5424489B2	2009-03-05	2014-02-26	パナソニック株式会社	Electronics
US9004360B2 *	2009-06-10	2015-04-14	Infineon Technologies Ag	Contactless communication via a plurality of interfaces
US20110159824A1 *	2009-12-31	2011-06-30	Peter Kenington	Active antenna array for a mobile communications network employing a first conductive layer and a second conductive layer
KR101175173B1 *	2010-03-11	2012-08-20	최형림	Sealing device of a container
EP2795541A4 *	2011-12-21	2015-07-29	Intel Corp	Tap zones for near field coupling devices
US9830556B2 *	2013-10-02	2017-11-28	Honeywell International Inc.	System incorporating actively authenticated multifactor proximity card

KR200483258Y1 *	2015-06-09	2017-05-02	브릴리언츠 주식회사	Multi smart card

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
JP3180086B2	2001-06-25	Mobile communication device, information transmission system and method, non-contact IC media usable in mobile communication device
CN101351970B	2011-12-14	Data communication in an electronic device
USRE45767E1	2015-10-20	Information processing system, hand held cellular phone, and information processing method
CN100576266C	2009-12-30	Information handling system, messaging device and information processing method
US8245944B2	2012-08-21	Assembly consisting of a micro-module and a reproducing device which is equipped with contact-free near-communication means
IL132183A	2004-06-20	Electronic device, especially an electronic book
JP2001223631A	2001-08-17	Mobile communication system
JP3455497B2	2003-10-14	Non-contact IC media and system using the same
KR20190008502A	2019-01-24	The media card having an NFC tag and a memory for storing a sound source, and a device for reproducing data of the media card
JP4223739B2	2009-02-12	Reader / writer and contactless IC media
RU77989U1	2008-11-10	UNIVERSAL INTELLECTUAL CARD
CN103975536A	2014-08-06	Multi-tag operating system and operating method thereof
KR20180116714A	2018-10-25	A thin media card configured to transmit data in a storage memory to a device in contact or non-contact method, and a device
KR20190112374A	2019-10-07	A contact type memory card including a surface for printing an embedded content image and having pads in mutual contact with the connectors in the lateral and longitudinal directions
JP2001306995A	2001-11-02	Claim information display terminal
JP2001306974A	2001-11-02	Rate notifying method

Priority And Related Applications

Child Applications (1)

Application	Priority date	Filing date	Relation	Title
JP2000118571A	1998-08-31	2000-04-19	Division	Non-contact IC media and system using the same

Priority Applications (1)

Application	Priority date	Filing date	Title
JP24599598A	1998-08-31	1998-08-31	Mobile communication device, information transmission system and method, non-contact IC media usable in mobile communication device

Applications Claiming Priority (19)

Application	Filing date	Title
JP24599598A	1998-08-31	Mobile communication device, information transmission system and method, non-contact IC media usable in mobile communication device
EP99940552A	1999-08-30	NONCONTACT reader/writer
EP07014227A	1999-08-30	Contactless IC media and system applying the same
CNB998102139A	1999-08-30	Non-contact IC medium and system using the same
US09/763,523	1999-08-30	Noncontact IC medium and system using the same
CNB200410057563A	1999-08-30	Contactless IC media and system applying the same
AU54452/99A	1999-08-30	Noncontact ic medium and system using the same

KR1020017002533A	1999-08-30	Noncontact ic medium and system using the same
AT99940552T	1999-08-30	CONTACTLESS READER / WRITER
KR1020067013097A	1999-08-30	Noncontact ic medium and system using the same
CNA2007100063138A	1999-08-30	Contactless ic media and system applying the same
PCT/JP1999/004671	1999-08-30	Noncontact ic medium and system using the same
EP07014228A	1999-08-30	Contactless IC media and system applying the same
EP07014226A	1999-08-30	Contactless IC media and system applying the same
CN82007100063123A	1999-08-30	Non-contact reader
DE69937363T	1999-08-30	Contactless reader / writer
JP2000118571A	2000-04-19	Non-contact IC media and system using the same
US10/859,584	2004-06-02	Contactless IC media and system applying the same
HK05108600A	2005-09-29	Noncontact ic medium

Legal Events

Date	Code	Title	Description
2004-04-20	R250	Receipt of annual fees	**Free format text:** JAPANESE INTERMEDIATE CODE: R250
2005-04-19	R250	Receipt of annual fees	**Free format text:** JAPANESE INTERMEDIATE CODE: R250
2006-03-22	R250	Receipt of annual fees	**Free format text:** JAPANESE INTERMEDIATE CODE: R250
2007-04-24	R250	Receipt of annual fees	**Free format text:** JAPANESE INTERMEDIATE CODE: R250
2008-04-10	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20080413 **Year of fee payment:** 7
2008-04-15	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20090413 **Year of fee payment:** 8
2009-04-14	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20100413 **Year of fee payment:** 9
2009-10-06	S111	Request for change of ownership or part of ownership	**Free format text:** JAPANESE INTERMEDIATE CODE: R313117 **Free format text:** JAPANESE INTERMEDIATE CODE: R313113
2009-10-15	R350	Written notification of registration of transfer	**Free format text:** JAPANESE INTERMEDIATE CODE: R350
2009-10-15	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20100413 **Year of fee payment:** 9
2010-04-20	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20110413 **Year of fee payment:** 10
2011-04-12	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20120413 **Year of fee payment:** 11
2012-04-24	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20130413 **Year of fee payment:** 12
2013-04-13	LAPS	Cancellation because of no payment of annual fees	

Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

Ic card interactive plastic leaflet

Abstract

The present invention relates to an envelope (3) for receiving an IC card (1) comprising two opposite faces, an internal microprocessor and memory circuit, and a set of contacts (2) surface-mounted on one of the two faces of the IC card to access the microprocessor and memory circuit. The envelope (3) is formed by a leaflet including two flexible flaps defining between them a flat space for receiving the IC card (1). A window (7) is made in one of the two flaps for accessing the set of surface-mounted contacts (2). A graphic scheme, for example a keyboard layout, is printed on at least one of the two sheet members for permitting use of the IC card (1) for an additional, predetermined function, for example recording the answers given by the user during a TV game. The present invention also relates to the resulting IC card/envelope combination. The invention is further concerned with a system for using the IC card for the additional predetermined function, comprising the leaflet and an IC card reading and/or writing device having a transparent tactile keyboard membrane and a microcontroller. The IC card/leaflet combination is inserted behind the transparent tactile keyboard membrane so that the keyboard membrane of the leaflet appears through the keyboard membrane. The microcontroller writes information in the microprocessor and memory circuit of the IC card in relation to operation of the transparent tactile keyboard membrane.

Classifications

G07F7/1008 Active credit-cards provided with means to personalise their use, e.g. with PIN-introduction/comparison system

View 5 more classifications

WO2000014678A1

WIPO (PCT)

Download PDF Find Prior Art Similar

Other languages: French

Inventor: Pierre Michel Combaluzier

Worldwide applications

1999 WO AU

Application PCT/CA1999/000785 events

1998-09-04 Priority to US14813298A

1998-09-04 Priority to US09/148,132

1999-08-27 Application filed by Ic Tv Interactive Cyber Television Inc

2000-03-16 Publication of WO2000014678A1

Info: Patent citations (4), Cited by (8), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, PatentScope, Discuss

Claims

Hide Dependent

WHAT IS CLAIMED IS:

1. An envelope for receiving an IC card comprising two opposite faces, an internal microprocessor and memory circuit, and a set of contacts surface-mounted on one of the two faces of the IC card to access the microprocessor and memory circuit, comprising: two sheet members defining between them a flat space for receiving the IC card; a window in one of said two sheet members for accessing the set of surface-mounted contacts; and a graphic scheme printed on at least one of said two sheet members for permitting use of the IC card for an additional, predetermined function.

2. The envelope of claim 1 , wherein: - the envelope is a leaflet with two flexible flaps; and

- the two sheet members are formed by the two flexible flaps of the leaflet, respectively.

3. The envelope of claim 2, wherein the leaflet further comprises a reinforced edge portion for interconnecting the two flexible flaps and facilitating insertion of the leaflet through a slot of IC card reading and/or writing device.

4. The envelope of claim 3, further comprising a slippery coating covering at least in part the two flexible flaps and the reinforced edge portion to facilitate both insertion of the IC card in the leaflet and insertion of the leaflet through the slot of the IC card reading and/or writing device.

5 The envelope of claim 1 , wherein the graphic scheme comprises a keyboard layout

6. The envelope of claim 2, further comprising indications printed on the leaflet to guide both insertion of the IC card in the flat space between the two flexible flaps and insertion of the leaflet in a slot of IC card reading and/or writing device.

7. An IC card/envelope combination comprising: an IC card comprising two opposite faces, an internal microprocessor and memory circuit, and a set of contacts surface-mounted on one of the two faces of the IC card to access the microprocessor and memory circuit; and an envelope for receiving the IC card, including: two sheet members defining between them a flat space for receiving the IC card; a window in one of said two sheet members for accessing the set of surface-mounted contacts; and a graphic scheme printed on at least one of said two sheet members for permitting use of the IC card for an additional, predetermined function.

8. The IC card/envelope combination of claim 7, wherein: - the envelope is a leaflet with two flexible flaps; and - the two sheet members are formed by the two flexible flaps of the leaflet, respectively.

9. The IC card/envelope combination of claim 8, wherein the leaflet further comprises a reinforced edge portion for interconnecting the two flexible flaps and facilitating insertion of the IC card/envelope combination through a slot of IC card reading and/or writing device.

10. The IC card/envelope combination of claim 9, further comprising a slippery coating covering at least in part the two flexible flaps and the reinforced edge portion to facilitate both insertion of the IC card in the leaflet and insertion of the IC card/envelope combination through the slot of the IC card reading and/or writing device.

11. The IC card/envelope combination of claim 7, wherein the graphic scheme comprises a keyboard layout.

12. The IC card/envelope combination of claim 8, further comprising indications printed on the leaflet to guide both insertion of the IC card in the flat space between the two flexible flaps and insertion of the IC card/envelope combination in a slot of IC card reading and/or writing device.

13. A system for using an IC card for an additional predetermined function, the IC card comprising two opposite faces, an internal microprocessor and memory circuit, and a set of contacts surface-mounted on one of the two faces of the IC card to access the microprocessor and memory circuit, said system comprising: an envelope for receiving the IC card, including: two sheet members defining between them a flat space for receiving the IC card and form an IC card/envelope combination; a window made in a first one of said two sheet members for accessing the set of surface- mounted contacts; and a keyboard layout printed on the second one of said two flexible sheet members; and an IC card reading and/or writing device including: a housing defining a planar wall surface; a transparent tactile keyboard membrane mounted in front of but spaced apart from the planar wall surface to define a flat cavity between the transparent tactile keyboard membrane and the planar wall surface to receive the IC card/envelope combination; a connector mounted on the planar wall surface and having a plurality of contacts for connection to the surface-mounted contacts of said set, respectively; and a microcontroller for writing information in the microprocessor and memory circuit of the IC card through said the contacts of said connector and the surface-mounted contacts of said set in relation to operation of the transparent tactile keyboard membrane; whereby, in operation, when the IC card/envelope combination is inserted in the flat cavity with the contacts of the connector connected to the surface-mounted contacts of said set and with the keyboard layout visible through the transparent tactile keyboard membrane, the transparent tactile keyboard membrane can be operated in relation to the keyboard layout and the microcontroller can write information in the microprocessor and memory circuit of the IC card in relation to operation of the transparent keyboard membrane.

14. The system of claim 13, wherein: - the envelope is a leaflet with two flexible flaps; and

- the two flexible sheet members are formed by the two flexible flaps of the leaflet, respectively.

15. The system of claim 13, wherein: - the IC card reading and/or writing device forms part of a TV remote control; the keyboard layout is a TV game keyboard layout for answering questions asked during a TV program; and the microcontroller comprises means for recording the answers to said questions given by a user through operation of the transparent tactile keyboard membrane.

Description

IC CARD INTERACTIVE PLASTIC LEAFLET

BACKGROUND OF THE INVENTION

1. Field of the invention:

The present invention relates to an envelope for receiving an IC (Integrated Circuit) card in view of permitting use of this IC card for an additional, predetermined function. The present invention also relates to the IC card/envelope combination. The present invention further relates to a system, including the envelope, for using the IC card for the additional, predetermined function.

2. Brief description of the prior art:

Chip cards are currently used as credit cards, for bank transactions, in security systems, etc. A chip card is a plastic card similar in appearance to a credit card, but containing a microprocessor and memory chip programmed to perform several functions when used at a suitable terminal. As well known to those of ordinary skill in the art, a chip card comprises surface-mounted contacts for connection to the terminal.

Certain chip cards, usually called IC (Integrated Circuit) or smart cards and used for making bank transactions at a terminal, contain not only ROM but RAM as well. Since these cards have microprocessor intelligence and a coded RAM memory, they can record card transactions and store data which are updated with each transaction.

OBJECT OF THE INVENTION

A general object of the present invention is to enable the use of IC cards for additional, predetermined functions.

SUMMARY OF THE INVENTION

More specifically, in accordance with the present invention, there is provided an envelope for receiving an IC card comprising two opposite faces, an internal microprocessor and memory circuit, and a set of contacts surface-mounted on one of the two faces of the IC card to access the microprocessor and memory circuit. The envelope of the invention comprises (a) two sheet members defining between them a flat space for receiving the IC card, (b) a window in one of the two sheet members for accessing the set of surface-mounted contacts, and (c) a graphic scheme printed on at least one of the two sheet members for permitting use of the IC card for an additional, predetermined function.

The present invention also relates to an IC card/envelope combination comprising an IC card and an envelope for receiving the IC card. The IC card comprises two opposite faces, an internal microprocessor and memory circuit, and a set of contacts surface- mounted on one of the two faces of the IC card to access the microprocessor and memory circuit. The envelope includes: two sheet members defining between them a flat space for receiving the IC card; a window in one of the two sheet members for accessing the set of surface-mounted contacts; and a graphic scheme printed on at least one of the two sheet members for permitting use of the IC card for an additional, predetermined function.

In accordance with a preferred embodiment, the envelope is a leaflet with two flexible flaps, the two sheet members are formed by the two flexible flaps of the leaflet, respectively, and the leaflet further comprises a reinforced edge portion for interconnecting the two flexible flaps and facilitating insertion of the leaflet through a slot of IC card reading and/or writing device. A slippery coating may cover at least in part the two flexible flaps and the reinforced edge portion to facilitate both insertion of the IC card in the leaflet and insertion of the leaflet through the slot of the IC card reading and/or writing device.

According to another preferred embodiment of the invention, the graphic scheme comprises a keyboard layout.

Preferably, indications will be printed on the leaflet to guide both insertion of the IC card in the flat space between the two flexible flaps and insertion of the leaflet in the slot of an IC card reading and/or writing device.

Further in accordance with the present invention, there is provided a system for using an IC card for an additional predetermined function comprising an envelope for receiving the IC card and an IC card reading and/or writing device. The IC card comprises two opposite faces, an internal microprocessor and memory circuit, and a set of contacts surface-mounted on one of the two faces of the IC card to access the microprocessor and memory circuit. The envelope includes: two sheet members defining between them a flat space for receiving the IC card and form an IC card/envelope combination; a window made in a first one of the two sheet members for accessing the set of surface-mounted contacts; and a keyboard layout printed on the second one of the two flexible sheet members. The IC card reading and/or writing device includes: a housing defining a planar wall surface; a transparent tactile keyboard membrane mounted in front of but spaced apart from the planar wall surface to define a flat

cavity between the transparent tactile keyboard membrane and the planar wall surface to receive the IC card/envelope combination; a connector mounted on the planar wall surface and having a plurality of contacts for connection to the surface- mounted contacts, respectively, and a microcontroller for writing information in the microprocessor and memory circuit of the IC card through the connector contacts and the surface-mounted contacts in relation to operation of the transparent tactile keyboard membrane.

In operation, when the IC card/envelope combination is inserted in the flat cavity with the connector contacts connected to the surface-mounted contacts and with the keyboard layout visible through the transparent tactile keyboard membrane, the transparent tactile keyboard membrane can be operated in relation to the keyboard layout and the microcontroller can write information in the microprocessor and memory circuit of the IC card in relation to operation of the transparent keyboard membrane.

In accordance with a preferred embodiment, the IC card reading and/or writing device forms part of a TV remote control, the keyboard layout is a TV game keyboard layout for answering questions asked during a TV program, and the microcontroller comprises means for recording the answers to the questions given by a user through operation of the transparent tactile keyboard membrane.

The objects, advantages and other features of the present invention will become more apparent upon reading of the following non restrictive description of a preferred embodiment thereof, given by way of example only with reference to the accompanying drawings. BRIEF DESCRIPTION OF THE DRAWINGS

In the appended drawings:

Figure 1 is a perspective view of a leaflet in accordance with the invention for receiving an IC card and thereby form an IC card/leaflet combination, showing a window in one of the flexible flaps for accessing the surface-mounted contacts of the IC card;

Figure 2 is a side elevational view of the leaflet of Figure 1 ;

Figure 3 is a front elevational view of the IC card and leaflet;

Figure 4 is a rear elevational view of a TV remote control including an IC card reading and/or writing device for receiving the IC card/leaflet combination;

Figure 5 is a side elevational view of a leaflet according to the invention including two flexible flaps and a reinforced edge portion for interconnecting these two flexible flaps;

Figure 6a is an example of keyboard layout that can be printed on the outer face of the rear flap of the leaflet according to the invention;

Figure 6b is an example of illustration that can be printed on the outer face of the front flap of the leaflet according to the invention, and Figure 7 is a block diagram of the electronic circuit of the TV remote control of Figure 4.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring to Figure 1 of the appended drawings, the IC card 1 comprises surface-mounted contacts 2 for connection to a bank terminal or any other terminal (not shown). Just a word to mention that the format of most of the IC cards presently available on the market conforms with an ISO standard.

Preferably, the leaflet 3 is made of transparent plastic sheet material. The leaflet 3 comprises a rear flap 5 and a front flap 6 having a configuration and dimensions corresponding to those of the IC card 1. The leaflet 3 comprises a reinforced edge portion 4 for interconnecting the flexible flaps 5 and 6 and facilitate insertion of the leaflet 3 through a slot of IC card reading and/or writing device. Front flap 6 comprises a rectangular window 7 to access the surface-mounted contacts 2 when the leaflet 3 envelops the IC card 1. On the outer face of the rear flap 5 is printed a graphic keyboard layout as shown for example by arrow 8 in Figure 4. This graphical keyboard layout 8 may be composed of various icons, letters, numbers, or other characters or illustrations such as 22.

To further facilitate penetration of the slot of an IC card reading and/or writing device, outer faces 29 and 30 of the reinforced edge portion 4 as well as portion of the flaps 5 and 6 can be covered with a slippery coating (not shown). In the same manner, portions of the flaps 5 and 6 can be covered with a slippery coating to facilitate insertion of the IC card 1 in the flat space defined between the flaps 5 and 6.

Arrow-like indications such as 31 can also be printed onto the outer faces 29 and 30 to indicate to a user a direction of insertion of the IC card/leaflet combination in the slot of the reading and/or writing device. In addition, guide marks can be printed on the leaflet 3 to guide insertion of the IC card 1 between the two flaps 5 and 6 of the leaflet 3. Finally, visual indications of the new function(s) added to the IC card 1 through the leaflet 3 can be printed onto the leaflet 3, in particular on the outer face of the front flap 6.

Referring now to Figures 1-3, the IC card 1 is inserted between the two flaps 5 and 6 (see arrows 9 in Figure 1 , arrow 10 in Figure 2, arrows 12 in Figure 3, and arrow 28 in Figure 5) in such a way as to expose the contacts 2 through the window 7, as best shown in Figure 3.

The IC card 1 can be used in combination with a universal remote control 13 shown in Figure 4. The remote control 13 incorporates all the function protocols of the TV, VCR, Audio commands of most of the brands available on the market (95%). Figure 8 shows a schematic block diagram of the electronic circuit of the remote control 13.

The remote control 13 comprises a plastic housing 14. On the back of the housing 14 is defined a planar wall surface 17. A transparent tactile keyboard membrane 18 is mounted in front but spaced apart from the planar wall surface to define a flat cavity between the transparent tactile keyboard membrane and the planar wall surface 17 to receive the IC card 1/leaflet 3 combination. In the illustrated non limitative example, the transparent tactile keyboard membrane 18 comprises 15 resistive tactile zones such as 21. The plastic housing 14 of the remote control 13 has a top face 15 formed with a slot 16 for longitudinal insertion of the IC card 1/leaflet 3 combination in the flat cavity behind the transparent tactile keyboard membrane.

On a planar wall surface 17 of the housing 14 situated behind keyboard 18 is mounted a universal IC card connector 19 including a standard group of contacts such as 20 for connection to respective surface-mounted contacts 2 in order to automatically establish a bidirectional communication link between the microprocessor and memory circuit of the IC card 1 and the microcontroller 30 of the remote control 13 (Figure 7) each time the IC card 1 covered by the leaflet 3 is longitudinally inserted through the slot 16.

Of course, the leaflet 3 is so designed that the reinforced edge portion 4 (Figure 5) is introduced first to thereby greatly facilitate insertion of the IC card 1/leaflet 3 combination through the slot 16. After the IC card 1/leaflet 3 combination has been inserted through the slot 16, each icon, letter, number or other illustration 22 appears in a corresponding, for example resistive tactile zone 21.

Referring to Figure 7, the electronic circuit of the remote control

13 comprises the above mentioned microcontroller 30 and a universal remote control circuit 35 incorporating, as stated above, all the function protocols of the TV, VCR, Audio commands of most of the brands available on the market (95%).

The microcontroller 30 is connected to (a) the transparent tactile keyboard membrane 18 to detect depression of any zone 21 of that membrane, (b) a 4-digit liquid crystal display 25, (c) a piezoelectric transducer 31 to activate this piezoelectric transducer and produce a "bip" when required or desired, (d) a programmable real-time clock 32, (e) an identification number memory 33 for giving to the microcontroller 30 an identification of the user, and (f) the reading head 34 through a card interface 35. The microcontroller 30 is conventionally powered by an electric power supply 37, for example a 9-volt battery, through a 5-volt voltage regulator of circuit 38. The universal remote control circuit 36 is powered by the electric power supply 37 through a 3-volt voltage regulator of circuit 38.

The reading head 34 includes the connector 19 of Figure 4 and is advantageously of the GEMCORE™ technology. This technology has been developed by the company GemPlus to read and write on IC cards.

Regarding the card interface 35, it uses the language MEL

(MULTOS Executable Language) developed by the MULTOS which is a merger of financial institutions which establishes standard characteristics to ensure a compatibility of the communications between the members. MULTOS is an industrial standard for many applications of the IC cards, including the electronic purse application. The remote control 13 may further perform, amongst others, the following functions:

- a pawl 23 to trigger a mechanism (not shown) for ejecting the IC card 1/leaflet 3 combination from the flat cavity through the slot 16 after use (such a mechanism is well known to those of ordinary skill in the art and will not be further described in the present specification);

- a switch 24 to switch the tactile keyboard 18 on;

- the microcontroller 30 will display on the 4-digit liquid crystal display 25:

- the time obtained from the programmable real-time clock 32;

- the TV channel in interaction obtained from the universal remote control circuit 36;

- number of score units recorded and determined from the answers given by the user;

- minimum and maximum scores reached during a TV game as recorded by the microcontroller 30;

- the charge of the battery obtained through the voltage regulator circuit 38, - etc.

- a push-button 26 connected to the microcontroller 30 for adjusting the time given by the clock 32 and displayed by the microcontroller 30 on the display 25, and for adjusting the intensity of the "bip" produced by the piezoelectric transducer 31 to confirm interactive actions on the transparent tactile keyboard membrane 18 (upon adjustment of the intensity of the "bip" through the push-button 26, a bar code representative of this intensity is displayed by the microcontroller 30 on the 4-digit liquid crystal display 25);

- a push-button 27 for resetting the score after saving of the game.

Although application of the leaflet 3 to form an IC card 1/leaflet

3 combination to be inserted in a remote control 13 has been described in the foregoing description, the leaflet 3 according to the invention can also be used in connection with an IC card and thereby form an IC card 1/leaflet 3 subsequently inserted into any other type of bank, transaction, communication and/or exchange terminal.

The leaflet 3 according to the invention is also designed for and capable of customizing, adapting, humanizing and/or promoting a functional card of the security type, or creating actions, synergies or interoperabilities for such cards. To easily penetrate the public at large with functional cards of the security type, the leaflet 3 may be used to dress, to complete with added functions or values and/or to make user- friendly and less formal such security cards, while satisfying the standards, prints, ISO 1 back magnetic stripe and/or functional prints of the security organization, monetary or monetics transaction organization, and/or initial issuing organization.

The leaflet 3 according to the invention can further be used:

- to promote or lead towards customer loyalty to any privative bank card, commercial card, credit card, debit card, etc.; - to instantaneously optimize the visual access of applications of the card being used,

- to guide transactions on a portable card reader, and

- as an envelope for interactive direct television advertising.

Example

The following example is concerned with a leaflet 3 having a back flap 5 on which is printed the layout of a keyboard for playing a game related to a given TV program, for example the popular program ENTERTAINMENT TONIGHT™. Figure 6a illustrates an example of keyboard layout which can be printed on the outer face of the rear flap 5, and Figure 6b illustrates the outer face of the front flap 6 on which can be printed, for example, identification of the issuing organization, advertising of the TV program, identification of the produces, etc

Just a word to mention that the leaflet 3 according to the present invention can be produced at low cost (some cents by unit) and can be distributed to the public at large:

- on wine bottles;

- on soft drink packs;

- inside weekly TV guides;

- by direct mail; - in fragrance boxes;

- in magazines;

- on cigarette boxes; - in photo film boxes;

- in airflight tickets;

- in show tickets envelopes;

- in gift menus;

- in check flyers; - etc.

Since the leaflet 3 according to the invention is susceptible to increase their sales and profits, the companies involved are likely to incorporate the leaflet to their products at no extra charge.

To use the leaflet 3 according to the present invention, the first step consists of inserting the IC card 1 into the leaflet 3 and inserting the IC card 1/leaflet 3 combination through the slot 16. The keyboard layout of Figure 6a then appears through the transparent tactile keyboard 18. As can be appreciated, each icon of the keyboard layout of Figure 6a appears through a respective resistive area 21 of the transparent tactile keyboard 18.

The microcontroller can further be programmed to respond to insertion of the IC card 1/leaflet 3 combination by:

- pre-programming the clock 32 to synchronize it with the TV program in order to enable correct time dating of the answers selected by the card user on the transparent tactile keyboard membrane 18. This is made by means of a time correction increment or decrement recorded in the microprocessor and memory circuit of the IC card 1 by a bank terminal or any other type of terminal as will be explained hereinafter; - control the universal remote control circuit 36 to automatically turn the TV set on.

Then the user use the remote control 13 to tune the TV set to the channel on which the TV program associated to the leaflet 3 is broadcasted. Then, the user can answer the questions broadcasted during the TV program. A list of possible questions is presented in attached Appendix 1. As can be seen, an icon 22 of the keyboard layout 8 is associated to each question.

If the user chooses answer 1 as a response to a question, he

(she) presses once on the zone 21 of the transparent tactile keyboard 18 behind which the icon 22 corresponding to the question appears. If answer 2 is selected, the user presses twice on the zone 21 of the transparent tactile keyboard 18 behind which the corresponding icon 22 appears. If the user chooses answer 3 as a response to the question, he (she) presses three times on the zone 21 of the transparent tactile keyboard 18 corresponding to the icon 22 associated to the question.

The user will answer to a series of questions during one, two, or up to five TV programs of a TV channel using one or more leaflets such as leaflet 3.

The microcontroller 30 of the remote control 13 is responsive to depression of the tactile zones 21 of the transparent keyboard membrane 18 to record the answers of the user in the microprocessor and memory circuit of the IC card 1 and the time at which these answers are given through the card interface 35, the reading head 34 including the contacts 20 of the connector 19, and the surface-mounted contacts 2 of the IC card 1. The user's identification number stored in memory 33 will also be recorded in the microprocessor and memory circuit of the IC card 1 for identifying the user.

In this way, the user accumulates rights in relation to his (her) answers. He (She) also defines, in time, his (her) consumer profile. The user can then use his (her) IC card 1 to obtain these rights, through an appropriate terminal, in particular but not exclusively a sponsor banking terminal rent for that purpose, or simply a dedicated terminal.

As soon as the IC card 1 is inserted in the terminal, the server of the TV channel or the sponsor network is contacted. The software of the server reads the contents of the IC card 1 , analyses the recorded times and answers, compare the results with the answer key of the questionnaire and/or TV game, and decides the value of the rights to be attributed in relation to the accuracy of the answers recorded in the memory of the IC card 1. Finally, the server of the TV channel and/or sponsor will attribute a remuneration corresponding to the value of rights acquired, consisting of points, coupons, units, miles, etc in the IC card 1. The user can then choose to use this gain to obtain free units or, for example, to credit his (her) VISA account with a corresponding amount of money. To credit his (her) account, the user has simply to type the number of his (her) VISA card on the keyboard of the terminal being used.

Finally, the recorded data are erased by the terminal to prepare the card for a new TV program. Before erasing the recorded data, the terminal analyses the time dating of the answer recorded and will store in the microprocessor and memory circuit of the IC card 1 the above mentioned time correction increment or decrement that should be applied to the real-time clock 32 to synchronize this clock 32 with the TV program in order to enable correct time dating of the answers given by the card user on the transparent tactile keyboard membrane 18.

At the beginning of each game played or operation made through the remote control 13, the microcontroller 30 stores the user's identification number from memory 33 in the microprocessor and memory circuit of the IC card 1 , next to the time dating of the answers. This will enable survey of the population for rating (percent of TV households that are tuned, on the average, to one time period in a particular program).

Finally, it should be mentioned that the above mentioned gain can be paid by any interested party, for example public survey organizations.

Although the present invention has been described hereinabove by way of a preferred embodiment thereof, this embodiment can be modified at will, within the scope of the appended claims, without departing from the spirit and nature of the subject invention.

Patent Citations (4)

Publication number	Priority date	Publication date	Assignee	Title
FR2674649A1 *	1991-03-28	1992-10-02	Dom Intell Ingenieries	Remote control process, device for its implementation and microcircuit card associated with this device
DE9407198U1 *	1994-04-30	1994-09-22	Ociepka Roman	Adapter for adapting D-Netz plug-in chips to large D-Netz phone cards
DE4419073A1 *	1993-05-31	1994-12-01	Nokia Mobile Phones Ltd	SIM card adapter
DE29503892U1 *	1995-03-07	1995-05-18	Kemmler Manfred	Emergency mini card, electronic identification system with photo
Family To Family Citations				

* Cited by examiner, † Cited by third party

Cited By (8)

Publication number	Priority date	Publication date	Assignee	Title

EP1314133A1 *	2000-09-01	2003-05-28	Canon Kabushiki Kaisha	Networked business system
EP1388811A1	2002-07-05	2004-02-11	Christof Huber	Method and module for expanding the function of a chip card, and card having such a module
WO2006108184A1 *	2005-04-07	2006-10-12	Tyfone, Inc.	Sleeve for electronic transaction card
US8231061B2	2009-02-24	2012-07-31	Tyfone, Inc.	Contactless device with miniaturized antenna
US8814053B2	2008-08-08	2014-08-26	Tyfone, Inc.	Mobile payment device with small inductive device powered by a host device
US8866614B2	2008-08-08	2014-10-21	Tyfone, Inc.	Active circuit for RFID
US9004361B2	2005-02-22	2015-04-14	Tyfone, Inc.	Wearable device transaction system
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
Family To Family Citations				

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
US7191952B2	2007-03-20	Selectable multi-purpose card
US5973475A	1999-10-26	Remote smart battery
US7306143B2	2007-12-11	Dynamic smart card/media imaging
US5128752A	1992-07-07	System and method for generating and redeeming tokens
US5932869A	1999-08-03	Promotional system with magnetic stripe and visual thermo-reversible print surfaced medium
US6623039B2	2003-09-23	Multi-purpose card
CA2375609C	2013-01-08	Multi-purpose card
US5762376A	1998-06-09	Methods and apparatus for providing a prepaid, remote entry transaction instrument having multiple language capability
PL196157B1	2007-12-31	Transaction effecting apparatus
US20130048712A1	2013-02-28	Nagraid information card
WO1988009018A1	1988-09-01	A portable device for storing and transferring data
WO2005008446A3	2006-08-17	Cashless payment system
WO1994020929A1	1994-09-15	Smart card
US20060081702A1	2006-04-20	System and method for universal consumer cards
KR10032939481	2002-09-25	Chip card read/write device
WO2000014678A1	2000-03-16	Ic card interactive plastic leaflet
US20050010490A1	2005-01-13	Internet-based electronic lottery card
US20210103917A1	2021-04-08	Payment device applets with pre-stored messages and triggerable logic
US20090078756A1	2009-03-26	Method and Apparatus for Identifying and Dispensing Currency and Non Cash Media from Automated Teller Machine or Cash Dispensing Device
AU714577B2	2000-01-06	Vending machine
US20020103768A1	2002-08-01	Secure payment system allowing selection of any payable amount
JP2000059535A	2000-02-25	Advertisement system through portably recording medium
GB2351830A	2001-01-10	Electronic messaging system
KR20110071151A	2011-06-29	Objects have data record tag
BG109760A	2008-06-30	Method, system and article for communication storage, access and assessment

Priority And Related Applications

Priority Applications (2)

Application	Priority date	Filing date	Title
US14813298A	1998-09-04	1998-09-04	*US Provisional Application*
US09/148,132		1998-09-04	

Applications Claiming Priority (1)

Application	Filing date	Title
AU53676/99A	1999-08-27	Ic card interactive plastic leaflet

Legal Events

Date	Code	Title	Description
2000-03-16	AK	Designated states	**Kind code of ref document:** A1 **Designated state(s):** AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZA ZW
2000-03-16	AL	Designated countries for regional patents	**Kind code of ref document:** A1 **Designated state(s):** GH GM KE LS MW SD SL SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
2000-05-10	121	Ep: the epo has been informed by wipo that ep was designated in this application	
2001-01-04	REG	Reference to national code	**Ref country code:** DE **Ref legal event code:** 8642
2001-05-04	NENP	Non-entry into the national phase in:	**Ref country code:** CA
2001-08-08	122	Ep: pct application non-entry in european phase	

Data provided by IFI CLAIMS Patent Services

Patents at399405T

SYSTEM AND METHOD FOR ENCRYPTING MESSAGES AND REGISTERING IN A TRANSACTION PROCESSING SYSTEM

Classifications

H04L9/3247 Cryptographic mechanisms or cryptographic arrangements for secret or secure communication including means for verifying the identity or authority of a user of the system or for message authentication, e.g. authorization, entity authentication, data integrity or data verification, non-repudiation, key authentification or verification of credentials involving digital signatures

View 5 more classifications

AT399405T

Austria

Other languages: German

Inventor: Edward P Felt, John R Wells

Worldwide applications

2002 AT EP US WO DE AU JP 2008 US

Application AT02721082T events

2001-02-22 Priority to US27110601P

2002-02-21 Application filed by Sea Systems Inc

2008-07-15 Publication of AT399405T

Info: Patent citations (35), Cited by (166), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Patent Citations (35)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US4200770A *	1977-09-06	1980-04-29	Stanford University	Cryptographic apparatus and method
US4937863A	1988-03-07	1990-06-26	Digital Equipment Corporation	Software licensing management system
US5023907A *	1988-09-30	1991-06-11	Apollo Computer, Inc.	Network license server
US5438508A	1991-06-28	1995-08-01	Digital Equipment Corporation	License document interchange format for license management system
US5940504A *	1991-07-01	1999-08-17	Infologic Software, Inc.	Licensing management system and method in which datagrams including an address of a licensee and indicative of use of a licensed product are sent from the licensee's site
JPH07230388A *	1994-02-15	1995-08-29	Internati Business Mach Corp <ibm>	Method and system for controlling utilization of application program
JPH10512074A *	1995-02-13	1998-11-17	インタートラスト テクノロジーズ コーポレイション	System and method for secure transaction management and electronic rights protection
US5809144A *	1995-08-24	1998-09-15	Carnegie Mellon University	Method and apparatus for purchasing and delivering digital goods over a network
US5758068A	1995-09-19	1998-05-26	International Business Machines Corporation	Method and apparatus for software license management
US5671279A *	1995-11-13	1997-09-23	Netscape Communications Corporation	Electronic commerce using a secure courier system
US5671285A *	1995-12-13	1997-09-23	Newman; Bruce D.	Secure communication system
US5790664A	1996-02-26	1998-08-04	Network Engineering Software, Inc.	Automated system for management of licensed software

US5678316A *	1996-03-29	1997-09-30	International Business Machines Corporation	Creation and distribution of cryptographic envelope
US6327656B2 *	1996-07-03	2001-12-04	Timestamp.Com, Inc.	Apparatus and method for electronic document certification and verification
US6029145A *	1997-01-06	2000-02-22	Isogon Corporation	Software license verification process and apparatus
US6009173A *	1997-01-31	1999-12-28	Motorola, Inc.	Encryption and decryption method and apparatus
US6014688A *	1997-04-25	2000-01-11	Postx Corporation	E-mail program capable of transmitting, opening and presenting a container having digital content using embedded executable software
US6161181A *	1998-03-06	2000-12-12	Deloitte & Touche Usa Llp	Secure electronic transactions using a trusted intermediary
US6336186B1 *	1998-07-02	2002-01-01	Networks Associates Technology, Inc.	Cryptographic system and methodology for creating and managing crypto policy on certificate servers
US6442686B1 *	1998-07-02	2002-08-27	Networks Associates Technology, Inc.	System and methodology for messaging server-based management and enforcement of crypto policies
US6055413A *	1998-07-21	2000-04-25	Motorola, Inc	System and method for including origination time and update lifetime with updateable messages
US6324578B1	1998-12-14	2001-11-27	International Business Machines Corporation	Methods, systems and computer program products for management of configurable application programs on a network
US7143093B1 *	1998-12-17	2006-11-28	Webmethods, Inc.	Enterprise computer system
CA2256934C	1998-12-23	2002-04-02	Hamid Bacha	System for electronic repository of data enforcing access control on data retrieval
US6446136B1 *	1998-12-31	2002-09-03	Computer Associates Think, Inc.	System and method for dynamic correlation of events
FI1072058	1999-02-16	2001-06-15	Sonera Oyj	A method to secure information
US6766305B1 *	1999-03-12	2004-07-20	Curl Corporation	Licensing system and method for freely distributed information
US6760752B1 *	1999-06-28	2004-07-06	Zix Corporation	Secure transmission system
US6895507B1 *	1999-07-02	2005-05-17	Time Certain, Llc	Method and system for determining and maintaining trust in digital data files with certifiable time
US6609128B1 *	1999-07-30	2003-08-19	Accenture Llp	Codes table framework design in an E-commerce architecture
US6640244B1 *	1999-08-31	2003-10-28	Accenture Llp	Request batcher in a transaction services patterns environment
US6691176B1 *	2000-02-25	2004-02-10	Sun Microsystems, Inc.	Method and apparatus for managing data propagation between software modules
US7155414B2	2000-04-05	2006-12-26	International Business Machines Corporation	License compliance verification system
US7234103B1 *	2000-04-26	2007-06-19	Accenture Llp	Network-based tax framework database
US6917976B1 *	2000-05-09	2005-07-12	Sun Microsystems, Inc.	Message-based leasing of resources in a distributed computing environment

* Cited by examiner, † Cited by third party

Cited By (166)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US6636733B1	1997-09-19	2003-10-21	Thompson Trust	Wireless messaging method
US7003304B1	1997-09-19	2006-02-21	Thompson Investment Group, Llc	Paging transceivers and methods for selectively retrieving messages
US6253061B1	1997-09-19	2001-06-26	Richard J. Helferich	Systems and methods for delivering information to a transmitting and receiving device
US6983138B1	1997-12-12	2006-01-03	Richard J. Helferich	User interface for message access
US6826407B1	1999-03-29	2004-11-30	Richard J. Helferich	System and method for integrating audio and visual messaging
US8103588B2 *	2000-11-06	2012-01-24	Innovation Connection Corporation	System, method and apparatus for electronic ticketing
US8438465B2 *	2001-04-03	2013-05-07	Purdue Pharma L.P.	Privileged communication system with routing controls

US7844813B2 *	2001-07-13	2010-11-30	Dunward D. Dupre	Method, system and process for data encryption and transmission
JP2003249919A *	2001-12-17	2003-09-05	Fujitsu Ltd	Two-way communication method
US7185359B2 *	2001-12-21	2007-02-27	Microsoft Corporation	Authentication and authorization across autonomous network systems
EP3570178B1	2002-01-08	2020-05-27	Seven Networks, LLC	Secure transport for mobile communication network
US7039596B1	2002-01-18	2006-05-02	America Online, Inc.	Calendar overlays
US7660988B2 *	2002-03-18	2010-02-09	Cognomina, Inc.	Electronic notary
US8082575B2	2002-03-28	2011-12-20	Rampart-Id Systems, Inc.	System, method and apparatus for enabling transactions using a user enabled programmable magnetic stripe
US8015592B2 *	2002-03-28	2011-09-06	Innovation Connection Corporation	System, method and apparatus for enabling transactions using a biometrically enabled programmable magnetic stripe
US7222148B2 *	2002-05-02	2007-05-22	Bea Systems, Inc.	System and method for providing highly available processing of asynchronous service requests
US20030229672A1 *	2002-06-05	2003-12-11	Kohn Daniel Mark	Enforceable spam identification and reduction system, and method thereof
US6990504B2 *	2002-10-18	2006-01-24	Tybera Development Group, Inc.	Method and system for transmitting secured electronic documents
US7574607B1 *	2002-10-29	2009-08-11	Zix Corporation	Secure pipeline processing
US7778304B2 *	2003-02-20	2010-08-24	Proofpoint, Inc.	System for on-line and off-line decryption
US9781154B1	2003-04-01	2017-10-03	Oracle International Corporation	Systems and methods for supporting information security and sub-system operational protocol conformance
US20040218762A1 *	2003-04-29	2004-11-04	Eric Le Saint	Universal secure messaging for cryptographic modules
US7461080B1	2003-05-09	2008-12-02	Sun Microsystems, Inc.	System logging within operating system partitions using log device nodes that are access points to a log driver
US20040226017A1 *	2003-05-09	2004-11-11	Leonard Ozgur C.	Mechanism for associating resource pools with operating system partitions
US8892878B2 *	2003-05-09	2014-11-18	Oracle America, Inc.	Fine-grained privileges in operating system partitions
US8468330B1	2003-06-30	2013-06-18	Oracle International Corporation	Methods, systems, and data structures for loading and authenticating a module
US20050086513A1 *	2003-09-29	2005-04-21	Actional Corporation	Concept based message security system
US8103592B2 *	2003-10-08	2012-01-24	Microsoft Corporation	First computer process and second computer process proxy-executing code on behalf of first process
US7979911B2	2003-10-08	2011-07-12	Microsoft Corporation	First computer process and second computer process proxy-executing code from third computer process on behalf of first process
US7788496B2 *	2003-10-08	2010-08-31	Microsoft Corporation	First computer process and second computer process proxy-executing code on behalf thereof
US8190893B2	2003-10-27	2012-05-29	Jp Morgan Chase Bank	Portable security transaction protocol
US8185475B2 *	2003-11-21	2012-05-22	Hug Joshua D	System and method for obtaining and sharing media content
US8495361B2 *	2003-12-31	2013-07-23	International Business Machines Corporation	Securely creating an endorsement certificate in an insecure environment
US7751568B2 *	2003-12-31	2010-07-06	International Business Machines Corporation	Method for securely creating an endorsement certificate utilizing signing key pairs
EP1560137A1 *	2004-01-30	2005-08-03	Sap Ag	Technique for reliable message confirmation
US20050269401A1 *	2004-06-03	2005-12-08	Tyfone, Inc.	System and method for securing financial transactions
DE112004002974A5 *	2004-07-21	2007-07-12	Memory Data Gmbh	Proof-proof and fast WORM storage system based on hard drives
US7565577B2	2004-07-22	2009-07-21	Research In Motion Limited	Method and apparatus for providing intelligent error messaging

US8181182B1	2004-11-16	2012-05-15	Oracle America, Inc.	Resource allocation brokering in nested containers
US7730298B2 *	2004-11-22	2010-06-01	Hubspan Inc.	Method and apparatus for translating information between computers having different security management
GB2421097B *	2004-12-10	2009-07-01	Hewlett Packard Development Co	Methods, devices and computer programs for creating ciphertext, plaintext and a cryptographic key
US7890762B2 *	2004-12-30	2011-02-15	Sap Ag	Differentiated proxy digital signatures
GB2422208B *	2005-01-21	2009-09-09	Hewlett Packard Development Co	Method and system for contained cryptographic separation
US7860802B2 *	2005-02-01	2010-12-28	Microsoft Corporation	Flexible licensing architecture in content rights management systems
US20060184628A1 *	2005-02-14	2006-08-17	International Business Machines Corporation	Method and system to compose and transmit different contents to different recipients in a single message
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
US7630383B2 *	2005-03-29	2009-12-08	Alcatel-Lucent Usa Inc.	Synchronization of time stamps of peer devices in a communication node
US8091142B2 *	2005-04-26	2012-01-03	Microsoft Corporation	Supplementary trust model for software licensing/commercial digital distribution policy
DE602005025701D1 *	2005-06-21	2011-02-10	Research In Motion Ltd	Automatic selection and inclusion of a message signature
US20100203960A1 *	2005-07-20	2010-08-12	Wms Gaming Inc.	Wagering game with encryption and authentication
US8560853B2 *	2005-09-09	2013-10-15	Microsoft Corporation	Digital signing policy
US8281374B2 *	2005-09-14	2012-10-02	Oracle International Corporation	Attested identities
US10275723B2 *	2005-09-14	2019-04-30	Oracle International Corporation	Policy enforcement via attestations
US10063523B2 *	2005-09-14	2018-08-28	Oracle International Corporation	Crafted identities
KR100651744B1 *	2005-11-10	2006-12-01	한국전자통신연구원	Apparatus and method for unification of multiple radio-frequency identifications
US8839299B2 *	2005-12-19	2013-03-05	White Cyber Knight Ltd.	Apparatus and methods for assessing and maintaining security of a computerized system under development
US20070269041A1 *	2005-12-22	2007-11-22	Rajat Bhatnagar	Method and apparatus for secure messaging
FR2897223B1 *	2006-02-08	2008-05-09	Sts Group Sa	METHOD FOR THE ELECTRONIC ARCHIVING, IN PARTICULAR REMOTELY, OF DOCUMENTS OR OBJECTS
US7991158B2 *	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
JP2008257478A *	2007-04-04	2008-10-23	Internatl Business Mach Corp <ibm>	Device and method for outputting storage position of verification target character string and computer program
US8738919B2 *	2007-04-20	2014-05-27	Stmicroelectronics S.A.	Control of the integrity of a memory external to a microprocessor
US9137664B2 *	2007-05-01	2015-09-15	Qualcomm Incorporated	Application logging interface for a mobile device
US8341733B2 *	2007-06-20	2012-12-25	International Business Machines Corporation	Creating secured file views in a software partition
WO2009040140A1 *	2007-09-21	2009-04-02	Siemens Aktiengesellschaft	Decentralized energy system and method for distributing energy in a decentralized energy system
US8341410B2 *	2007-10-08	2012-12-25	Microsoft Corporation	Efficient certified email protocol
US9092388B1 *	2007-10-11	2015-07-28	Norberto Menendez	System and method of communications with supervised interaction
EP2202913B1 *	2007-10-19	2012-12-05	Nippon Telegraph and Telephone Corporation	User authentication and method for the same

US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US20090164477A1 *	2007-12-20	2009-06-25	Anik Ganguly	Method of electronic sales lead verification
NZ586279A *	2007-12-21	2012-08-31	Cocoon Data Holdings Ltd	System and method for securing data distributed by a first user to at least one recipient user
US20090193026A1 *	2008-01-25	2009-07-30	Sony Ericsson Mobile Communications Ab	Integrated database replay protection
US8739292B2 *	2008-03-04	2014-05-27	Apple Inc.	Trust exception management
WO2009131538A1 *	2008-04-21	2009-10-29	Agency For Science, Technology And Research	A portable system and method for remotely accessing data
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US20100070419A1 *	2008-09-17	2010-03-18	Srinivas Vadhri	System and method to initiate a function with an email message
US20100088234A1 *	2008-10-03	2010-04-08	Microsoft Corporation	Unified analytics across a distributed computing services infrastructure
US8644511B2 *	2008-11-05	2014-02-04	Comcast Cable Communications, LLC.	System and method for providing digital content
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
US8844024B1 *	2009-03-23	2014-09-23	Symantec Corporation	Systems and methods for using tiered signing certificates to manage the behavior of executables
JP2010238102A *	2009-03-31	2010-10-21	Fujitsu Ltd	Information processor, authentication system, authentication method, authentication device and program
US8281126B2 *	2009-08-14	2012-10-02	Canon Kabushiki Kaisha	Sending signed e-mail messages from a device
US20110083015A1 *	2009-10-05	2011-04-07	Eidgenossische Technische Hochschule Zurich	System and method for an electronic signature for quick and efficient data authentication
US20110238402A1 *	2010-03-23	2011-09-29	Fujitsu Limited	System and methods for remote maintenance in an electronic network with multiple clients
BR112013004074A2 *	2010-08-24	2016-07-26	Koninkl Philips Electronics Nv	attribute-based digital signature system, workstation, attribute-based digital signature generation method, and computer program product
FR2965431B1 *	2010-09-28	2013-01-04	Mouchi Haddad	SYSTEM FOR EXCHANGING DATA BETWEEN AT LEAST ONE TRANSMITTER AND ONE RECEIVER
US8782397B2 *	2011-01-06	2014-07-15	International Business Machines Corporation	Compact attribute for cryptographically protected messages
US10614417B2 *	2011-05-12	2020-04-07	ActiveProspect, Inc.	System and method for electronic lead verification
US20120294445A1 *	2011-05-16	2012-11-22	Microsoft Corporation	Credential storage structure with encrypted password
US8549579B2 *	2011-07-06	2013-10-01	International Business Machines Corporation	Dynamic data-protection policies within a request-reply message queuing environment
US8800058B2	2011-07-27	2014-08-05	Microsoft Corporation	Licensing verification for application use
US8819428B2 *	2011-10-21	2014-08-26	Ebay Inc.	Point of sale (POS) personal identification number (PIN) security
US9137235B2 *	2012-03-23	2015-09-15	Cloudpath Networks, Inc.	System and method for providing a certificate based on list membership
US9118633B2	2013-06-18	2015-08-25	International Business Machines Corporation	Topic protection policy for publish-subscribe messaging system
US10365832B1	2013-06-28	2019-07-16	Winklevoss Ip, Llc	Computer-generated graphical user interface
US9892460B1	2013-06-28	2018-02-13	Winklevoss Ip, Llc	Systems, methods, and program products for operating exchange traded products holding digital math-based assets

US10269009B1	2013-06-28	2019-04-23	Winklevoss Ip, Llc	Systems, methods, and program products for a digital math-based asset exchange
US10068228B1	2013-06-28	2018-09-04	Winklevoss Ip, Llc	Systems and methods for storing digital math-based assets using a secure portal
FR3018378A1 *	2014-03-12	2015-09-11	Enrico Maim	TRANSACTIONAL SYSTEM AND METHOD WITH DISTRIBUTED ARCHITECTURE BASED ON TRANSFER TRANSFERS OF ACCOUNT UNITS BETWEEN ADDRESSES
US10680816B2 *	2014-03-26	2020-06-09	Continental Teves Ag & Co. Ohg	Method and system for improving the data security during a communication process
US9521001B2 *	2014-04-28	2016-12-13	Adobe Systems Incorporated	Privacy preserving electronic document signature service
US11037110B1	2014-05-20	2021-06-15	Wells Fargo Bank, N.A.	Math based currency point of sale systems and methods
US11170351B1	2014-05-20	2021-11-09	Wells Fargo Bank, N.A.	Systems and methods for identity verification of math-based currency account holders
US10909509B1	2014-05-20	2021-02-02	Wells Fargo Bank, N.A.	Infrastructure for maintaining math-based currency accounts
US10565645B1 *	2014-05-20	2020-02-18	Wells Fargo Bank, N.A.	Systems and methods for operating a math-based currency exchange
US10970684B1	2014-05-20	2021-04-06	Wells Fargo Bank, N.A.	Systems and methods for maintaining deposits of math-based currency
US11176524B1	2014-05-20	2021-11-16	Wells Fargo Bank, N.A.	Math based currency credit card
US11062278B1	2014-05-20	2021-07-13	Wells Fargo Bank, N.A.	Systems and methods for math-based currency credit transactions
US9258117B1	2014-06-26	2016-02-09	Amazon Technologies, Inc.	Mutual authentication with symmetric secrets and signatures
CA2959732A1 *	2014-09-08	2016-03-17	Good Technology Holdings Limited	Shared lock state
US10481763B2 *	2014-09-17	2019-11-19	Lettrs LLC.	Mobile stamp creation and management for digital communications
US9985933B2 *	2014-12-29	2018-05-29	Entefy Inc.	System and method of sending and receiving secret message content over a network
US9990513B2	2014-12-29	2018-06-05	Entefy Inc.	System and method of applying adaptive privacy controls to lossy file types
US9614681B2 *	2015-01-09	2017-04-04	Adobe Systems Incorporated	Private electronic signature service for electronic documents
US9853977B1	2015-01-26	2017-12-26	Winklevoss Ip, Llc	System, method, and program product for processing secure transactions within a cloud computing system
US10915891B1	2015-03-16	2021-02-09	Winklevoss Ip, Llc	Autonomous devices
US10158480B1	2015-03-16	2018-12-18	Winklevoss Ip, Llc	Autonomous devices
WO2016161073A1 *	2015-03-31	2016-10-06	Nasdaq, Inc.	Systems and methods of blockchain transaction recordation
TWI581599B *	2015-04-30	2017-05-01	鴻海精密工業股份有限公司	Key generation system, data signature and encryption system and method
US10607913B2 *	2015-05-05	2018-06-26	ShoCard, Inc.	Identity management service using a blockchain providing identity transactions between devices
US9876646B2	2015-05-05	2018-01-23	ShoCard, Inc.	User identification management system and method
US10122889B2 *	2015-06-16	2018-11-06	Amazon Technologies, Inc.	Load balancing with handshake offload
US10122692B2 *	2015-06-16	2018-11-06	Amazon Technologies, Inc.	Handshake offload
EP3317775A4	2015-07-02	2019-02-20	Nasdaq, Inc.	Systems and methods of secure provenance for distributed transaction databases
US10027688B2	2015-07-28	2018-07-17	Entit Software Llc	Shared symmetric key encryption
US10719816B1	2015-11-19	2020-07-21	Wells Fargo Bank, N.A.	Systems and methods for math-based currency escrow transactions
KR101637863B1 *	2016-01-05	2016-07-08	주식회사 코인플러그	Security system and method for transmitting a password
US10108812B2	2016-01-28	2018-10-23	Nasdaq, Inc.	Systems and methods for securing and disseminating time sensitive information using a blockchain

AU2017216289A1	2016-02-04	2018-09-27	Nasdaq Technology Ab	Systems and methods for storing and sharing transactional data using distributed computer systems
US10587609B2	2016-03-04	2020-03-10	ShoCard, Inc.	Method and system for authenticated login using static or dynamic codes
US10509993B2	2016-03-07	2019-12-17	ShoCard, Inc.	Large data transfer using visual codes with feedback confirmation
US10600826B2	2016-03-07	2018-06-26	ShoCard, Inc.	Transferring data files using a series of visual codes
US10104119B2 *	2016-05-11	2018-10-16	Cisco Technology, Inc.	Short term certificate management during distributed denial of service attacks
LU93150B1 *	2016-07-13	2018-03-05	Luxtrust S A	Method for providing secure digital signatures
US10187203B2	2016-08-30	2019-01-22	Workday, Inc.	Secure storage encryption system
US10177908B2	2016-08-30	2019-01-08	Workday, Inc.	Secure storage decryption system
US10460118B2	2016-08-30	2019-10-29	Workday, Inc.	Secure storage audit verification system
US10505741B1 *	2016-09-29	2019-12-10	Amazon Technologies, Inc.	Cryptographically provable data certification and provenance
US10547457B1 *	2016-10-21	2020-01-28	Wells Fargo Bank N.A.	Systems and methods for notary agent for public key infrastructure names
US10484181B2 *	2016-12-12	2019-11-19	Datiphy Inc.	Streaming non-repudiation for data access and data transaction
US11049210B2 *	2016-12-27	2021-06-29	Fotonation Limited	Systems and methods for detecting data insertions in biometric authentication systems utilizing a secret
US10587585B2	2016-12-31	2020-03-10	Entefy Inc.	System and method of presenting dynamically-rendered content in structured documents
US10003741B2	2016-12-31	2018-07-31	Entefy Inc.	System and method of applying multiple adaptive privacy control layers to encoded media file types
US10395047B2	2016-12-31	2019-08-27	Entefy Inc.	System and method of applying multiple adaptive privacy control layers to single-layered media file types
US10169597B2	2016-12-31	2019-01-01	Entefy Inc.	System and method of applying adaptive privacy control layers to encoded media file types
GB201700367D0 *	2017-01-10	2017-02-22	Trustonic Ltd	A system for recording and attesting device lifecycle
US10581909B2 *	2017-06-26	2020-03-03	Oath Inc.	Systems and methods for electronic signing of electronic content requests
US10484397B2 *	2017-06-30	2019-11-19	Fortinet, Inc.	Automatic electronic mail (email) encryption by email servers
US10410000B1	2017-12-29	2019-09-10	Entefy Inc.	System and method of applying adaptive privacy control regions to bitstream data
US10630683B1	2017-12-29	2019-05-28	Entefy Inc.	System and method of applying multiple adaptive privacy control layers to multi-channel bitstream data
US10540654B1	2018-02-12	2020-01-21	Winklevoss Ip, Llc	System, method and program product for generating and utilizing stable value digital assets
US11113995B1	2018-02-12	2021-10-05	Winklevoss Ip, Llc	Systems, methods, and program products for loaning digital assets and for depositing, holding and/or distributing collateral as a token in the form of digital assets on an underlying blockchain
US10373158B1	2018-02-12	2019-08-06	Winklevoss Ip, Llc	System, method and program product for modifying a supply of stable value digital asset tokens
US10438290B1	2018-03-05	2019-10-08	Winklevoss Ip, Llc	System, method and program product for generating and utilizing stable value digital assets
US10929842B1	2018-03-05	2021-02-23	Winklevoss Ip, Llc	System, method and program product for depositing and withdrawing stable value digital assets in exchange for fiat
US10373129B1	2018-03-05	2019-08-06	Winklevoss Ip, Llc	System, method and program product for generating and utilizing stable value digital assets
US10491404B1	2018-09-12	2019-11-26	Hotpyp, Inc.	Systems and methods for cryptographic key generation and authentication
CN109040134B *	2018-09-28	2021-03-16	武汉斗鱼网络科技有限公司	Information encryption design method and related device
US11082221B2	2018-10-17	2021-08-03	Ping Identity Corporation	Methods and systems for creating and recovering accounts using dynamic passwords
US10979227B2	2018-10-17	2021-04-13	Ping Identity Corporation	Blockchain ID connect

CN109450881B *	2018-10-26	2019-10-15	天津海泰方圆科技有限公司	A kind of data transmission system, method and device
US11099975B2	2019-01-24	2021-08-24	International Business Machines Corporation	Test space analysis across multiple combinatoric models
US11106567B2	2019-01-24	2021-08-31	International Business Machines Corporation	Combinatoric set completion through unique test case generation
US10715330B1 *	2019-04-23	2020-07-14	Accenture Global Solutions Limited	Cryptologic blockchain-based custody and authorization tracking for physical concessions
US10970197B2 *	2019-06-13	2021-04-06	International Business Machines Corporation	Breakpoint value-based version control
US11170130B1	2021-04-08	2021-11-09	Aster Key, LLC	Apparatus, systems and methods for storing user profile data on a distributed database for anonymous verification

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
DE602272470D1	2008-08-07	SYSTEM AND METHOD FOR ENCRYPTING MESSAGES AND REGISTERING IN A TRANSACTION PROCESSING SYSTEM
DE60131833D1	2008-01-24	METHOD AND DEVICE FOR EXCHANGING INFORMATION IN A COMMUNICATION SYSTEM
DE60019173D1	2005-05-04	METHOD AND SYSTEM FOR HIGH-PARALLEL RECOVERY AND RECOVERY OPERATION IN MAIN STATION TRANSACTION PROCESSING SYSTEMS
DE602386840D1	2011-02-03	METHOD AND SYSTEM FOR PREVENTING TRANSFER GRINDING IN A LABEL LINKING AREA
DE60007883D1	2004-02-26	METHOD AND DEVICE FOR CARRYING OUT ELECTRONIC TRANSACTIONS
AU6680201A	2001-12-17	Method and system for automated transaction compliance processing
DE60307604D1	2006-09-28	METHOD AND DEVICE FOR CARRYING OVERPASS IN A COMMUNICATION SYSTEM SUPPORTING SEVERAL SERVICE POINTS
DE60113539D1	2006-02-02	METHOD AND DEVICE FOR PROVIDING COMPUTER SERVICES
DE602274960D1	2008-08-21	METHOD AND SYSTEM FOR ADMINISTERING CONFIGURATION CHANGES IN A DATA PROCESSING SYSTEM
DE50000288D1	2002-08-22	DEVICE AND METHOD FOR HIDING INFORMATION, AND DEVICE AND METHOD FOR EXTRACTING INFORMATION
DE10196669T1	2003-08-21	System and method for facilitating electronic commerce transactions
DE60209579D1	2006-04-27	Apparatus and method for transmitting / receiving error detection information in a communication system
DE60119403D1	2006-06-14	Apparatus and method for changing card information
DE69922970D1	2005-02-03	METHOD AND DEVICE FOR COUNTING POLLENKÖRNERN
DE60216767D1	2007-01-25	PROCESS AND DEVICE FOR THE REPLACEMENT OF SOFTWARE INFORMATION IN A DATA PACKET TRANSMISSION SYSTEM
DE60123111D1	2006-10-26	METHOD AND DEVICE FOR PROCESSING SEISMATIC DATA
AT384390T	2008-02-15	DEVICE AND SYSTEM FOR RECALLING INFORMATION IN A NETWORK
EP1301845A4	2009-10-28	Automated transaction machine system and method
DE60231344D1	2009-04-09	METHOD AND DEVICE FOR PROCESSING TRANSACTIONS IN A DATA PROCESSING SYSTEM
AT263725T	2004-04-15	METHOD AND DEVICE FOR CONVEYING OBJECTS
AT445296T	2009-10-15	METHOD AND DEVICE FOR PRIORIZING INTERRUPTS IN A COMMUNICATION SYSTEM
DE59903326D1	2002-12-12	METHOD AND DEVICE FOR PROCESSING DATA
DE59901901D1	2002-08-08	Method and device for sorting out short lengths in fine steel alignment
AT227445T	2002-11-15	METHOD AND DEVICE FOR PROCESSING DATA
DE69935216D1	2007-04-05	Method and device for grinding curved surfaces

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
US27110601P	2001-02-22	2001-02-22	*US Provisional Application*

Legal Events

Date	Code	Title	Description
2008-12-15	RER	Ceased as to paragraph 5 lit. 3 law introducing patent treaties	

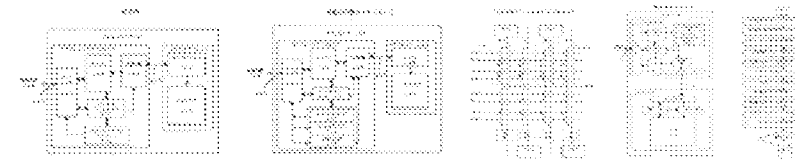
Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

Patents JP4086584

Memory card capable of simplifying test process and memory card test method

Images (6)



Classifications

G11C29/48 Arrangements in static stores specially adapted for testing by means external to the store, e.g. using direct memory access [DMA] or using auxiliary access paths

JP4086584B2
Japan

Download PDF Find Prior Art Similar

Other languages: Japanese

Inventor: 秀之 吉川

Worldwide applications

2002 JP 2003 US

Application JP2002231453A events

2002-08-08 Application filed by 富士通株式会社
2002-08-08 Priority to JP2002231453A
2004-03-04 Publication of JP2004070806A
2008-05-14 Application granted
2008-05-14 Publication of JP4086584B2
Status Active
2022-08-08 Anticipated expiration

Info: Patent citations (3), Cited by (12), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (8) Hide Dependent

1. In the memory card,
A memory chip and a buffer connected to the memory chip and temporarily storing data, and a controller for transferring data between the outside and the memory chip via the buffer;
In the first operation mode, the controller clears the data in the buffer when the data in the buffer is transferred to the memory chip. In the second operation mode, the controller clears the data in the buffer to the memory chip. A memory card characterized by not clearing data in the buffer when transferred.

2. In claim 1,
The memory card, wherein the controller transfers data in the buffer to a memory chip in response to an external write command.

3. In claim 1,
The controller includes a transfer circuit that transfers data in the buffer to the memory chip, and the transfer circuit transfers the data in the buffer to the memory chip without inversion in the non-inversion mode, and the inversion mode. A memory card characterized in that the data in the buffer is inverted and transferred to the memory chip at the time.

4. A memory card test method comprising: a memory chip; and a controller connected to the memory chip and having a buffer for temporarily storing data, and a controller for transferring data between the outside and the memory chip via the buffer In
Inputting predetermined write data into a memory card and storing it in the buffer;
Repetitively inputting a write destination address and a write command to the memory card, and writing the write data stored in the buffer to the write destination address in the memory chip,
In the writing step, a non-clear mode that is not cleared when write data stored in the buffer is transferred to the memory chip is set.

5. In claim 4,
The method for testing a memory card, wherein the writing step is repeated a plurality of times for one storing step.

6. A memory card test method comprising: a memory chip; and a controller connected to the memory chip and having a buffer for temporarily storing data, and a controller for transferring data between the outside and the memory chip via the buffer In
Inputting predetermined write data into a memory card and storing it in the buffer;
A first writing step of inputting a first group of write destination addresses and a write command to the memory card and causing the write data stored in the buffer to be written to the write destination addresses in the memory chip without being inverted;
A second writing step of inputting a second group of write destination addresses and a write command to the memory card, inverting the write data stored in the buffer,

and writing to the write destination address in the memory chip; And
In the writing step, a non-clear mode that is not cleared when write data stored in the buffer is transferred to the memory chip is set.

7. in claim 6,
A test method for a memory card, wherein the first writing step and the second writing step are alternately repeated.

8. in claim 6,
A method for testing a memory card, wherein the first writing step and the second writing step are each repeated continuously.

Description

[0001]
BACKGROUND OF THE INVENTION
The present invention relates to a memory card with a built-in memory chip, and more particularly to a memory card that can simplify a test process. Furthermore, the present invention relates to a method for testing a memory card
[0002]
[Prior art]
Memory cards are widely used as data storage media such as digital cameras. Such a memory card incorporates a flash memory which is a semiconductor nonvolatile memory. In addition, in order to perform input / output control to the flash memory, the memory card incorporates a controller chip in addition to the memory chip.
[0003]
FIG. 1 is a configuration diagram of a conventional memory card. The memory card 101 is connected to an external device 104 such as a digital camera via the external terminal 100. In the memory card 101, a memory chip 103 having a memory core 110 and an input / output buffer 109, and a controller chip 102 for controlling writing, reading, erasing and the like to the memory chip 103 are incorporated. .
[0004]
The memory chip 103 has many external terminals 107 such as a command terminal, an address terminal, a data input / output terminal, and a power supply terminal, and is connected to the controller chip 102. On the other hand, the number of external terminals 100 of the memory card 101 must be reduced in order to eliminate data inversion errors due to noise. Therefore, the controller chip 102 temporarily stores write data and addresses from the external device 104 in the buffer 105, and further transfers the data and addresses to the memory chip 103 together with a control command from the external device 104.
[0005]
The controller chip 102 includes a card interface 111, a buffer 105, a transfer circuit 106 that performs transfer with the memory chip 103, and a buffer controller 108 that controls the buffer 105. Furthermore, the controller chip 102 has a buffer status register 112 that indicates that valid data and addresses are stored in the buffer 105.
[0006]
An example of a conventional memory card writing operation is as follows. A data transfer command and transfer data are serially input via the external terminal 100, and the transfer data is stored in the buffer 105. This is called external transfer. Subsequently, an address transfer command and a transfer address are serially input, and the transfer address is also stored in the buffer 105. As valid data is stored in the buffer 105, the buffer controller 108 sets the flag of the buffer status register 112 to "1". When a memory access command and a write command indicating the access contents are serially input, the buffer controller 108 checks the valid flag "1" of the buffer status register 112 and transfers the transfer data and transfer address in the buffer 105. Are transferred to the input / output buffer 109 of the memory chip 103 via the transfer circuit 106. This is called internal transfer. At this time, the write command is also transferred to the memory chip 103. As a result, data writing to the memory core 110 is completed. When the internal transfer is performed, the buffer controller 108 clears the flag of the buffer status register 112 to "0". As a result, the data in the buffer 105 is cleared.
[0007]
[Problems to be solved by the invention]
In the shipping test process, predetermined data is written to the memory card, and it is checked whether the data can be read correctly. In the shipping test, it is necessary to write data that is likely to cause a read error due to a defect. For example, in order to detect a short defect between adjacent bit lines, inverted data is written in adjacent cells. Alternatively, checker pattern data that is inverted vertically and horizontally is written in four adjacent cells.
[0008]
However, as described above, the number of external terminals 100 of the memory card is small, and it takes a long time to write test data through such an external terminal with a narrow bus width. In particular, along with the recent high integration and large capacity of flash memory, the memory capacity of memory cards tends to increase. Therefore, the man-hours for writing the test pattern are increased, leading to an increase in the cost of the memory card.
[0009]
Accordingly, an object of the present invention is to provide a memory card that can reduce the number of writing steps.
[0010]
[Means for Solving the Problems]
In order to achieve the above object, according to one aspect of the present invention, in a memory card having a memory chip and a controller connected to the memory chip and transferring data from the outside, the controller includes a buffer for temporarily storing data. In the first operation mode, the controller clears the data in the buffer when the data in the buffer is transferred to the memory chip. In the second operation mode, the controller clears the data in the buffer to the memory chip. The data in the buffer is not cleared.
[0011]
Further, in a more preferred embodiment of the above aspect of the invention, the controller further comprises a transfer circuit for transferring the data in the buffer to the memory chip, and the controller inverts the data in the buffer when in the inversion mode. The data is transferred to the memory chip, and in the non-inversion mode, the data in the buffer is transferred to the memory chip without being inverted.
[0012]
According to the above invention, in addition to the first mode in which the transferred data in the buffer is cleared when the data in the buffer transferred from the outside is internally transferred to the memory chip, the second mode that is not cleared is set. Thus, when writing the test pattern in the test process, the externally transferred data can be internally transferred a plurality of times and written to the memory chip. Therefore, it is not necessary to repeat external transfer and internal transfer every time, and the number of writing processes can be reduced.
[0013]
Further, according to the above preferred embodiment, since the transfer circuit is provided in the controller so that either the transfer mode or the non-transfer mode can be selected, the test pattern once transferred externally is directly or inverted. Can be transferred internally to the memory chip. Therefore, a test pattern of a checker pattern often used as a test pattern can be written into the memory chip with a small number of man-hours.
[0014]
In a preferred embodiment of the above invention, the controller includes a first register in which the first operation mode and the second operation mode are specified, and a second register in which the inversion mode and the non-inversion mode are specified. . Therefore, by setting the mode in these registers from the outside, data once stored in the buffer by external transfer can be transferred to the memory chip as it is or after being inverted.

[0015]

DETAILED DESCRIPTION OF THE INVENTION

Embodiments of the present invention will be described below with reference to the drawings. However, the protection scope of the present invention is not limited to the following embodiments, but extends to the invention described in the claims and equivalents thereof.

[0016]

FIG. 2 is a schematic configuration diagram of the memory card in the present embodiment. In FIG. 2, the same reference numerals are given to the same components as in FIG. The memory card 101 according to the present embodiment internally transfers the data in the buffer to the memory chip in addition to the buffer status register 112 indicating that valid data is stored in the buffer 105 in the controller chip 102. in some cases, it has a buffer clear register 113 for setting whether to clear data in the buffer or not, and an inversion register 114 for setting mode whether to invert data in the buffer during internal transfer. Further, the transfer circuit 106 has a function of inverting the internally transferred data according to the inverting mode of the inverting register 114.

[0017]

The buffer clear register 113 can set a clear mode in which data in the buffer 105 is cleared after internal transfer and a non-clear mode in which data is not cleared Therefore, if the register 113 is set to the non-clear mode in the test process, first, when predetermined write data is stored as a test pattern in the buffer 105 in the controller chip 102 by external transfer, the stored write is thereafter performed. Since the data is not cleared by internal transfer, the write data can be internally transferred to the memory chip 103 a plurality of times while changing the address. Therefore, it is not necessary to repeat the external transfer and the internal transfer every time as in the prior art.

[0018]

Further, the inversion register 114 can set a non-inversion mode in which the transfer circuit 106 does not invert data in the buffer and an inversion mode in which the data is inverted during internal transfer. Therefore, by appropriately setting the inversion mode in the test process, the write data stored in the buffer by the first external transfer can be inverted and internally transferred to the memory chip 103. Therefore, even when it is necessary to write the inversion pattern at a predetermined address in the test process, the external transfer can be omitted.

[0019]

FIG. 3 is a schematic configuration diagram of a memory core of a NAND flash memory. A flash memory is often used as a memory chip built in a memory card. The NAND flash memory shown in FIG. 3 is provided with a plurality of bit lines BL0 to BL3 in the column direction and a plurality of word lines WL0-0 to WLn-0 and WL0-1 to WLn-1 in the row direction. . A memory cell MC is connected to the word line. A plurality of memory cells MC are connected in series to form a cell string CST. The cell string CST is connected to the bit line via a transistor that is turned on by the selection signals SG1-0 and SG1-1, and the selection signal SG2 -0 and SG2-1 are connected to the in-array ground voltage ARVSS via a transistor that is turned on. Each bit line is provided with page buffers PB0 to PB3 for temporarily storing write data, detecting the bit line potential, and temporarily storing read data.

[0020]

The failure mode detected in the shipping test includes a failure mode in which adjacent bit lines are short-circuited, short-circuited via a PN junction, and similarly, word lines are similarly short-circuited. There are many. In order to detect such a defect, it is effective to write an inversion pattern in an adjacent memory cell MC and check whether the inversion pattern can be read normally. That is, it is effective to write and read a checker pattern composed of data that is inverted in the left, right, up and down directions to adjacent memory cells.

[0021]

in this case, depending on the correspondence between the page buffer or memory cell and the address, a predetermined test pattern is written as it is or in an inverted manner according to the address. For example, when the word line WL0-0 is selected at the first address and the write data is written into the memory cells from all the page buffers PB, the write data is preferably "0101". By using such write data, inverted data is written in the memory cells adjacent to the left and right, and therefore, if the adjacent bit lines are short-circuited, the read data will be different. It is possible to detect a defective mode. In addition, when the adjacent word line is selected at the second address and the write data is written from all the page buffers PB to the memory cells, it is preferably "1010" which is the inversion pattern of the write data. . As a result, inverted data is written in the vertically adjacent memory cells, so that a failure mode in which adjacent word lines are short-circuited can be detected.

[0022]

In another correspondence relationship, write data may be written from the even-numbered page buffers PB0 and PB2 at the first address, and write data may be written from the odd-numbered page buffers PB1 and PB3 at the second address. . In this case, it is preferable to set the write data to "00" for the first address, for example, and set the write data to "11" for the second address. Thereby, the write data "0101" can be written to the memory cells connected to the common word line. After the selection of the word line is shifted, the write data is set to "11" for the first address and the write data is set to "00" for the second address. Can write.

[0023]

Thus, depending on the configuration of the memory core, the test pattern that can detect the failure mode differs. However, in any case, if a predetermined test pattern can be inverted and written to a different address, the failure mode can be detected

[0024]

Returning to the memory card of FIG. 2, in the test process, the buffer clear register 113 is set to the non-clear mode, predetermined write data is transferred to the buffer 105 by external transfer, and thereafter the inversion register 114 is set according to the address. By switching to the inversion mode or non-inversion mode, the write data in the buffer is internally transferred to the memory chip 103, so that external transfer can be omitted and a test pattern necessary for defective mode detection can be internally transferred to the memory chip. .

[0025]

FIG. 4 is a detailed configuration diagram of the memory card in the present embodiment. Again, the same reference numbers are given to the same components as in FIG. The memory card of FIG. 4 is provided with a command controller 118 and a memory interface 116 in the controller chip 102 in addition to the configuration of the memory card of FIG. The command controller 118 decodes the operation command supplied along with the memory access command, and causes the buffer controller 108 to perform control according to the operation command. Examples of the operation command include a write command, a read command, and an erase command. Further, the memory chip 103 of the memory card of FIG. 4 is provided with a memory interface 120 and a control unit 121 that performs operation control. The control unit 121 performs corresponding operation control on the memory core 110 in accordance with an operation command supplied from the controller chip 102.

[0026]

A normal write operation in FIG. 4 will be described. First, a normal write operation will be described. In the default state, the buffer clear register 113 is set to the clear mode flag "1", and the inversion register 114 is set to the non-inversion mode flag "0".

[0027]

When a data transfer command and write data are serially input from the external device 104 via the external terminal 100, the card interface 111 interprets the data transfer command, transfers the write data to the buffer 105, and stores it. . Similarly, when the address transfer command and the write destination address are serially input, the card interface 111 interprets the address transfer command and transfers the write destination address to the buffer 105 for storage. Accordingly, the buffer controller 108 sets the buffer clear status register 112 to the valid flag "1" in order to indicate that valid data or the like has been stored in the buffer 105.

[0028]

When the memory access command and the write command are input serially, the card interface 111 interprets the memory access command and transfers the write command to the command controller 118. The command controller 118 interprets the write command and internally transfers the write data and the write destination address stored in the buffer 105 to the buffer controller 108 to the memory chip 103 via the transfer circuit 106 and the memory interface 116. At this time, the transfer circuit 106 confirms that the inversion register 114 is in the non-inversion mode, and transfers the write data to the memory chip without inversion. This internal transfer

is performed via the internal connection terminal 107 having a large bus width. At the time of this internal transfer, a write command is also supplied to the memory chip 103.

[0029]

In response to this internal transfer, the control unit 121 of the memory chip 103 performs control to write the write data to the write destination address. After the internal transfer, the buffer controller 108 confirms that the buffer clear register 113 is in the clear mode, changes the buffer status register 112 to the invalid flag "0", and clears the data and address in the buffer 105. . The above is the normal write operation.

[0030]

Next, the write operation in the test process will be described. FIG. 5 is a flowchart showing a first example of the write operation in the test process according to the present embodiment. In the test process, a clear register write command and register data "0" are input from a test device which is an external device, and the buffer controller 108 sets the buffer clear register 113 to "0" in the non-clear mode (S401). Next, a data transfer command and write data are serially input from the external device, and the write data is externally transferred to the memory card 101 (S402). In response to this, the card interface 111 stores the write data in the buffer 105, and the buffer controller 108 sets the buffer status register 112 to valid "1" (S403). This write data is checker pattern data such as "0101

[0031]

The external device serially inputs an inversion register write command and non-inversion data "0", and the buffer controller 108 sets the inversion register 114 to "0" in the non-inversion mode (S404). Then, the external device inputs an address transfer command and a write destination address, stores the write address in the buffer 105, and further inputs a memory access command and a write command (S405). The write address at this time is an even address. Specifically, it is assumed that write data is supplied from all page buffers to all bit lines for the row address for selecting the word line in FIG.

[0032]

The write command is interpreted by the command controller 118, and the buffer controller 108 confirms that the buffer status register 112 is valid "1", and transfers the write data in the buffer 105 to the transfer circuit 106. Since the inverting register 114 is in the non-inverting mode "0", the transfer circuit 106 supplies the write data from the memory interface 116 to the memory chip 103 without inverting the write data. At this time, a write destination address and a write command are also supplied to the memory chip 103. In response to this, the memory chip 103 writes the write data to the write destination address (S406).

[0033]

After the internal transfer of the data, the buffer controller 108 confirms that the buffer clear register 113 is "0" in the non-clear mode, and maintains the valid state "1" of the buffer status register 112. As a result, the write data in the buffer 105 is not cleared (S407).

[0034]

Next, an inversion register write command and inversion data "1" are input from the external device, and the inversion register 114 is set to the inversion mode (S408). Then, an address transfer command and an odd write destination address are serially input from an external device, and further a memory access command and a write command are serially input (S409). In response to this, the buffer controller 108 outputs the write data in the buffer 105 to the transfer circuit 106. Since the inversion register 114 is in the inversion mode, the transfer circuit inverts the write data and internally transfers the data "1010..." From the memory interface 116 to the memory chip 103. Further, the write destination address and the write command are also transferred, and the memory chip writes the internally transferred write data to the even write address (S410). After the internal transfer, the write data in the buffer 105 is not cleared (S411).

[0035]

The above steps S404 to S411 are repeated up to the final address (S412). According to the above writing process, the external transfer for transferring the write data through the external terminal 100 having a narrow bus width is performed only once in the process S402. Then, since the internal transfer is performed simply by repeatedly inputting only the write address and the write command to the memory card, the writing process can be shortened. In particular, since write data has a larger amount of data than addresses and commands, external transfer itself requires man-hours, and avoiding repeated external transfer of write data can greatly reduce man-hours

[0036]

FIG. 6 is a flowchart showing a second example of the write operation in the test process according to the present embodiment. In this example, even address writing is repeated, and then odd address writing is repeated. The rest is the same as the first example. Therefore, the same step numbers as in FIG. 5 are given to the respective steps in FIG.

[0037]

First, the buffer clear register 113 is set to the non-clear mode "0" (S401), the write data is transferred to the memory card (S402), the data is stored in the buffer 105 (S403), and the inversion register 114 is non-inverted. Up to the mode "0" (S404) is the same as the first example.

[0038]

Then, an even write address and a write command are input (S405), write data is transferred to the memory chip for writing (S406), and the buffer 105 is not cleared (S407). It repeats until it becomes (S414). Then, after the inversion register 114 of the memory card is set to the inversion mode "1" (S408), the write operation (S409, S410, S411) for the odd address is repeated until the final odd address (S415).

[0039]

As described above, in the second example, writing to even addresses and writing to odd addresses are separately performed, so that it is not necessary to repeat the setting process of the inversion register 114, and the man-hours of the writing process are further reduced. Can do.

[0040]

in the first and second write examples, write addresses are divided into even addresses and odd addresses, and one is internally transferred in the non-inverted mode and the other in the inverted mode. However, as described above, depending on the configuration of the memory core of the memory chip, another address division may be effective. In that case, internal transfer is performed in the non-inversion mode in the first address group, and internal transfer is performed in the inversion mode in the second address group.

[0041]

Furthermore, the command system in the above embodiment is merely an example, and other commands, transfer data, and transfer address formats may be used.

[0042]

The exemplary embodiments are summarized as follows.

[0043]

(Appendix 1) In memory cards,

A memory chip and a buffer connected to the memory chip and temporarily storing data, and a controller for transferring data between the outside and the memory chip via the buffer;

In the first operation mode, the controller clears the data in the buffer when the data in the buffer is transferred to the memory chip. In the second operation mode, the controller clears the data in the buffer to the memory chip. A memory card characterized by not clearing data in the buffer when transferred.

[0044]

(Appendix 2) In Appendix 1,

The memory card, wherein the controller transfers data in the buffer to a memory chip in response to an external write command.

[0045]

(Appendix 3) In Appendix 1,

The memory card, wherein the controller has a buffer clear register for setting the first operation mode and the second operation mode, and the buffer clear register can

be set from the outside.
[0046]
(Appendix 4) In Appendix 1,
The controller includes a transfer circuit that transfers data in the buffer to the memory chip, and the transfer circuit transfers the data in the buffer to the memory chip without inversion in the non-inversion mode, and the inversion mode. A memory card characterized in that the data in the buffer is inverted and transferred to the memory chip at the time.
[0047]
(Appendix 5) In Appendix 4,
The memory card, wherein the controller has an inverting register for setting the inverting mode and the non-inverting mode, and the inverting register can be set from the outside.
[0048]
(Appendix 6) In Appendix 1,
The number of external terminals provided in the controller is smaller than the number of connection terminals between the controller and the memory chip.
[0049]
(Supplementary note 7) Memory having a memory chip and a controller connected to the memory chip and having a buffer for temporarily storing data, and a controller for transferring data between the outside and the memory chip via the buffer In the card testing method, inputting predetermined write data into the memory card and storing it in the buffer;
Repetitively inputting a write destination address and a write command to the memory card, and writing the write data stored in the buffer to the write destination address in the memory chip,
in the writing step, a non-clear mode that is not cleared when write data stored in the buffer is transferred to the memory chip is set.
[0050]
(Appendix 8) In Appendix 7,
The method for testing a memory card, wherein the writing step is repeated a plurality of times for one storing step.
[0051]
(Supplementary note 9) Memory having a memory chip and a controller connected to the memory chip and having a buffer for temporarily storing data, and a controller for transferring data between the outside and the memory chip via the buffer In the card testing method, inputting predetermined write data into the memory card and storing it in the buffer;
A first writing step of inputting a first group of write destination addresses and a write command to the memory card and causing the write data stored in the buffer to be written to the write destination addresses in the memory chip without being inverted;
A second writing step of inputting a second group of write destination addresses and a write command to the memory card, inverting the write data stored in the buffer, and writing to the write destination address in the memory chip, And
In the writing step, a non-clear mode that is not cleared when write data stored in the buffer is transferred to the memory chip is set.
[0052]
(Appendix 10) In Appendix 9,
A test method for a memory card, wherein the first writing step and the second writing step are alternately repeated.
[0053]
(Appendix 11) In Appendix 9,
A method for testing a memory card, wherein the first writing step and the second writing step are each repeated continuously.
[0054]
(Appendix 12) In Appendix 9,
In the first writing step, the controller is set to a non-inversion mode, and in the second writing step, the controller is set to an inversion mode.
[0055]
【The invention's effect】
As described above, according to the present invention, it is possible to reduce the number of writing steps and the test cost in the test process of the memory card.
[Brief description of the drawings]
FIG. 1 is a configuration diagram of a conventional memory card.
FIG. 2 is a schematic configuration diagram of a memory card in the present embodiment. FIG. 3 is a schematic configuration diagram of a memory core of a NAND flash memory.
FIG. 4 is a detailed configuration diagram of a memory card in the present embodiment.
FIG. 5 is a flowchart showing a first example of a write operation in a test process according to the present embodiment.
FIG. 6 is a flowchart showing a second example of a write operation in a test process according to the present embodiment.
[Explanation of symbols]
101 Memory Card 102 Controller Chip 103 Memory Chip 104 External Device 105 Buffer 106 Transfer Circuit

Patent Citations (3)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
KR970008188B1 *	1993-04-08	1997-05-21	가부시끼가이샤 히다찌세이사꾸쇼	Control method of flash memory and information processing apparatus using the same
WO1997032253A1 *	1996-02-29	1997-09-04	Hitachi, Ltd.	Semiconductor memory device having faulty cells
US6646903B2 *	2001-12-03	2003-11-11	Intel Corporation	Ferroelectric memory input/output apparatus

* Cited by examiner, † Cited by third party

Cited By (12)

Publication number	Priority date	Publication date	Assignee	Title

Family To Family Citations

TWI226643B *	2003-10-31	2005-01-11	C One Technology Corp	Simulated SmartMedia/xD-Picture memory card using any nonvolatile memory
JP2005222201A *	2004-02-04	2005-08-18	Matsushita Electric Ind Co Ltd	Memory access device and semiconductor memory card
EP1630657A1 *	2004-08-30	2006-03-01	STMicroelectronics S.r.l.	Embedded storage device with integrated data-management functions and storage system incorporating it
KR100729351B1 *	2004-12-31	2007-06-15	삼성전자주식회사	Nand flash memory device and program method thereof
US7588178B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
DE102005011891B3 *	2005-03-15	2006-09-21	Infineon Technologies Ag	Semiconductor memory unit e.g. dynamic RAM, has I/O skip unit that is erased, when memory cells assigned to data lines are identified as non-functional, and erased skip unit forces error free signal to PF-signal line
KR100694968B1 *	2005-06-30	2007-03-14	주식회사 하이닉스 반도체	Non-volatile memory device and multi-page programming, reading and copyback programming method thereof
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US20100033310A1 *	2008-08-08	2010-02-11	Narendra Siva G	Power negotation for small rfid card
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
US6937526B2	2005-08-30	Memory card enabling simplified test process and memory card test method
US7724573B2	2010-05-25	Nonvolatile semiconductor storage device, nonvolatile semiconductor storage system and method of managing of defective column in nonvolatile semiconductor storage system
US7042770B2	2006-05-09	Memory devices with page buffer having dual registers and method of using the same
US7236424B2	2007-06-26	Semiconductor memory device
KR100785184B1	2007-12-11	Semiconductor memory device
JP4122185B2	2008-07-23	Nonvolatile memory device, program method thereof, and pass / fail inspection method
US7952958B2	2011-05-31	Non-volatile semiconductor storage system
JP2007517353A	2007-06-28	Flexible and area efficient column redundancy for non-volatile memory
TW388881B	2000-05-01	A nonvolatile memory and a semiconductor device with the nonvolatile memory
US7859900B2	2010-12-28	Built-in self-repair method for NAND flash memory and system thereof
US20100195396A1	2010-08-05	Semiconductor memory device and self-test method of the same
US8400406B2	2013-03-26	Semiconductor memory device and method of testing the same
JP2009099202A	2009-05-07	Semiconductor device
JP5023208B2	2012-09-12	Semiconductor memory device and test method thereof
JP5010263B2	2012-08-29	Nonvolatile semiconductor memory device
US7991945B2	2011-08-02	Semiconductor memory device and semiconductor device
EP0844619A2	1998-05-27	Nonvolatile semiconductor memory device having test circuit for testing erasing function thereof
US20010014034A1	2001-08-16	Nonvolatile semiconductor memory device
JP2005141417A	2005-06-02	Memory controller and flash memory system having the same, and control method for flash memory
JPH10511205A	1998-10-27	Floating gate memory device with protocol for terminating program load cycle
JP2003203500A	2003-07-18	Semiconductor memory device, test board, and test method

JP2000340380A	2000-02-08	Nonvolatile semiconductor storage

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
JP2002231453A	2002-08-08	2002-08-08	Memory card capable of simplifying test process and memory card test method

Applications Claiming Priority (2)

Application	Filing date	Title
JP2002231453A	2002-08-08	Memory card capable of simplifying test process and memory card test method
US10/634,757	2003-08-06	Memory card enabling simplified test process and memory card test method

Legal Events

Date	Code	Title	Description
2005-07-05	A621	Written request for application examination	**Free format text:** JAPANESE INTERMEDIATE CODE: A621 **Effective date:** 20050704
2008-02-12	TRDD	Decision of grant or rejection written	
2008-02-12	A977	Report on retrieval	**Free format text:** JAPANESE INTERMEDIATE CODE: A971007 **Effective date:** 20080212
2008-02-20	A01	Written decision to grant a patent or to grant a registration (utility model)	**Free format text:** JAPANESE INTERMEDIATE CODE: A01 **Effective date:** 20080219
2008-02-28	A61	First payment of annual fees (during grant procedure)	**Free format text:** JAPANESE INTERMEDIATE CODE: A61 **Effective date:** 20080219
2008-02-29	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20110228 **Year of fee payment:** 3
2008-02-29	R150	Certificate of patent or registration of utility model	**Ref document number:** 4086584 **Country of ref document:** JP **Free format text:** JAPANESE INTERMEDIATE CODE: R150 **Free format text:** JAPANESE INTERMEDIATE CODE: R150
2008-08-06	S111	Request for change of ownership or part of ownership	**Free format text:** JAPANESE INTERMEDIATE CODE: R313111
2008-08-14	R350	Written notification of registration of transfer	**Free format text:** JAPANESE INTERMEDIATE CODE: R350
2008-08-14	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20110228 **Year of fee payment:** 3
2010-12-02	S533	Written request for registration of change of name	**Free format text:** JAPANESE INTERMEDIATE CODE: R313533
2010-12-02	S531	Written request for registration of change of domicile	**Free format text:** JAPANESE INTERMEDIATE CODE: R313531
2010-12-02	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20110228 **Year of fee payment:** 3
2010-12-10	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20110228 **Year of fee payment:** 3

2010-12-10	R350	Written notification of registration of transfer	Free format text: JAPANESE INTERMEDIATE CODE: R350
2011-01-04	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20120229 Year of fee payment: 4
2011-12-27	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20130228 Year of fee payment: 5
2013-01-29	FPAY	Renewal fee payment (event date is renewal date of database)	Free format text: PAYMENT UNTIL: 20140228 Year of fee payment: 6
2015-05-19	S111	Request for change of ownership or part of ownership	Free format text: JAPANESE INTERMEDIATE CODE: R313111
2015-05-27	R350	Written notification of registration of transfer	Free format text: JAPANESE INTERMEDIATE CODE: R350

Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

Patents CA2337672

Payment for network-based commercial transactions using a mobile phone

Abstract

Method for enabling a customer, who has access to a customer system (40) and a mobile phone (43) with associated phone number, to order a deliverable (41) offered by a merchant system (45) at a certain price. The merchant system (45) is accessed through the customer system (40) and a network (44). The deliverable (41) can be ordered using the customer system (40). An order confirmation for the deliverable (41) is sent to the mobile phone (43) using the phone number of this phone and the ordering of the deliverable (41) is confirmed by using the mobile phone (43) to transmit a response to the merchant system (45) or to a carrier system (48). The phone bill (51) issued by the carrier system (48) for the mobile phone (43) is charged with the deliverable's price and the deliverable (41) is made available to the customer.

Classifications

G06Q20/16 Payments settled via telecommunication systems

View 10 more classifications

CA2337672A1

Canada

Download PDF Find Prior Art Similar

Other languages: French

Inventor: Dirk Husemann, Reto Hermann, Michael Moser, Andreas Schade

Current Assignee : International Business Machines Corp

Worldwide applications

2001 CA SG JP US

Application CA002337672A events

2000-04-26 Priority to EP00108820.2

2000-04-26 Priority to EP00108820

2001-02-22 Application filed by International Business Machines Corp

2001-10-26 Publication of CA2337672A1

Status Abandoned

Info: Patent citations (5), Cited by (175), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, CIPO, Discuss

Claims (43)

Hide Dependent

1. Method for enabling a customer, who has access to a customer system (40;
70) and a mobile phone (43; 73) with associated phone number, to order a deliverable (41; 71) offered by a merchant system (45; 75) at a certain price, comprising ~ accessing the merchant system (45; 75) through the customer system (40; 70) and a network (44; 74);
~ performing an action on the customer system (40; 70) to order the deliverable (41; 71);
~ obtaining the phone number of the mobile phone (43; 73);
~ sending an order confirmation for the deliverable (41; 71) to the mobile phone (43; 73) using the phone number of the mobile phone (43; 73);
~ confirming the ordering of the deliverable (41; 71) by using the mobile phone (43; 73) to transmit a response to the merchant system (45; 75) or to a carrier system (48; 78);
~ charging a phone bill (51; 81) issued by the carrier system (48, 78) for the mobile phone (43; 73) with the certain price, and ~ making the deliverable (41; 71) available to the customer.

2. Method for ordering a deliverable (41; 71) that is offered. by a merchant system (45; 75) at a certain price, comprising ~ accessing the merchant system (45; 75) through a customer system (40; 70) and a network (44; 74);
~ displaying the deliverable (41; 71) to a customer on the customer system (40, 70);

performing an action on the customer system (40; 70) to order the deliverable (41; 71) at the merchant system (45; 75);
~ sending the phone number of a mobile phone (43; 73) of the customer to the merchant system (45, 75);
~ receiving an order confirmation for the deliverable (41; 71) on the mobile phone (43; 73);
~ confirming the ordering of the deliverable (41; 71) using the mobile phone (43, 73) to transmit a response to the merchant system (45; 75) or a carrier system (48;
78);
~ obtaining the deliverable (41; 71).

3. Method for processing by a merchant system (45; 75) the order of a customer for a deliverable (41; 71) that is offered by the merchant system (45; 75) at a certain price, the customer having access to a customer system (40; 70) and a mobile phone (43;
73) with associated phone number, comprising ~ enabling the customer system (40; 70) to display the deliverable (41; 71) to the customer;
~ enabling the customer to order the deliverable (41; 71) at the merchant system (45; 75) via the customer system (40; 70) and a network (44; 74);
~ enabling the sending of an order confirmation for the deliverable (41; 71) to the mobile phone (43; 73) using the phone number;
~ receiving an order confirmation or payment confirmation from a carrier system (48; 78);
and ~ making the deliverable (41; 71) available to the customer.

4. Method for handling by a carrier system (48; 78) the payment process for a customer who ordered a deliverable (41; 71) through a merchant system (45; 75) at a certain price, the customer having access to a customer system (40, 70) and a mobile phone (43;

73) with associated phone number, comprising ~ obtaining transaction information for the ordering of the deliverable from the merchant system (45; 75);
~ obtaining the phone number of the mobile phone (43; 73),
~ sending an order confirmation for the deliverable (41; 71) to the mobile phone (43; 73) using the phone number;
~ receiving through the mobile phone (43; 73) an order confirmation for the deliverable (41;
71);
~ charging a phone bill (51; 81) maintained by the carrier system (48; 78) for the mobile phone (43; 73) with the certain price; and ~ sending an order confirmation or payment confirmation to the merchant system (45; 75)

5. The method of claim 1 or claim 3, wherein the merchant system (45; 75) offers an online catalog (47; 77) with a plurality of deliverables for selection by the customer.

6. The method of claim 1 or 2, comprising a checkout step (21) after the step of performing an action on the customer system (40; 70) in order to select the deliverable (41;
71).

7. The method of claim 1 or 2, comprising the steps:
~ sending the phone number of the mobile phone (43; 73) from the customer system (40;
70) or the mobile phone (43; 73) to the merchant system (45; 75);

~ storing the phone number so that it is obtainable if needed by the carrier system (48; 78) and/or merchant system (45; 75).

8. The method of claim 3 or 4, comprising the steps:
~ receiving the phone number of the mobile phone (43; 73) from the customer system (40;
70) or the mobile phone (43; 73).
~ storing the phone number so that it is obtainable if needed by the carrier system (48; 78) and/or merchant system (45; 75).

9. The method of claim 1, 3, or 4, wherein the step of sending an order confirmation for the deliverable (41; 71) to the mobile phone (43; 73) is done by means of a GSM SMS message.

10. The method of claim 2, wherein the step of receiving an order confirmation for the deliverable (41; 71) by the mobile phone (43; 73) is done through a GSM SMS message.

11. The method of claim 9 or claim 10, wherein the GSM SMS message comprises a special call-in phone number and/or an order identifier (order ID).

12. The method of claim 10, wherein the customer performs an action on the mobile phone (43;
73) in order to confirm the ordering of the deliverable (41; 71).

13. The method of claim 1, 2, 3, or 4, wherein the mobile phone (43; 73) prompts the customer for a personal identification number (PIN) for authentication purposes.

14. The method of claim 1 or claim 3, wherein a plurality of deliverables is offered for selection by the customer.

15. The method of claim 1, 3, or 4, wherein the step of sending an order confirmation for the deliverable (41; 71) to the mobile phone (43; 73) is done using the push feature of the wireless application protocol (WAP) in order to push a wireless markup language (WML) script applet to the mobile phone (43; 73).

16. The method of claim 1, 2, 3, or 4, wherein the merchant system (45; 75) assigns an order identifier (order ID) for each deliverable (41; 71) or set of deliverables ordered.

17. The method of claim 1, 2, 3, or 4, wherein the merchant system (45; 75) or carrier system (48; 78) maintains a list of open orders.

18. The method of claim 17, wherein a housekeeping process is carried out to remove open orders for which no confirmation is received within a pre-defined period of time.

19. The method of claim 1 or claim 4, wherein the phone bill (51; 81) is either delivered to the customer through a conventional distribution channel (52), preferably by mail, or to the customer system (70) through a communication link (82, 74).

20. Merchant system (45, 75) for offering a deliverable (41; 71) via a network (44, 74) to a potential customer using a customer system (40; 70) and a mobile phone (43;
73), comprising ~ a network interface connectable to the network (44; 74), ~ a processing unit (46; 76);
~ a database (47; 77) for maintaining detailed information about the deliverable (41; 71);
~ a module for making the deliverable and some or all of the detailed information about the deliverable (41; 71) displayable to the potential customer on the customer system (40;
70);
~ a module for making the deliverable (41; 71) selectable by the potential customer on the customer system (40; 70);
~ a module for receiving an order for the deliverable (41; 71) from the customer system (40;
70) via the network and network interface;

a module for causing a confirmation address to be transmitted to the mobile phone (43;
73) through a mobile telephone network (53; 83);
~ a module for receiving an order confirmation issued by the mobile phone (43;
73), or a payment confirmation issued by a carrier system (48; 78);
~ a module for making the deliverable (41; 71) available to the customer.

21. The merchant system (45; 75) of claim 20, whereby some or all of the modules are realized in form of software modules that, when executed by the processing unit (46,
76), provide the modules' functionality.

22. The merchant system (45) of claim 20, comprising a call-in unit (55) connectable to a telephone network (56, 53).

23. The merchant system (45) of claim 22, whereby a special call-in number is assigned to the call-in unit (55) so that the call-in unit (55) is reachable form the mobile phone (43) when dialing the call-in number.

24. The merchant system (45; 75) of claim 20, whereby the processing unit (46; 76) resides in a computer system.

25. The merchant system (45; 75) of claim 20, whereby the module for making the deliverable and some or all of the detailed information about the deliverable (41; 71) displayable is an online-catalogue module.

26. The merchant system (45; 75) of claim 20, whereby the module for making the deliverable (41; 71) available to the customer either causes the deliverable (41; 71) to be delivered via a conventional distribution channel, or whereby the module causes the deliverable (41; 71) to be delivered via a communication link (82, 74) to the customer system (70), or whereby the module causes the deliverable (41; 71) to be made downloadable through a communication link (82, 74).

27. The merchant system (45; 75) of claim 20, whereby the confirmation address is a call-in number or an e-mail address.

28. The merchant system (45, 75) of claim 20, whereby the module for causing a confirmation address to be transmitted generates a GSM SMS message comprising the confirmation address.

29. Carrier system (48; 78) for handling the payment process part of a commercial transaction between a customer, using a customer system (40; 70) and a mobile phone (43; 73), and a merchant system (45; 75), whereby the customer orders a deliverable (41; 71) at a certain price at the merchant system (45; 75); the carrier system (48; 78) comprising ~ an interface connectable to a telephone network (56, 53; 86; 83), ~ a processing unit (49; 79),
~ a module for receiving via a communication link (57; 87) detailed information about the ordered deliverable (41; 71) from the merchant system (45; 75) ~ a module for causing a confirmation address to be transmitted to the mobile phone (43; 73) through a mobile telephone network (53; 83);
~ a module for receiving an order confirmation returned by the mobile phone (43; 73) using the confirmation address;
~ a module (49, 50; 79, 80) for charging the customer's phone bill (51; 81) with the certain price;
~ a module (49; 79) for sending a payment confirmation to the merchant system (45; 75) causing the merchant system (45; 75) to make the ordered deliverable (41; 71) available to the customer.

30 30. The carrier system (48; 78) of claim 29, whereby some or all of the modules are realized in form of software modules that, when executed by the processing unit (49; 79), provide the modules' functionality

31. The carrier system (48; 78) of claim 29, whereby the telephone network is a public switched telephone network (56; 86) that is connectable to the mobile telephone network (53; 83).

32. The carrier system (48; 78) of claim 29, whereby the processing unit (49; 79) resides in a computer system.

33. The carrier system (48; 78) of claim 29, whereby the confirmation address is a call-in number or an e-mail address.

34. The carrier system (48; 78) of claim 29, whereby the module for causing a confirmation address to be transmitted generates a GSM SMS message comprising the confirmation address.

35. The carrier system (78) of claim 29, comprising a call-in unit (85) connectable to the telephone network (86, 83).

36. The carrier system (78) of claim 35, whereby a special call-in number is assigned to the call-in unit (85) so that the call-in unit (85) is reachable form the mobile phone (73) when dialing the call-in number.

37. The carrier system (78) of claim 29, comprising a housekeeping module that removes open orders for which no confirmation is received within a pre-defined period of time.

38. A computer program product comprising a computer readable medium, having thereon:
computer program code means, when said program is loaded, for enabling a customer to order a deliverable (41; 71) that is offered by a merchant system (45; 75) at a certain price, whereby the customer uses a customer system (45; 75) and a mobile phone (43; 73), execute procedure to access the merchant system (45, 75) through the customer system (40; 70) and a network (44; 74);
~ display the deliverable (41; 71) to the customer on the customer system (40; 70);
~ perform an action on the customer system (40; 70) to order the deliverable (41; 71) at the merchant system (45; 75);
~ send the phone number of the mobile phone (43; 73) to the merchant system (45, 75);
~ receive an order confirmation for the deliverable (41; 71) on the mobile phone (43; 73),
~ confirm the ordering of the deliverable (41; 71) using the mobile phone (43; 73) to transmit a response to the merchant system (45; 75) or a carrier system (48; 78);
~ obtain the deliverable (41; 71).

39. A computer program element comprising:
computer program code means for enabling a customer to order a deliverable (41, 71) that is offered by a merchant system (45; 75) at a certain price, whereby the customer uses a customer system (45; 75) and a mobile phone (43; 73), execute procedure to ~ access the merchant system (45; 75) through the customer system (40; 70) and a network (44; 74);
~ display the deliverable (41; 71) to the customer on the customer system (40; 70);
~ perform an action on the customer system (40, 70) to order the deliverable (41; 71) at the merchant system (45; 75);
~ send the phone number of the mobile phone (43; 73) to the merchant system (45; 75);

~ receive an order confirmation for the deliverable (41; 71) on the mobile phone (43; 73);
~ confirm the ordering of the deliverable (41; 71) using the mobile phone (43; 73) to transmit a response to the merchant system (45, 75) or a carrier system (48; 78);
~ obtain the deliverable (41; 71).

40. A computer program product comprising a computer readable medium, having thereon:
computer program code means, when said program is loaded, for processing by a merchant system (45; 75) the order of a customer for a deliverable (41; 71) that is offered by the merchant system (45; 75) at a certain price, the customer having access to a customer system (40; 70) and a mobile phone (43; 73) with associated phone number, execute procedure to ~ enable the customer system (40; 70) to display the deliverable (41; 71) to the customer;
~ enable the customer to order the deliverable (41; 71) at the merchant system (45; 75) via the customer system (40; 70) and a network (44; 74);
~ enable the sending of an order confirmation for the deliverable (41; 71) to the mobile phone (43; 73) using the phone number;
~ receive an order confirmation or payment confirmation from a carrier system (48; 78);
~ make the deliverable (41; 71) available to the customer.

41. A computer program element comprising:
computer program code means for processing by a merchant system (45; 75) the order of a customer for a deliverable (41; 71) that is offered by the merchant system (45; 75) at a certain price, the customer having access to a customer system (40; 70) and a mobile phone (43; 73) with associated phone number, execute procedure to ~ enable the customer system (40; 70) to display the deliverable (41; 71) to the customer;
~ enable the customer to order the deliverable (41; 71) at the merchant system (45; 75) via the customer system (40; 70) and a network (44; 74);
~ enable the sending of an order confirmation for the deliverable (41; 71) to the mobile phone (43; 73) using the phone number;
~ receive an order confirmation or payment confirmation from a carrier system (48; 78);
~ make the deliverable (41; 71) available to the customer.

42. A computer program product comprising a computer readable medium, having thereon:
computer program code means, when said program is loaded, for handling by a carrier system (48; 78) the payment process for a customer who ordered a deliverable (41; 71) through a merchant system (45; 75) at a certain price, the customer having access to a customer system (40; 70) and a mobile phone (43; 73) with associated phone number, execute procedure to ~ obtain transaction information for the ordering of the deliverable (41; 71) from the merchant system (45; 75);
~ obtain the phone number of the mobile phone (43; 73);
~ send an order confirmation for the deliverable (41; 71) to the mobile phone (43; 73) using the phone number;
~ receive through the mobile phone (43; 73) an order confirmation for the deliverable (41;
71);
~ charge a phone bill (51, 81) maintained by the carrier system (48; 78) for the mobile phone (43; 73) with the certain price; and ~ send an order confirmation or payment confirmation to the merchant system (45; 75).

43. A computer program element comprising:
computer program code means for handling by a carrier system (48; 78) the payment process for a customer who ordered a deliverable (41; 71) through a merchant system (45; 75) at a certain price, the customer having access to a customer system (40;
70) and a mobile phone (43; 73) with associated phone number, execute procedure to ~ obtain transaction information for the ordering of the deliverable (41; 71) from the merchant system (45; 75);
~ obtain the phone number of the mobile phone (43; 73);
~ send an order confirmation for the deliverable (41; 71) to the mobile phone (43; 73) using the phone number;
~ receive through the mobile phone (43; 73) an order confirmation for the deliverable (41;
71);
~ charge a phone bill (51, 81) maintained by the carrier system (48; 78) for the mobile phone (43; 73) with the certain price; and ~ send an order confirmation or payment confirmation to the merchant system (45; 75).

Description

PAYMENT FOR NETWORK-BASED COMMERCIAL TRANSACTIONS
USING A MOBILE PHONE

TECHNICAL FIELD

The invention concerns a commercial transaction scheme, and in particular the payment process of such a transaction scheme. Also concerned are systems, computer program products, and computer program elements implementing aspects of such a commercial transaction scheme.

BACKGROUND OF THE INVENTION

The advent of the internet and other communications networks led to a whole new set of network-based commercial transaction schemes which are; quite commonly referred to as electronic commerce (herein referred to as e-commerce) schemes. A commercial transaction in its broadest sense comprises three basic activities. A customer selects and orders goods or services. This step or sequence of steps is referred to as ordering process.

After the completion of the ordering process, there is usually a service rendered or some goods delivered by a 'merchant' (herein referred to as delivery process) and there is some money or other consideration to be paid by the 'customer' for these services or goods, referred to as payment process.

Typically, a network-based commercial transaction follows the patterns shown in Figure 1 or Figure 2. Either the customer has to register once (which includes the one-time disclosure of credit-card details) and then whenever the customer returns to a merchant's system identify itself to the system (e.g., by logging in or sending a cookie), or the customer has to provide credit card details every time he enters into a transaction with the merchant.

As shown in Figure 1, in a first step 10, the customer selects one or more deliverables. This can be done by browsing an online catalog, for example. Then., the customer invokes a checkout process - step 11 in Figure 1 - of the merchant's system. In step 12, the customer now needs to disclose credit card details and other data, such as the delivery address, to the merchant. In subsequent step 13, the merchant charges the customer's credit card account.

Finally, the deliverables) are dispatched by the merchant to the customer (step 14 in Figure 1). The network-based commercial transaction scheme illustrated in Figure 1 is a transaction scheme without pre-registration.

Usually, all the steps 10 - 13 take place over the Internet. With some systems the customer can either phone in the credit card number to an operator (or an automated phone menu system) or fax it in. Such a system is described in US patent 5,727,163, assigned to Amazon.Com, Inc.

Instead of providing the merchant with the credit card details, sometimes the customer can provide checking account details and thus authorize the merchant to do a direct debit to the respective account. The company Amazon.de offers this scheme, for example.

A very similar scheme is illustrated in Figure 2. This scheme is different from the one described in connection with Figure 1 in that it comprises a separate one-time registration step 15. This registration step 15 is usually carried out just once, preferably when ordering a deliverable for the first time. During this registration step, the customer registers with the merchant and provides address information and credit-card details to the merchant. Steps 10, 11, 13, and 14 are the same as in Figure 1.

Since the customer has already registered all the necessary information with the merchant in step 15, the merchant simply needs to fetch this information from the merchant system, as depicted by step 16. This is a typical example of a network-based commercial transaction scheme with pre-registration.

An inherent problem of e-commerce over the Internet is the payment process. In most cases the customer is required to enter credit-card details (e.g., the card number, the name of the card holder, and the card's expiry date) into an electronic form and transmit the data - in the best case encrypted - over the Internet to the merchant who is supposed to deliver. The problem with this solution is manifold:

~ The customer has to entrust the credit card details to the merchant; not only can the merchant then potentially use the credit card details for other purposes, the customer also has to trust the merchant to protect the credit card data adequately. Recent events have shown that assumption to be a risky one. Even though the customer at least has the; remedy of disputing the purchase and have the credit card company cancel the transaction, the customer nevertheless carries the burden and risk.

~ The merchant incurs the risk of accepting forged credit card details and delivers without getting reimbursed by the credit card company. The remedy of obtaining clearance from the credit card company is not always economical and typically time-consuming.

~ Payment by credit card is too expensive for small amounts of money.

Mobile telephone systems are very widely used communication systems that are to a large extent independent from the Internet and other networks. There is a secure payment process in place that allows the carriers to bill their customers for the usage of the mobile phone.

The global system for mobile (GSM) communications, an international fast growing digital cellular standard, is one particular example of a very popular mobile telephone system. The GSM

system is a digital-based system created to provide a network which allows customers to use their GSM phones in many countries. The GSM network is implemented by a number of different carriers in different countries. Each Garner has it's own customers, in respect of whom the carrier holds private information relating to names, addresses, billing information, call destinations, and methods of paying bills. The carriers are independently administrated and are responsible for their customers for billing purposes. In other words, there exists a well established and secure payment process between the carriers and their customers.

It is an object of the present invention to provide an improvc;d transaction scheme. It is another object of the present invention to provide an implementation for such an improved transaction scheme.

I I. SUMMARY OF THE INVENTION

According to the present invention, a transaction scheme is proposed that ties together the existing mobile telephone infrastructure and the fixed network (e.g., the internet) to solve the problems identified in the introductory portion of this specification.

There is therefore provided, in accordance with a preferred embodiment of the present invention, a method for enabling a customer having access to a customer system and a mobile phone with associated phone number, to order a deliverable that is offered by a merchant system at a certain price. The merchant system is accessed through the customer system and a network and an action is performed on the customer system to order the deliverable; The phone number of the mobile phone is used to send an order confirmation for the deliverable to the mobile phone. Then, the ordering of the deliverable is confirmed using the mobile phone to transmit a response to the merchant system or to a carrier system. According to the present invention, a phone bill issued by the carrier system for the mobile phone is charged with the certain price and the deliverable are made available to the customer.

There is moreover provided, in accordance with a preferred embodiment of the present invention, a method for ordering a deliverable that is offered by a merchant system at a certain price. In accordance with the invention, the merchant system is accessed through a customer system and network. The deliverable is displayed to a customer on the customer system and an action is performed on the customer system to order the deliverable. The phone number of a mobile phone (43; 73) of the customer is sent to the merchant system .and an order confirmation for the deliverable is received on the mobile phone. The ordering of the deliverable is confirmed using the mobile phone by transmitting a response to the merchant system or to a carrier system.

Finally, the deliverable is obtained by the customer.

Furthermore, there is provided, in accordance with a preferred embodiment of the present invention, a method for processing by a merchant system the order of a customer for a deliverable that is offered by this merchant system at a certain price.

Whereby the customer has access to a customer system and a mobile phone with an associated phone number. According to the invention, the customer system is enabled to display the deliverable and to allow the customer to order the deliverable at the merchant system via the customer system and a network.

An order confirmation for the deliverable is sent to the mobile phone using the phone number and an order confirmation or payment confirmation is received from a carrier system. Then, the deliverable is made available to the customer.

There is moreover provided, in accordance with a preferred embodiment of the present invention, a method for handling by a carrier system the payment process for a customer who ordered a deliverable through a merchant system at a certain price, whereby the customer has access to a customer system and a mobile phone with and associated phone number. According to this method, transaction information and the phone number of the mobile phone are obtained for the ordering of the deliverable from the merchant system. An order confirmation for the deliverable is sent to the mobile phone using the phone number and an order confirmation for the deliverable is received through the mobile phone. A phone bill maintained by the carrier system for the mobile phone is charged with the certain price and an. order confirmation or payment confirmation is sent to the merchant system.

There is moreover provided, in accordance with a preferred embodiment of the present invention, a merchant system for offering a deliverable via a network to a potential customer. Also provided is, in accordance with a preferred embodiment of the present invention, a carrier system for handling the payment process part of a commercial transaction between a customer, using a customer system and a mobile phone, and a merchant system.

in addition, a computer program product and a computer x>rogram element are provided that implement the methods according to the present invention.

The drawbacks of known systems and schemes are avoided by the schemes and systems as claimed in the attached claims. The present invention allows to implement a more secure marketplace for commercial transactions.

.... ~~l ..i i.

DESCRIPTION OF THE DRAWINGS

The invention is described in detail below with reference to the following schematic drawings. It is to be noted that the Figures are not drawn to scale.

FIG.1 is a schematic representation of a known electronic transaction scheme.

FIG. 2 is a schematic representation of a known electronic transaction scheme with pre-registration step.

FIG. 3 is a schematic representation of an electronic transaction scheme with pre-registration step, according to one embodiment of the present invention.

FIG. 4 is a schematic representation of another electronic transaction scheme, according to another embodiment of the present invention.

FIG. 5 is a schematic block diagram of an embodiment in accordance with the present invention.

FIG. 6 is a schematic block diagram of another embodiment in accordance with the present invention.

FIG. 7 is a schematic representation of the electronic transaction scheme underlying some of the embodiments of the present invention.

DESCRIPTION OF PREFERRED EMBODIMENTS:

The basic concept of the present invention is described after th.e basic terminology is defined.

Customer system: A customer system is a network-attachable device that has some computing capabilities. Examples are. personal computers (PCs), workstations, servers, laptops, personal digital assistants (PDAs), network computers, and so forth. Other examples are WAP phones, palm pilots, belt computers, pocket computers, wrist watches with integrated computer, electronic wallets, car computers, etc. The network connection is either established via some cable or fiber, or by means of an infrared or RF link. A customer system can also be an aggregation of several devices. This customer system is suited for operation by a customer desiring to obtain some service or to buy some goods via a network. The customer system may be a general purpose device especially programmed to perform the steps of the present invention, or a device equipped with appropriate software that controls the device to perform these steps. In addition, a customer system may comprise a database entertaining a list of transactions, a call-in unit that connects to a telephone network, and other devices or units.

Merchant system: A merchant system is a network-attachable system or aggregation of systems, which are employed by the merchant, or by somebody on behalf of the

Merchant system: A merchant system is a network-attachable, system or aggregation of systems, which are employed by the merchant, or by somebody on behalf of the merchant, in order to offer services and/or goods via a network. Such a merchant system has computing capabilities. A merchant system may comprise, for example: personal computers (PCs), workstations, laptops, network computers, servers, and so forth. In addition, a merchant system may comprise a database entertaining an electronic (online) catalog, a call-in unit that connects to a telephone network, and other devices or units. The merchant system is programmed to perform the steps of the present invention. For this purpose, the merchant system may be equipped with appropriate software that controls the system to perform these steps.

The word 'deliverable' is herein used as a synonym for goods, products, articles, items, subscriptions, services, etc. It subsumes everything - tangible as well as intangible - that either can be delivered (e.g., via a network or through conventional distribution channels, such as regular mail or courier), or that can be made accessible, such as a database, or some collection of digitized art. Examples are: effects, furnishings, furniture, gear, movables, possessions, property, commodities, merchandise, stock, stuff, wares, articles, subscriptions, newspapers, journals, printed media, equipment, softcopies, digitized images, videos, audio streams, software, currency, and so forth.

The word 'network' is herein used as a synonym for computer networks and communication networks of any kind. When referring to networks, wireless, fiber-based, or cable-based networks are meant.

A 'merchant' is a legal entity or person that directly or indirectly offers, sells, or lends one or more deliverables. Typical examples of merchants are: agents, dealers, suppliers, distributors, representatives, retailers, salespersons, shopkeepers; trad.espersons, vendors, warehouses, licensors, manufacturers, broker, bank, financial institutions, agency, and so forth.

A 'customer' is a legal entity or person that directly or indirectly wishes to accept, buy, lease, or borrow one or more deliverables. Typical examples are: buyers, clients, consumers, prospects, purchasers, shoppers, readers, subscribers, licensees.

The term "mobile phone" is used to subsume analog and digital phones that connect to a wireless channel. Examples are: handportables, GSM phones, cellular phones, Smartphones, Featurephones, transportables, satellite phones, and so forth.

The present invention changes the current network-based commercial schemes.

Instead of using a credit card, it is proposed to utilize the existing mobile phonf, network infrastructure to do order confirmation and billing.

Assuming an inventive scheme with pre-registration step (similar to the one of Figure 2), the customer provides the mobile phone number to the merchant in a registration step 28, as illustrated in Figure 3. The selection of deliverables) and the checkout steps remain more or less as they are. The result of the checkout process, however, changes, as illustrated in Figure 3 and as outlined below.

~ the customer accesses the merchant system through the customer system. The customer system is connected through a network (e.g., the Internet or world wide web) to the merchant system.

A browser may be used on the customer system in order to be able to access the merchant system.

~ the customer performs an action on the customer system in order to select the deliverables) (step 20 in Figure 3). There are different schemes known in the art that allow a customer to select a deliverables) online. The customer can, for example, select a deliverable from an electronic catalog by a mouse click, or by putting a deliverable into a shopping cart;

~ in an optional step, the customer invokes a checkout process (step 21 in Figure 3). This is usually done by clicking on a button to submit the order, ~or by having the customer confirm that the selection of deliverables was completed. No conventional checkout process is required if a single-action ordering scheme is implemented, as for example described and claimed in US patent 5,960,411. This US patent is incorporated by reference.

~ the merchant needs to obtain the phone number of the customer's mobile phone (step 22 in Figure 3). Since the mobile phone number has been registered with the merchant in a pre-registration step 28, the merchant system may fetch this phone number from a memory;

~ the merchant provides the customer with a confirmation address (e.g., a special confirmation phone number or a special confirmation e-mail address) by sending this confirmation address to the customer's mobile phone (step 23 in Figure 3).

~ the customer confirms the order by using the mobile phone and the confirmation address (step 24 in Figure 3). If the confirmation address is a special confirmation phone number, then the customer dials this confirmation phone number with the mobile phone.

Otherwise, the customer sends an e-mail from the mobile phone to the confirmation e-mail address.

~ the merchant monitors the incoming call indications ("caller ID") on the phone connection associated with the confirmation phone number or the incoming e-mails (step 25 in Figure 3).

The caller ID usually is the caller's mobile phone number and/or name. The merchant may keep a list of open transactions and the respective mobile phone numbers or e-mail addresses of the associated customers in a database. Once the customer's response (e.g., the customer's mobile phone number or name) is detected, the merchant considers the open transaction associated with the mobile phone to be successfully closed (;confirmed);

~ the merchant and/or mobile phone carrier triggers the charging of the amount due to the customer via the mobile phone carrier's billing system where the customer is uniquely identified through the mobile phone number (step 26 in Figure 3);

~ the merchant makes the deliverable available to the customer (step 27 in Figure 3)

A scheme, according to the present invention, without pre-registration is illustrated in Figure 4.

This scheme comprises the following steps:

~ the customer accesses the merchant system through the customer system and a network;

~ the customer performs an action on the customer system in order to select the deliverables) (step 30 in Figure 4);

~ in an optional step, the customer invokes a checkout process (step 31 in Figure 4). This is usually done by clicking on a button to submit the order, or by having the customer confirm that the selection of goods was completed;

~ the merchant needs to obtain the phone number of the customer's mobile phone (step 32 in Figure 4). Since in the present example the mobile phone number has not been registered with the merchant in a pre-registration step, the customer has to~ provide the merchant system with the phone number;

~ the merchant provides the customer with a confirmation address (e.g., a special confirmation phone number or a special confirmation e-mail address) by sending this confirmation address to the customer's mobile phone (step 33 in Figure 4).

~ the customer confirms the order by using the mobile phone and the confirmation address (step 34 in Figure 4). If the confirmation address is a special confirmation phone number, then the customer dials this confirmation phone number with the mobile phone.

Otherwise, the customer sends an e-mail from the mobile phone to the con:C~rmation e-mail address.

~ the merchant monitors the incoming call indications ("caller ID") on the phone connection associated with the confirmation phone number or the incoming e-mails (step 35 in Figure 4).

; ii

The merchant may keep a list of open transactions and the respective mobile phone numbers or e-mail addresses of the associated customers in a database. Once the customer's response (e.g., the customer's mobile phone number) is detected, the merchant considers the open transaction associated with the mobile phone to be successfully closed (confirmed);

~ the merchant and/or mobile phone carrier triggers the charging of the amount due to the customer via the mobile phone carrier's billing system where the customer is uniquely identified through the mobile phone number (step 36 in Figure 4);

~ the merchant makes the deliverable available to the customf,r (step 37 in Figure 4).

Another embodiment of the present invention is schematically depicted in Figure 5. This Figure gives an overview of the different parties and systems involved. The customer uses a customer system 40, such as a portable computer, that is connected to a network 44 (e.g., the Internet). The customer system 40 comprises a keyboard

91 and a display 1~2. in addition, the customer has a mobile phone 43 with a subscriber identity module (SIM) 54 card. A SIM card is a credit-card or mini sized card which holds a microprocessor chip which stores information such as the mobile phone number. The SIM card 54 can be inserted into the mobile phone 54 to make it live, as indicated by arrows in Figure 5.

The mobile phone 43, after being activated, connects via a mobile telephone network 53 (e.g., a GSM network) and to a fixed telephone network 56 (e.g., a public switched telephone network.

PSTN) and a carrier system 48. The mobile telephone network 53 and the fixed telephone network 56 are arranged such that the fixed telephone network 56 can be reached from the mobile phone 43. In other words, the mobile phone 43 has access to the services offered by the fixed telephone network 56. For sake of simplicity, the carrier system 48 just comprises a server 49 and a printer 50.

In the present example, the merchant system 45 comprises a server 46, a database 47 with an online catalog, and a database 58 with a list of open transactions. The merchant system 45 is linked to the network 44. Furthermore, the merchant system 45 in the present embodiment has a call-in unit 55 that is connected to the fixed telephone network 56. Note that the call-in unit 55 might also be connected to the mobile network directly.

The customer accesses the merchant system 45 through the customer system 40 and the network 44. The merchant system 45 offers an online catalog with various items together with a price for each item. In the present example, the deliverable 41 is displayed on the display of the customer system 40. The customer now performs an action on the customer system 40 in order to select the deliverable 41. This can be done by a left-mouse-click on the radio button 42 that is also displayed. If this is the only deliverable the customer wants to obtain, or if there are no other deliverables available, the selection process may be finished. The merchant system 45 may thus proceed to an order confirmation process. In an optional step, the customer may invoke a checkout process prior to the confirmation process. This is usually done by clicking on a button to submit the order, or by having the customer confirm that the selection of deliverables was completed.

According to the present invention, the merchant system 45 needs to obtain the phone number of the customer's mobile phone 43. If the mobile phone number has been registered with the merchant system 45 in a pre-registration step, the merchant system 45 can fetch this phone number from a memory inside the server 46, for example. If no mobile phone number has been pre-registered, the customer needs to provide this number to the merchant system 45. This can be done via the customer system 44 or via the mobile phone 43.

The merchant system 45 provides the customer with a confirmation address. In the present example, this confirmation address is a special call-in phone number provided by the merchant system 45. For this purpose, the merchant system 45 has a call-in unit 55 that is connected to the fixed telephone network 56. The customer confirms the order by dialing this special call-in number with the mobile phone 43. A connection is established from the mobile phone 43 via a wireless channel to a base station. The base station feeds the call into the fixed telephone network 56. The server 46 monitors the incoming call indications ("caller ID"). The merchant system 45 keeps a list of open transactions and the respective mobile phone numbers of the associated customers in database 58. The server 46 compares the customer's response (received from the call-in unit 55 via link 59) with the entries in the database 58.

Once the customer's response (e.g., the customer's caller ID) is matched with an entry in the database 58, the merchant system 45 considers the open transaction associated with the mobile phone 43 to be successfully closed (confirmed). The merchant system 45 triggers the charging of the amount due to the customer via the mobile phone carrier's billing system where the customer is uniquely identified through the mobile phone number. For this purpose, the server 46 may connect to the server 49, e.g., via a leased line 57. The carrier system 48 comprises a printer 50 that is controlled by a billing software residing on the server 49. The billing software sends a print job to the printer 50 to generate a bill 51. This bill 51 is sent to the customer by regular mail, as schematically depicted by the arrow 52. One has many different options as the when and how to create the bill. The billing software may comprise an accrual module which collects all items that need to be bill on a per-customer basis. At the end of an accounting period, e.g. at the end of each month, the bill may be created, printed, and send to the customer. This approach is acceptable if the deliverables are not too expensive. For more expensive deliverables, it is appropriate to issue a bill right away. Delivery of the deliverable may even be conditioned on the payment of the bill

The carrier may also subcontract/outsource the bill handling procedures to a trusted party. The present scheme remains more or less the same, except for the fact that the necessary information needs to be forwarded to the respective trusted party.

Payment of open bills can be accepted via bank account, credit card, cash, check, and wire transfer. The carrier and/or merchant can specify a credit limit for some or all of their customers.

After the bill 51 was issued, or after the bill 51 was issued and the amount paid by the customer, the merchant system 45 makes the deliverable 41 available to the customer.

Depending on the kind of deliverable, there are many different ways to actually do this. If the deliverable is a tangible item, then it is prepared for shipment and delivered to the customer by mail of courier.

Likewise, the customer may pick it up. When the deliverable is an intangible item, the server 46 may simply make it available for download by the customer system 40 (pull approach), or the server 46 may send it to the customer system 40 (push approach).

The merchant system 45 and/or the carrier system 48 may comprise hardware modules, software modules or hardware and software modules that perform the various steps of the present scheme.

According to the above described embodiments, the carrier system handled the payment process mainly. In another embodiment of the present invention, the carrier system can also carry out certain of the transaction closure steps. For this purpose, the merchant system may forward the details of an open transaction to the carrier system. The carrier closes the transaction with the customer as described above. In this case, the carrier system needs a special call-in number and a call-in unit that is able to monitor incoming calls. When the customer calls this call-in number, the call-in unit recognizes the caller ID and notifies the carrier system's server. The open transactions are stored in a database in the carrier system. The server compares the caller ID with the entries in this database to complete a transaction. If the server is able to match the caller ID

with an entry in the database, the customer's order is deemed to be completed and the payment process is initiated. As part of this payment process, the carrier directly charges the amount due to the customer's phone bill. The carrier system also notifies the merchant system of the successful completion of the transaction and credits the merchant's account with the amount due.

The merchant makes the deliverables) available to the customer.

Several extensions to these embodiments are possible.

Instead of providing the confirmation call-in number to the customer, the merchant (or carrier) can send a GSM short message service (SMS) message to the customer system containing an order ID (which~is displayed to the customer on the customer system's screen or on the mobile phone display) and the confirmation phone number to dial. T he SMS is the ability to send and receive text messages to and from mobile phones. The text can comprise of words or numbers or an alphanumeric combination.

The customer can then match the order ID contained in the GSM SMS received to the order ID

displayed. Using the GSM phone's SMS number extraction feature, for example, the customer can confirm the order by calling the merchant or carrier from the GSM phone.

Another alternative is that the merchant system transmits (as part of the checkout process) a Web page containing a checkout applet that can communicate locally with the customer's mobile phone (for example, using the Bluetooth protocol). The customer would confirm the order through the applet and the applet causes the mobile phone to prepare the confirmation call. The customer would then just have to initiate the call.

Instead of doing a confirmation call, the customer could send a GSM SMS or an e-mail to the merchant system.

Yet another embodiment is illustrated in Figure 6. The customer uses a customer system 70, such as a personal computer with a touch screen 93, that is connected to a network 74 (e.g., the world wide web). In addition, the customer has a mobile phone 73 with a SIM card 74.

network 74 (e.g., the World Wide Web). In addition, the customer has a mobile phone 73 with a SIM card 74.

The mobile phone 73 connects via a mobile telephone network 83 (e.g., a GSM network) and to a fixed telephone network 86 (e.g., a PSTN) and a carrier system 78. The mobile telephone network 83 and the fixed telephone network 86 are arranged such that the fixed telephone network 86 can be reached from the mobile phone 73. For sake of simplicity, the carrier system 78 just comprises a server 79, a database 88, and a billing module 80. Furthermore, the carrier system 78 in the present embodiment is connected via a link 89 to a call-in unit, 85 that is connected to the mobile telephone network 83.

In the present example, the merchant system 75 comprises a~ server 76, a database 77 with an online catalog. The merchant system 75 is linked to the network 74 (e.g., via a modem). The customer accesses the merchant system 75 through the custonner system 70 and the network 74.

The merchant system 75 offers an online catalog with various items together with a price for each item. In the present example, the deliverable 71 is displayed on the display 93 of the customer system 70. 'The customer now performs an action on the customer system 70 in order to select the deliverable 71. This can be done by touching the radio button 72 that is also displayed on the touch screen 93. If this is the only deliverable the customer wants to obtain, or if there are no other deliverables available, the selection process may be finished. An order confirmation process may thus follow. In an optional step, the customer may invoke a checkout process prior i~

to the confirmation process. This is usually done by clicking on a button to submit the order, or by having the customer confirm that the selection of deliverables was completed.

According to the present invention, the carrier system 78 needs to obtain the phone number of the customer's mobile phone 73. If the mobile phone number has been registered with the merchant system 75 and/or the Garner system 78 in a pre-registration step, the carrier system 78 can fetch this phone number from a memory inside the server 76 or 79, for example. If no mobile phone number has been pre-registered, the customer needs to provide this number to the merchant system 75 or Garner system 78. This can be done vi<~ the customer system 70 or via the mobile phone 73.

The merchant system 75 forwards the details of an open transaction, e.g., the order identifier (order ID) and a unique transaction number, to the carrier system 78. For this purpose, the merchant system 75 assigns an order ID for each deliverable 71 or set of deliverables ordered a particular customer. This information can be exchanged via a dedicated line 87, for example.

Likewise, the carrier system 78 can be linked via the network 74 to the merchant system 75. The carrier system 78 keeps a list of open transactions and the respective mobile phone numbers of the associated customers in database 88. The server 79 compares the customer's response (received from the call-in unit 85 via link 89) with the entries in the database 88. Once the customer's response (e.g., the customer's caller ID and/or the order ID) is matched with an entry in the database 88, the carrier system 78 considers the opi,n transaction associated with the mobile phone 73 to be successfully closed (confirmed). The .carrier system 78 needs to provide the customer with a confirmation address. In the present example, this confirmation address is a special call-in phone number (e.g., a special GSM service number). The carrier system 78 generates a GSM SMS message with the order ID and a unique transaction number.

This SMS is send to the customer's mobile phone 73. The customer receives this SMS on the mobile phone 73. The customer then returns the received SMS message to the special call-in phone number provided that he wants to complete the ordering process he initiated for the deliverable 71. Once the SMS message is received by the carrier system 78 via call-in unit 85 and the link 89, the closeout of the transaction is deemed to be completed and the payment process is initiated using a billing module 80. In the present example, the billing module 80 generates a so-called online-bill 81. This bill is not printed and delivered through a conventional mail system. It is delivered to the customer as an electronic document, preferat>ly in an encrypted fashion. In the present embodiment, the online-bill 81 is delivered via a link 82 and the network 74 to the customer's system 70. The customer can pay the bill using an online-banking software, for example. All this can be done within minutes or even seconds. The remainder is the same as above.

The above embodiments can be modified by implementing a, housekeeping process that checks the database for transactions that are older than a pre-defined expiry age. In Figure 6 this is schematically illustrated by the symbol 90. In this example, the housekeeping process goes through the database 88 to find entries that have expired. These entries are then flushed/removed.

This allows to remove open transactions that have not been confirmed by the customer within a predefined period of time. The expiry time can be anything between seconds, hours and even days. The housekeeping process avoids the database to be filled up and it provides for additional security because any open transaction might be misused if somebody manages to break into the carrier's system.

The merchant system 75 and/or the carrier system 78 may comprise hardware modules, software modules or hardware and software modules that perform the various steps of the present scheme.

Extending the previous embodiment, the customer can send the GSM SMS message received from the carrier to another special service number to abort the transaction. For this purpose, the carrier may entertain two special service numbers: one for transaction confirmation, the other for transaction abort.

According to another embodiment, the carrier or merchant system may send a GSM
SMS
message with a "receipt" to the customer's mobile phone once the transaction has been successfully concluded. The customer can store this "receipt" <~way.

Another improvement would be to send a GSM SMS to the customer's mobile phone with details about the bill. This gives the customer to review what he just has order, together with the price and probably the mode and terms of payment.

It is also possible to send a GSM SMS to the customer once the delivery process has been initiated or completed. If the deliverable is some online content, e.g., an online document, then the customer could receive a user ID and password via a GSM SMS.

Another embodiment is conceivable where the customer's GSM SIM card is employed to provide for a transaction scheme that is very convenient. In this embodiment, a SIM card is employed that contains a specific SIM application. The merchant system or the carrier system (depending on which embodiment of the invention is implemented) sends a special GSM SMS
message containing order details (e.g., a special call-in number and/or an order ID) to the customer's mobile phone. The customer's SIM card sits in the phone and intercepts this SMS
message, extracts the order details from the SMS message, and interactively obtains the customer's consent to the order process. This can be done using the keypad and screen of the GSM phone, for example. In case the customer confirms the order, the SIM card automatically sends off a GSM SMS message to either the merchant system or the carrier (or it initiates the confirmation call).

Another variation on the previously described embodiments i.s possible if one uses the wireless application protocol (WAP). Instead of using a SIM application, as described in the last paragraph, the merchant system may use the push feature of WAP to push a wireless markup language (WML) deck (script applet) to the customer's WAf-enabled GSM phone.

This WML
applet contains the order ID and asks the customer to confirm the order.

in yet another embodiment, the merchant system forwards the details of an open transaction to a third-party company that specializes in transaction capturing. The customer is registered with that company and provided it with the credit card details (or account details for direct debit or something similar).

CH9-2000-0021 I g The preferred implementation of the present invention is the case where the merchant system transfers an open transaction to a GSM carrier. The GSM: carrier then sends a GSM SMS
message, containing the merchant's order ID and a unique transaction ID, to the customer's GSM
phone. The customer confirms the order by sending the SMS message on to a special service number entertained by the GSM carrier. The GSM carrier charges the amount due to the customer's phone bill, notifies the merchant of the customer's confirmation, and credits the merchant's account with the amount due.

The authentication of customers is an interesting issue that needs to be considered in light of the present invention. The present schemes are based on the assumption

that there is one customer per mobile phone, namely the owner. In other words, it is not envisaged to "share" a mobile phone with another person since this would give the other person the opportunity to order deliverables on behalf of the owner

A logical improvement which rectifies this weakness is described below in form of another embodiment.

According to another embodiment, protection against misuse is obtained by requiring the user of a mobile phone to type in a short PIN before the phone be used. This PIN may be combined with the key stored in the mobile phone to form a composite key, which could be used for authentication. Such an embodiment can be designed around a SIM card which offers a mechanism for authentication via a PIN. This PIN is required as authorization before or while using a mobile phone in connection with the present transaction schemes. This inhibits unauthorized usage of the mobile phone.

Those skilled in the art will understand that the systems illustrated in Figures 5 and 6 are examples of systems implementing the present invention and that the configuration and construction of the various elements of the systems may use well-known hardware and/or software. Those skilled in the art will recognize that many modifications and changes can be made to the particular embodiments described herein above without departing from the spirit and scope of the invention.

In Figure 7 a simplified representation of the scheme, according to the present invention, is given. In this graphical representation the order confirmation process is assumed to be part of the payment process. Figure 7 is a generalized representation of a transaction scheme, according to the present invention, where the customer 60, merchant 61, and carrier 62 interact with each other. The ellipse 63 indicates that the customer 60 and merchant 61 interaction concentrates on the ordering process and the delivery process. The payment process is between the customer 60 and carrier 62 (ellipse 64) on one hand, and between the carrier 62 and merchant 61 on the other hand (ellipse 65).

In the present example, the ordering process (ellipse 63), comprises the following activities/actions: (1) the customer 60 contacts the merchant 61 through the customer system and a network; (2) the customer 60 performs an action on the customer system in order to select the deliverable(s); (3) in an optional step, the customer 60 invokes a checkout process. (4) the merchant 61 obtains the phone number of the customer's mobile phone; and (5) the merchant 61 or carrier 62 provides the customer 60 with a confirmation address (e.g., a special phone call-in number).

The payment process (ellipse 64), comprises the following activities/actions:

(1) the customer 60 confirms the order by using the mobile phone and the confirmation address; (2) the carrier 62 monitors the incoming call indications ("caller ID") on a phone line associated with the confirmation phone number or the incoming e-mails (note that this is a variation of the scheme presented in Figures 4 and 5 where the merchant system monitors incoming calls). The carrier 62 may receive a list of open transactions and the respective mobile phone numbers or e-mail addresses of the associated customers from the merchant 61. This information is kept by the Garner 62 in a database; (3) the carrier 62 triggers the charging of the amount due to the customer 60 via the carrier's billing system.

The payment process (ellipse 65), comprises the following activities/actions:

(1) the carrier 62 notifies the merchant 61 of the successful transaction and credits the merchant's account with the amount due.

The delivery process (ellipse 63), comprises the following activities/actions:

(1) the merchant 61 makes the deliverable available to the customer 60.

With the mobile phone a security token is introduced. A mobile phone (such as a GSM phone) can be PIN-protected (personal identification number) by its owner. Each mobile phone is thus uniquely identified and its owner is known (the exception being customers using prepaid SIM cards for their GSM phones). The customer already has a contractual relationship with a carrier for billing purposes. There are billing standards (e.g., the TAf3 standard introduced by the GSM Association) that are continually extended and enhanced. In contrast to the current model of payment over the Internet - transmitting ones credit card details to the merchant, who then can in the worst case misuse the credit card data - with the present invention in its various implementations the customer is in control of the payment process again as he has to give consent for each and every payment. Furthermore, the customer is dealing with an organization he is already familiar with (the carrier) and which serves as a neutral third party (in most cases).

The merchant on the other hand deals with a known organization as well (again, the carrier) and can rely on the customer being verified and probably even having a certain credit limit granted by the carrier.

Since the payment process is done via a secure and well established channel between the customer and the carrier, there is no need for encryption of the transactions and exchange of information between the customer system and the merchant system. This allows to simplify many of today's transaction schemes.

A GSM-based scheme has the advantage over other mobile telephone systems that the data transmission between the transmitters and the GSM units is encrypted. Without encryption, eavesdropping is very simple in a wireless network (e.g., previous analog mobile phone systems).

Mobile telephone networks are implemented by a number of different carriers.

Each carrier has it's own customers, in respect of whom the carrier holds private information relating to names, addresses, billing information, methods of paying bills, etc. Thus, a distinction should be made in connection with the herein described transaction schemes between the information which the carrier shares with the merchant system or other parties involved, and the information which is generally private as between the customer, and the carrier.

Carriers have two methods to differentiate themselves in the marketplace;

selling basic telephone services at a lower price point, or by providing new (probably fee-based) services that are viewed as added value by their customers. The present invention is a good example for such a service that can be offered by a carrier. Consumers and businesses want 'easy to understand and use' products that satisfy their complex needs and are easily accessible. The growth of the Internet and the new commercial transaction schemes presented herein are good examples of these market forces at work.

Note, that the invention is not restricted to Internet payment schemes. It can essentially be used for every process where a confirmed and authenticated transaction is required.

The individual steps of the processes described herein and listed in the attached claims not necessarily have to be carried out in the given order.

The present invention can be realized in hardware, software, or a combination of hardware and software. Any kind of computer system or other apparatus adapted for carrying out the methods described herein is suited. A typical combination of hardware and software could be a general purpose computer system with a computer program that, when being loaded and executed, controls the computer system such that it carries out the methods described herein. The present invention can also be embedded in a computer program product, which comprises all the features enabling the implementation of the methods described herein, and which - when loaded in a computer system - is able to carry out these methods.

Patent Citations (5)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US6883091B1 *	1997-04-15	2005-03-15	Telefonaktiebolaget Lm Ericsson (Publ)	Tele/datacommunications payment method and apparatus
AU780943B2 *	1999-12-30	2005-04-28	International Business Machines	Method of payment by means of an electronic communication device

			Corporation	
FI112286B *	2000-01-24	2003-11-14	Smarttrust Systems Oy	Payment service apparatus and secure payment procedure
US20010037254A1 *	2000-03-09	2001-11-01	Adi Glikman	System and method for assisting a customer in purchasing a commodity using a mobile device
US20030164400A1 *	2000-04-18	2003-09-04	Boyd Leslie Fergus	Method of operating a ticketing system

* Cited by examiner, † Cited by third party

Cited By (175)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
EP1323140B1 *	2000-08-28	2006-09-06	Axalto S.A.	Method for providing identification data of a banking card to a user
JP2002203189A *	2000-12-28	2002-07-19	Ntt Docomo Inc	Method and system for processing payment
US6968174B1	2001-03-22	2005-11-22	Callwave, Inc.	Call routing apparatus
US20020198790A1 *	2001-06-26	2002-12-26	Paulo Daniel Leonard	Method and system for ordering goods or services
SE523979C2 *	2001-07-02	2004-06-08	Telia Ab	Mobile electronic commerce system and procedure
KR100831985B1 *	2001-07-10	2008-05-23	삼성전자주식회사	Apparatus of managing SMS messages for HHP and method thereof
US8737959B2	2001-08-21	2014-05-27	Bookit Oy Ajanvarauspalvelu	Managing recurring payments from mobile terminals
US8666380B2	2001-08-21	2014-03-04	Bookit Oy Ajanvarauspalvelu	Communication method and system
US11004114B2	2001-08-21	2021-05-11	Bookit Oy	Components, system, platform and methodologies for mediating and provisioning services and product delivery and orchestrating, mediating and authenticating transactions and interactions
US10929784B2	2001-08-21	2021-02-23	Bookit Oy	Booking method and system
FI20011680A	2001-08-21	2003-02-22	Bookit Oy	Appointment method and system
US9406062B2 *	2001-08-21	2016-08-02	Bookit Oy Ajanvarauspalvelu	Authentication method and system
US9171307B2	2002-08-21	2015-10-27	Bookit Oy Ajanvarauspalvelu	Using successive levels of authentication in online commerce
US9501775B2	2009-03-10	2016-11-22	Bookit Oy Ajanvarauspalvelu	Managing recurring payments from mobile terminals
US9807614B2	2001-08-21	2017-10-31	Bookit Oy Ajanvarauspalvelu	Using successive levels of authentication in online commerce
US9418361B2	2001-08-21	2016-08-16	Bookit Oy Ajanvarauspalvelu	Managing recurring payments from mobile terminals
US10902491B2	2001-08-21	2021-01-26	Bookit Oy	Product/service reservation and delivery facilitation with semantic analysis enabled dialog assistance
US8737954B2	2001-08-21	2014-05-27	Bookit Oy Ajanvarauspalvelu	Managing recurring payments from mobile terminals
US10469591B2	2001-08-21	2019-11-05	Bookit Oy	Method and system for mediating and provisioning services
US9288315B2	2001-08-21	2016-03-15	Bookit Oy Ajanvarauspalvelu	Method and system for mediating and provisioning services
US8737955B2	2001-08-21	2014-05-27	Bookit Oy Ajanvarauspalvelu	Managing recurring payments from mobile terminals
US9578022B2	2001-08-21	2017-02-21	Bookit Oy Ajanvarauspalvelu	Multi-factor authentication techniques
US9406032B2	2001-08-21	2016-08-02	Bookit Oy Ajanvarauspalvelu	Financial fraud prevention method and system
US8737958B2	2001-08-21	2014-05-27	Bookit Oy Ajanvarauspalvelu	Managing recurring payments from mobile terminals
SG101509A1 *	2001-09-12	2004-01-30	Sin Etke Technology	On-board wireless transaction system and method

			Co Ltd	
MXPA04002541A	2001-09-24	2004-05-31	E2Interactive Inc	System and method for supplying communication service.
US20030069827A1 *	2001-10-04	2003-04-10	Koninklijke Philips Electronics N.V.	Ticket exchange system and method of operation
US20030093545A1 *	2001-11-14	2003-05-15	Inventec Tomorrow Work Studio Corporation, Taiwan	Method and system for downloading data to portable electronic device
JP2004005425A *	2002-02-08	2004-01-08	Mobusutaazu:Kk	Settlement method by various paying means using subscriber terminal machine for mobile communication
GB2387002A *	2002-02-20	2003-10-01	1Revolution Group Plc	Personal identification system and method using a mobile device
US7110987B2 *	2002-02-22	2006-09-19	At&T Wireless Services, Inc.	Secure online purchasing
US7007008B2 *	2002-02-22	2006-02-28	At&T Wireless Services, Inc.	Secure online purchasing
JP2004046286A *	2002-02-25	2004-02-12	Hiroshi Tatsuke	Charging method, program and information system
CA2479219A1 *	2002-03-22	2003-10-02	British Telecommunications Public Limited Company	Transaction authentication
TW561770B *	2002-04-18	2003-11-11	Benq Corp	Method for transforming personalized bills information of a mobile station user with short message service
WO2003094128A1 *	2002-04-30	2003-11-13	Saj Muzaffar	Payment system
US7266347B2	2002-05-24	2007-08-28	Cingular Wireless Ii, Llc	Biometric authentication of a wireless device user
US20040019564A1 *	2002-07-26	2004-01-29	Scott Goldthwaite	System and method for payment transaction authentication
US7792759B2	2002-07-29	2010-09-07	Emv Co. Llc	Methods for performing transactions in a wireless environment
US20040127256A1 *	2002-07-30	2004-07-01	Scott Goldthwaite	Mobile device equipped with a contactless smart card reader/writer
US7353382B2 *	2002-08-08	2008-04-01	Fujitsu Limited	Security framework and protocol for universal pervasive transactions
US7784684B2 *	2002-08-08	2010-08-31	Fujitsu Limited	Wireless computer wallet for physical point of sale (POS) transactions
US7801826B2 *	2002-08-08	2010-09-21	Fujitsu Limited	Framework and system for purchasing of goods and services
US7606560B2	2002-08-08	2009-10-20	Fujitsu Limited	Authentication services using mobile device
US7349871B2 *	2002-08-08	2008-03-25	Fujitsu Limited	Methods for purchasing of goods and services
US7822688B2	2002-08-08	2010-10-26	Fujitsu Limited	Wireless wallet
JP4511459B2 *	2002-10-17	2010-07-28	ヴォウダフォン・グループ・ピーエルシー	Facilitating and authenticating transactions
US7478057B2 *	2002-11-29	2009-01-13	Research In Motion Limited	Method for conducting an electronic commercial transaction
US20040141601A1 *	2003-01-22	2004-07-22	Yigang Cai	Credit reservation transactions in a prepaid electronic commerce system
US7382277B2 *	2003-02-12	2008-06-03	Edward D. Ioli Trust	System for tracking suspicious vehicular activity
US7996268B2 *	2003-03-03	2011-08-09	Poltorak Alexander I	Apparatus and method for an electronic telephone wallet
US7460653B2	2003-03-07	2008-12-02	Callwave, Inc.	Apparatus and methods for telecommunication authentication
US7321920B2	2003-03-21	2008-01-22	Vocel, Inc.	Interactive messaging system
AU2003235987A1 *	2003-05-14	2004-12-03	Cellmax Systems Ltd.	E-commerce transactions over a telecommunications device
JP4335874B2 *	2003-06-18	2009-09-30	テレフオンアクチーボラゲットエルエムエリクソン（パブル）	Online billing in mobile networks
WO2005024690A1 *	2003-09-08	2005-03-17	Jong-Do Park	Service system for free using of mobile contents

US20050060250A1 *	2003-09-17	2005-03-17	Mobile (R&D) Ltd.	Billing and ordering system and method for services provided over communications networks
DE10343566A1 *	2003-09-19	2005-05-04	Brunet Holding Ag	Process for processing an electronic transaction
KR100648064B1 *	2004-01-14	2006-11-23	주식회사 케이티프리텔	mobile terminal for certification, E-commerce system and method using the terminal
US7877605B2	2004-02-06	2011-01-25	Fujitsu Limited	Opinion registering application for a universal pervasive transaction framework
US8468093B2 *	2004-03-25	2013-06-18	International Business Machines Corporation	Method and system for performing a commercial transaction by using a short message service terminal
US20050222913A1 *	2004-04-01	2005-10-06	Ian Eisenberg	PR/SMS business method, system and method of conducting business
KR100629499B1 *	2004-05-22	2006-09-28	삼성전자주식회사	Method for charging for printing
JP2006012020A *	2004-06-29	2006-01-12	Aimnet Co Ltd	Order confirmation system and method using message serial number, and online result authentication method for transaction result using it
DE102004041356B4 *	2004-08-25	2006-12-07	Claudia Von Heesen	Method and system for the secure processing of electronic financial services using an electronic financial services intermediary
US20060047572A1 *	2004-08-26	2006-03-02	Jeffery Moore	Text and multimedia messaging-based layered service and contact method, auction method and method of conducting business
US20060064391A1 *	2004-09-20	2006-03-23	Andrew Petrov	System and method for a secure transaction module
US7581678B2 *	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
US20060258397A1 *	2005-05-10	2006-11-16	Kaplan Mark M	Integrated mobile application server and communication gateway
US8855107B1	2005-07-01	2014-10-07	Callwave Communications, Llc	Methods and systems for call routing via a telephone number
US8447700B2	2005-10-11	2013-05-21	Amazon Technologies, Inc.	Transaction authorization service
US8352376B2	2005-10-11	2013-01-08	Amazon Technologies, Inc.	System and method for authorization of transactions
US20070123219A1 *	2005-10-19	2007-05-31	Mobile 365, Inc.	System and method for item identification and purchase
US20070107017A1 *	2005-11-04	2007-05-10	Angel Albert J	Transaction Process Controller with User History, Selectable Profile Controls, Confirmation and User Control Options for Shopping with Video On Demand Cable Systems
FI117663B	2005-12-02	2006-12-29	Bookit Oy Ajanvarauspalvelu	Message sending method for telecommunication network, involves converting reply address information to correspond to dialogue so that message transmission and reception are implemented in different parts of telecommunication system
JP2007200144A *	2006-01-27	2007-08-09	Shigeto Mochizuki	Card use system, card use method, and unauthorized use determination device for card use system
US8662384B2 *	2006-02-28	2014-03-04	Google Inc	Text message payment
US20070228147A1 *	2006-03-30	2007-10-04	Reporo Limited	Application generation system, method and machine readable medium
FI119168B	2006-04-21	2008-08-15	Jukka Tapio Aula	SMS delivery method and system for queries and invitations
FI118858B	2006-05-02	2007-12-31	Bookit Oy Ajanvarauspalvelu	Procedure and system for combining text and audio messages in a communication dialogue
FI118586B	2006-05-02	2007-12-31	Bookit Oy Ajanvarauspalvelu	Procedure and system for combining text and audio messages in a communication dialogue
BRPI0604416A *	2006-09-27	2007-12-04	Paggo Participacoes S A	system that manages and facilitates transactions of a financial nature performed locally or remotely
US8548447B1	2006-10-06	2013-10-01	Callwave Communications, Llc	Methods and systems for blocking unwanted telecommunications
WO2008080173A2 *	2006-12-24	2008-07-03	Joseph Leo Moreno	Systems and methods for mobile payment
US8935187B2 *	2007-03-07	2015-01-13	Playspan, Inc.	Distributed payment system and method
US8620260B2	2007-04-27	2013-12-31	American Express Travel Related Services Company, Inc.	Payment application download to mobile phone and phone personalization
US20080270301A1 *	2007-04-27	2008-10-30	American Express Travel Related	Mobile payment system and method

			Services Co., inc.	
US8688570B2 *	2007-04-27	2014-04-01	American Express Travel Related Services Company, Inc.	System and method for performing person-to-person funds transfers via wireless communications
US8543496B2 *	2007-04-27	2013-09-24	American Express Travel Related Services Company, Inc.	User experience on mobile phone
US20080299970A1	2007-05-30	2008-12-04	Shoptext, Inc.	Consumer Registration Via Mobile Device
US8768778B2 *	2007-06-29	2014-07-01	Boku, Inc.	Effecting an electronic payment
US8239326B1	2007-09-19	2012-08-07	Amazon Technologies, Inc.	Method and apparatus for authorizing transactions using transaction phrases in a transaction authorization service
US7729989B1	2007-09-19	2010-06-01	Amazon Technologies, Inc.	Method and apparatus for message correction in a transaction authorization service
US20090112767A1 *	2007-10-25	2009-04-30	Ayman Hammad	Escrow system and method
US20090164371A1 *	2007-11-20	2009-06-25	M Commerce Data Systems, Inc.	Mobile Financial Transaction Method
US7958059B2	2007-12-31	2011-06-07	Mastercard International Incorporated	Methods and systems for cardholder initiated transactions
US8577804B1 *	2008-02-20	2013-11-05	Collective Dynamics LLC	Method and system for securing payment transactions
US9852426B2	2008-02-20	2017-12-26	Collective Dynamics LLC	Method and system for secure transactions
US8620826B2	2008-03-27	2013-12-31	Amazon Technologies, Inc.	System and method for receiving requests for tasks from unregistered devices
US8204827B1	2008-03-27	2012-06-19	Amazon Technologies, Inc.	System and method for personalized commands
US8244592B2	2008-03-27	2012-08-14	Amazon Technologies, Inc.	System and method for message-based purchasing
US20090248533A1 *	2008-03-31	2009-10-01	Txttunes Limited	Systems and methods for conducting transactions
US8837465B2	2008-04-02	2014-09-16	Twilio, Inc.	System and method for processing telephony sessions
AU2009231676B2	2008-04-02	2013-10-03	Twilio Inc.	System and method for processing telephony sessions
FR2930664A1 *	2008-04-24	2009-10-30	Netsize Sa	METHOD AND SYSTEM FOR TRANSACTING GOODS AND / OR SERVICES USING A TERMINAL VIA A COMMUNICATION NETWORK
EP2294539A1 *	2008-05-16	2011-03-16	Google Inc.	Secured electronic transaction system
CA2725312A1 *	2008-05-23	2009-11-26	Boku	Supplier funds reception electronically
GB0809381D0 *	2008-05-23	2008-07-02	Vidicom Ltd	Funds transfer electronically
GB0809386D0 *	2008-05-23	2008-07-02	Vidicom Ltd	Transferring funds electronically
GB0809382D0 *	2008-05-23	2008-07-02	Vidicom Ltd	Funds transfer electronically
GB0809383D0 *	2008-05-23	2008-07-02	Vidicom Ltd	Customer to supplier funds transfer
FI124899B	2008-07-04	2015-03-13	Bookit Oy Ajanvarauspalvelu	Method and system for sending messages
WO2010001423A1 *	2008-07-04	2010-01-07	Ooros S.R.L.	Method and system for managing financial transactions
RU2388058C1 *	2008-11-06	2010-04-27	Александр Геннадьевич Рокков	Transaction verification method, automatic transaction verification system and transaction verification unit (versions)
US20100131415A1 *	2008-11-24	2010-05-27	Research In Motion Limited	Electronic payment system including merchant server and associated methods
KR20100063846A *	2008-11-28	2010-06-14	엘지전자 주식회사	Mobile terminal and method for purchasing broadcast product thereof
US8116730B2 *	2009-01-23	2012-02-14	Vidicom Limited	Systems and methods to control online transactions
US8041639B2 *	2009-01-23	2011-10-18	Vidicom Limited	Systems and methods to facilitate online transactions

US9652761B2	2009-01-23	2017-05-16	Boku, Inc.	Systems and methods to facilitate electronic payments
US8548426B2 *	2009-02-20	2013-10-01	Boku, Inc.	Systems and methods to approve electronic payments
US9990623B2	2009-03-02	2018-06-05	Boku, Inc.	Systems and methods to provide information
EP2226997B1 *	2009-03-06	2020-09-09	Vodafone Holding GmbH	Billing mechanism for a mobile communication network
US9937531B2	2009-03-10	2018-04-10	Bookit Oy Ajanvarauspalvelu	Method and system for delivery of goods
US8700530B2	2009-03-10	2014-04-15	Boku, Inc.	Systems and methods to process user initiated transactions
US8160943B2 *	2009-03-27	2012-04-17	Boku, Inc.	Systems and methods to process transactions based on social networking
US8131258B2 *	2009-04-20	2012-03-06	Boku, Inc.	Systems and methods to process transaction requests
US8224727B2	2009-05-27	2012-07-17	Boku, Inc.	Systems and methods to process transactions based on social networking
US9595028B2 *	2009-06-08	2017-03-14	Boku, Inc.	Systems and methods to add funds to an account via a mobile communication device
US9697510B2	2009-07-23	2017-07-04	Boku, Inc.	Systems and methods to facilitate retail transactions
US9519892B2 *	2009-08-04	2016-12-13	Boku, Inc.	Systems and methods to accelerate transactions
US8713647B2 *	2009-08-21	2014-04-29	International Business Machines Corporation	End-of-session authentication
US8660911B2	2009-09-23	2014-02-25	Boku, Inc.	Systems and methods to facilitate online transactions
US8224709B2	2009-10-01	2012-07-17	Boku, Inc.	Systems and methods for pre-defined purchases on a mobile communication device
US8412626B2 *	2009-12-10	2013-04-02	Boku, Inc.	Systems and methods to secure transactions via mobile devices
US8566188B2	2010-01-13	2013-10-22	Boku, Inc.	Systems and methods to route messages to facilitate online transactions
SI23227A	2010-03-10	2011-05-31	Margento R&D D.O.O.	Wireless mobile transaction system and procedure of carrying out transaction with mobile telephone
US8219542B2	2010-03-25	2012-07-10	Boku, Inc.	Systems and methods to provide access control via mobile phones
US8583504B2 *	2010-03-29	2013-11-12	Boku, Inc.	Systems and methods to provide offers on mobile devices
US8355987B2	2010-05-06	2013-01-15	Boku, Inc.	Systems and methods to manage information
US10068287B2	2010-06-11	2018-09-04	David A. Nelsen	Systems and methods to manage and control use of a virtual card
US8589290B2	2010-08-11	2013-11-19	Boku, Inc.	Systems and methods to identify carrier information for transmission of billing messages
US9805348B2	2010-09-22	2017-10-31	Mastercard International Incorporated	Methods and systems for initiating a financial transaction by a cardholder device
US9483786B2	2011-10-13	2016-11-01	Gift Card Impressions, LLC	Gift card ordering system and method
US9031869B2	2010-10-13	2015-05-12	Gift Card Impressions, LLC	Method and system for generating a teaser video associated with a personalized gift
US8699994B2	2010-12-16	2014-04-15	Boku, Inc.	Systems and methods to selectively authenticate via mobile communications
US8412155B2	2010-12-20	2013-04-02	Boku, Inc.	Systems and methods to accelerate transactions based on predictions
US8583496B2	2010-12-29	2013-11-12	Boku, Inc.	Systems and methods to process payments via account identifiers and phone numbers
US8700524B2	2011-01-04	2014-04-15	Boku, Inc.	Systems and methods to restrict payment transactions
CN102610038B *	2011-01-24	2015-05-27	深圳富泰宏精密工业有限公司	Car renting management system
WO2012148842A1	2011-04-26	2012-11-01	Boku, Inc.	Systems and methods to facilitate repeated purchases
US9191217B2	2011-04-28	2015-11-17	Boku, Inc.	Systems and methods to process donations
US9830622B1	2011-04-28	2017-11-28	Boku, Inc.	Systems and methods to process donations
US8538845B2	2011-06-03	2013-09-17	Mozido, Llc	Monetary transaction system

US20130304620A1 *	2012-05-09	2013-11-14	Plastic Jungle, Inc.	Using a value-ascertainable item to obtain credit at a third-party merchant
WO2013055113A1 *	2011-10-13	2013-04-18	에스케이플래닛 주식회사	Mobile payment method, system and device using home shopping
US9208488B2	2011-11-21	2015-12-08	Mozido, Inc.	Using a mobile wallet infrastructure to support multiple mobile wallet providers
US10438196B2	2011-11-21	2019-10-08	Mozido, Inc.	Using a mobile wallet infrastructure to support multiple mobile wallet providers
FR2984420A1	2011-12-20	2013-06-21	Asah Lm	WIND TURBINE MOUNTED ON A ROTATING PLATFORM
US8924711B2	2012-04-04	2014-12-30	Zooz Mobile Ltd.	Hack-deterring system for storing sensitive data records
IL219597D0	2012-05-03	2012-10-31	Syndrome X Ltd	Malicious threat detection, malicious threat prevention, and a learning systems and methods for malicious threat detection and prevention
US8737962B2	2012-07-24	2014-05-27	Twilio, Inc.	Method and system for preventing illicit use of a telephony platform
US11055666B2	2012-08-08	2021-07-06	E2Interactive, Inc.	S/M for providing, reloading, and redeeming stored value cards used in transit applications
US9569769B2	2012-09-17	2017-02-14	E2Interactive, Inc.	Composite activation indicia substrate
US9566911B2	2013-02-15	2017-02-14	Gift Card Impressions, LLC	Gift card presentation devices
US9286528B2	2013-04-16	2016-03-15	Imageware Systems, Inc.	Multi-modal biometric database searching methods
US10580243B2	2013-04-16	2020-03-03	Imageware Systems, Inc.	Conditional and situational biometric authentication and enrollment
US10217107B2	2013-05-02	2019-02-26	Gift Card Impressions, LLC	Stored value card kiosk system and method
WO2014205490A2 *	2013-06-25	2014-12-31	Touch Networks Australia Pty Ltd	An e-product vending system and method
US9578509B1 *	2013-09-20	2017-02-21	Amazon Technologies, Inc.	Authentication via mobile telephone
US11120462B2	2013-11-04	2021-09-14	E2Interactive, Inc.	Systems and methods for using indicia of membership as a partial authorization in a transaction
EP2919178A1 *	2014-03-12	2015-09-16	Alcatel Lucent	System and method of account access notification
US9226217B2	2014-04-17	2015-12-29	Twilio, Inc.	System and method for enabling multi-modal communication
US10262346B2	2014-04-30	2019-04-16	Gift Card Impressions, Inc.	System and method for a merchant onsite personalization gifting platform
US10671983B2 *	2016-11-02	2020-06-02	Mastercard International Incorporated	Computer message routing and processing system and method
US10956049B2	2017-12-12	2021-03-23	E2Interactive, Inc.	Viscous liquid vessel for gifting

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
US20010037264A1	2001-11-01	Payment for network-based commercial transactions using a mobile phone
US7275688B2	2007-10-02	Method for electronic payment
AU2009322877B2	2012-11-29	Mobile barcode generation and payment
CN102859544B	2016-09-14	The system and method paid for using mobile device to be traded
US20020181710A1	2002-12-05	Mobile transaction system and method
US20020107007A1	2002-08-08	Method for wireless telephony payment and an apparatus therefor
US20040030607A1	2004-02-12	Transaction processing system
US9489662B2	2016-11-08	Apparatus and method for storing electronic receipts on a unified card or smartphone
US20020143634A1	2002-10-03	Wireless payment system
WO2003049364A1	2003-06-12	System and method for facilitating electronic financial transactions using a mobile telecommunication device

EP1150262A2	2001-10-31	Payment for network-based commercial transactions using a mobile phone
CN107967646A	2018-04-27	For providing the apparatus and method of transaction business
KR20030082090A	2003-10-22	System and method of electronic payment
KR100378366B1	2003-03-29	The system and method of clearing housing for payment of electronic commerce on the internet
KR20010074337A	2001-08-04	Certification and clearing system for charge of trades by communication device and method thereof
CA2313832A1	2001-11-15	Secure communication
KR101015256B1	2011-02-18	A system for phone-based fund transfer service using an intelligent network, and a method thereof
JP5097310B2	2012-12-12	Product purchase price settlement system and method
KR100476660B1	2005-03-17	Service system for electronic finance using telecommunication network and method thereof
WO2001095546A2	2001-12-13	A method for wireless telephony payment and an apparatus therefor
JP4616443B2	2011-01-19	Electronic payment system and electronic payment method using the same
AU2004100516A4	2004-08-19	Purchasing goods or services on the Internet
AU2013201177B2	2015-05-14	Mobile barcode generation and payment
JP2002074192A	2002-03-15	Network sales system
JP2001117981A	2001-04-27	Safe selling/account settling method for internet

Priority And Related Applications

Priority Applications (2)

Application	Priority date	Filing date	Title
EP00108820.2		2000-04-26	
EP00108820		2000-04-26	

Legal Events

Date	Code	Title	Description
2000-10-17	EEER	Examination request	
2008-11-25	FZDE	Dead	

Data provided by IFI CLAIMS Patent Services

Patents CN1653751

A method of processing an electronic payment cheque

Abstract

The invention relates to processing an electronic payment cheque that relates to a transfer of an amount of money from an account of a first user in a first banking institute to an account of a second user in a second banking institute, which processing includes generating digital signatures by means of asymmetric encryption. The method comprises the following steps:.in a first SIM card, creating an electronic payment cheque and signing the electronic payment cheque with a first signature;.transmitting the signed electronic payment cheque to a second SIM card in a second mobile equipment of the second user; in the second SIM card, additionally signing the electronic payment cheque with a second signature;.transmitting the thus signed electronic payment cheque to subsequently initiate a deposit of the amount of money in the electronic payment cheque into the account of the second user.

Classifications

» H04L63/0442 Network architectures or network communication protocols for network security for providing a confidential data exchange among entities communicating through data packet networks wherein the data content is protected, e.g. by encrypting or encapsulating the payload wherein the sending and receiving network entities apply asymmetric encryption, i.e. different keys for encryption and decryption

View 12 more classifications

CN1653751A

China

Download PDF Find Prior Art Similar

Other languages: Chinese

Inventor: S·安德松, P·卡尔勒, A·卡雷诺拉, P·埃尔德

Current Assignee : Beamtrust AS

Worldwide applications

2003 CN WO AU US EP

Application CNA038102803A events

2002-03-13 Priority to DKPA200200387

2002-03-13 Priority to DKPA200200387

2003-03-13 Application filed by Beamtrust AS

2005-08-10 Publication of CN1653751A

Status Pending

Info: Patent citations (7), Cited by (103), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (22)

Hide Dependent

1. a processing relates to the method for the electronic payment cheque of transferring from first user's of Bank One Corp. mechanism (500) account to second user's of secondary bank mechanism (550) account's the amount of money, described processing comprises that the asymmetric key that comprises private key and PKI by employing produces digital signature to carrying out asymmetric cryptosystem, it is characterized in that, said method comprising the steps of.

In described first user's first SIM card (101a), create electronic payment cheque, and adopt by first of right first private key generation of the first asymmetric key and sign described electronic payment cheque, this first private key resides in described first SIM card (101a) that first mobile device (101b) comprises

Via described first mobile device (101b) of the described SIM card (101a) that comprises described first user, described signed electronic payment cheque is sent to second SIM card (102a) in second mobile device (102b) that is included in described second user,

In described second SIM card (102a), employing is gone up additional second of generation by the second right private key of the second asymmetric key in described second SIM card (102a) and is signed the described electronic payment cheque that has adopted described first signature to sign, this second private key resides on described second SIM card (102a) that described second mobile device (102b) comprises

The described electronic payment cheque that adopts described first and second digital signature signature is sent to central hub (300) from described second mobile device (102b), and this central hub (300) communicates with described first and second banking institution (500,550).

In described central hub (300), banking institution (550) by being preset at described second user is to the checking of described second signature and the checking to described first signature in described first user's banking institution (500), and beginning deposits the amount of money in the described electronic payment cheque among described second user's the account in.

2. the method for claim 1 is characterized in that, described first and second private keys are gone up in described first and second SIM card (101a, 102a) respectively and generated.

3. the method for claim 1, it is characterized in that the transmission of described second SIM card (102a) of described signed electronic payment cheque from described first mobile device (101b) of the described SIM card (101a) that comprises described first user to second mobile device (102b) that is included in described second user is carried out via digital mobile telephone system.

4. as each the described method in the claim 1 to 3, it is characterized in that described signed payment check transmits as short message by SMS service system on gsm system.

5. as each the described method in the claim 1 to 3, it is characterized in that described signed payment check transmits as short message by Ir, bluetooth or Wi-Fi standard.

6. as each the described method in the claim 1 to 5, it is characterized in that the establishment of electronic payment cheque comprises and indicates the telephone number relevant with described second SIM card (102a), the amount of money that will transfer and should therefrom extract the account's of the described amount of money index.

7. as each the described method in the claim 1 to 6, it is characterized in that described method also comprises:

Via described first mobile device (101b), point out the establishment of described first user affirmation to electronic payment cheque, described first SIM card (101a) that described prompting comprises at described first mobile device (101b) goes up to be initiated.

8. method as claimed in claim 7 is characterized in that, described affirmation comprises input PIN-RSA number.

9. as each the described method in the claim 1 to 8, it is characterized in that the electronic payment cheque of described encryption transmits via the Message Agent in the described central hub (300).

10. method as claimed in claim 9 is characterized in that, the electronic payment cheque of described encryption is converted into SMS point-to-point data download message on described Message Agent, is sent to described second SIM card that described second mobile device comprises then.

11. one kind is sent the method that relates to the electronic payment cheque of transferring from first user's of Bank One Corp. mechanism (500) account to second user's of secondary bank mechanism (550) account's the amount of money, described sending comprises that the asymmetric key that comprises private key and PKI by employing produces digital signature to carrying out asymmetric cryptosystem, it is characterized in that, said method comprising the steps of:

In described first user's first SIM card (101a), create electronic payment cheque, and adopt by first of right first private key generation of the first asymmetric key and sign described electronic payment cheque, this first private key resides in described first SIM card (101a) that first mobile device (101b) comprises

Via described first mobile device (101b) of the described SIM card (101a) that comprises described first user, described signed electronic payment cheque is sent to second SIM card (102a) in second mobile device (102b) that is included in described second user.

12. method as claimed in claim 11 is characterized in that, described first private key is gone up in described first SIM card (101a) and is generated.

13. as claim 11 or 12 described methods, it is characterized in that the transmission of described second SIM card (102a) of described signed electronic payment cheque from described first mobile device (101b) of the described SIM card (101a) that comprises described first user to second mobile device (102b) that is included in described second user is carried out via digital mobile telephone system.

14. each the described method as in the claim 11 to 13 is characterized in that, described signed payment check transmits as short message by SMS service system on gsm system.

15. each the described method as in the claim 11 to 14 is characterized in that, described signed payment check transmits as short message by ir, bluetooth or Wi-Fi standard.

16. as each the described method in the claim 11 to 15, it is characterized in that the establishment of electronic payment cheque comprises and indicates the telephone number relevant with described second SIM card (102a), the amount of money that will transfer accounts and should therefrom extract the account's of the described amount of money index

17. each the described method as in the claim 11 to 16 is characterized in that described signed electronic payment cheque transmits via Message Agent.

18. method as claimed in claim 17, it is characterized in that, described signed electronic payment cheque is converted into SMS point-to-point data download message on described Message Agent, be sent to described second SIM card (102a) that described second mobile device (102b) comprises then.

19. method that deposits the electronic payment cheque that relating to of being received transfer from first user's of Bank One Corp. mechanism (500) account to second user's of secondary bank mechanism (550) account's the amount of money in, described processing comprises that the asymmetric key that comprises private key and PKI by employing produces digital signature to carrying out asymmetric cryptosystem, it is characterized in that, said method comprising the steps of:

In described second SIM card (102a), employing is gone up additional second of generation by the second right private key of the second asymmetric key in described second SIM card (102a) and is signed the described electronic payment cheque that received that has adopted first signature to sign, this second private key resides on described second SIM card (102a) that described second mobile device (102b) comprises

The described electronic payment cheque that adopts described first and second digital signature signature is sent to described central hub (300) from described second mobile device (102b), this central hub (300) and described first and second banking institution (500,550) communicate

In described central hub (300), banking institution (550) by being preset at described second user is to the checking of described second signature and the checking to described first signature in described first user's banking institution (500), and beginning deposits the amount of money in the described electronic payment cheque in described second user's account.

20. method as claimed in claim 19 is characterized in that, described second private key is gone up in described second SIM card (102a) and is generated.

21., it is characterized in that the described signed payment check that has received transmits as short message by SMS service system as claim 19 or 20 described methods on gsm system.

22. each the described method as in the claim 19 to 21 is characterized in that, the described signed electronic payment cheque that has received transmits via the Message Agent in the described central hub (300).

Description

Handle the method for electronic payment cheque

The present invention relates to handle the method about the electronic payment cheque of transferring from first user's of Bank One Corp. mechanism account to second user's of secondary bank mechanism account's the amount of money, this processing comprises that the asymmetric key that comprises private key and PKI by employing produces digital signature to carrying out asymmetric cryptosystem.

The multiple means of payment is at present common, for example currency and coins, check, the money transfer from a bank account to another bank account, credit card, debit card, Giro transfer table or the like.Part in these means of payment be more suitable in from a people to another person but not other remit money.The fail safe of money transfer is very important. Some do not want to carry buckets of cash, and everyone is ready that more the money transfer via the bank account or the account that remits and transfers arrives correct recipient's fail safe, and when the means of payment had the intrinsic protection that prevents utilization when being illegally accessed, this was welcome.

About money transfer, a kind of the solution of the safe and simple method of remitting money from a people to another person's electronics is provided is desirable, for example the electronics substitute of check.

United States Patent (USP) 5677955 has been described a kind of computer based electronic instrument that comprises the electronics substitute of check.Illustrate in the literary composition that this electronic instrument can be transferred to another computer from a computer, and can relate to fund and forward account payee to from payer account.This electronic instrument can be signed by the electronic signature that utilizes asymmetric secret key encryption art, and passes through the reception of the electronics substitute of check, and the payee can deposit check in its bank by internet and/or Email.

Even the electronics substitute of check can be stored in the portable pcmcia card, the use of the electronics substitute of check can thereby not moved yet, and it only limits to use in computer/PC.In addition, the electronics substitute of check may use cumbersome, because having relatively high expectations to the information that comprised.

Can use the electronics substitute of check, these reasons because of many former thereby common hope in mobile phone is intrinsic mobility, low-power consumption and many mobile phones facts of start all the time basically of mobile phone.The use of the electronics substitute of check do not realize on mobile phone yet because of still failing to reach high security, this high security for any allocation of the funds, comprise that the account transfer of the electronics substitute of check all is necessary.

Therefore, need a kind of safety method that the electronics substitute of check is forwarded to another mobile phone and/or forwards bank to from a mobile phone.

When being characterised in that when may further comprise the steps, the method described in the beginning paragraph realizes above-mentioned and other purpose: in first SIM card first user, create electronic payment cheque, employing first is signed electronic payment cheque by what right first private key of the first asymmetric key produced, and this first private key resides on first SIM card that first mobile device comprises; Via first mobile device of the SIM card that comprises first user, signed electronic payment cheque is sent to second SIM card that comprises in second user's second mobile device; In second SIM card, additional second signature that employing generates on second SIM card by the second right private key of the second asymmetric key, signature has adopted first electronic payment cheque of signing, this second private key to reside on second SIM card that second mobile device comprises; The electronic payment cheque of having signed first and second digital signature is sent to central hub from second travelling carriage, this central hub and first and second banking institution communicate, and in central hub, banking institution by being preset at second user is to the check of second signature and the check to first signature in first user's banking institution, and beginning deposits the amount of money in the electronic payment cheque in second user's account.

When in the establishment of having carried out electronic payment cheque on the SIM card and signature but also on SIM card, carried out to its credit/debit receive the signature of electronic payment cheque the time, obtain tight security, because SIM card and interface between the mobile device of this card is housed has limited visit inherently to data on the SIM card.The example of used digital mobile telephone system can be global system for mobile communications (GSM) or U.S.'s digital cellular phone service (D-AMPS).

First and second private keys are preferably to generate on first and second SIM card respectively according to method of the present invention.When private key is generating on the SIM card and never beyond SIM card openly the time, they are tamperproof.

In a preferred embodiment, signed electronic payment cheque is carried out via digital mobile telephone system from the transmission of second SIM card of first mobile device to second mobile device that is included in second user of the SIM card that comprises first user.In a further advantageous embodiment, signed payment check transmits as short message by IR, bluetooth or Wi-Fi standard.

According to a preferred embodiment of this method, create electronic payment cheque and comprise the account's index that indicates the telephone number relevant, the amount of money that will transfer accounts and should therefrom extract the account of this amount of money with second SIM card.Therefore, the user of first mobile device, be that the sender of electronic payment cheque only need know the check recipient, promptly the user's telephone number, the amount of money that he wants to transfer into the recipient of second mobile device and he want from which account to withdraw deposit.This method supports the sender of electronic payment

cheque to have the selective possibility therefrom to withdraw deposit of a plurality of accounts, and a default account preferably is set, if the user does not change this setting, then from wherein withdrawing deposit.

When signed payment check transmits as short message by SMS service system on gsm system, cheap, quick and simple money transfer mode that this method provides.

This method is preferably further comprising the steps of: via first mobile device, and the establishment of pointing out first user to confirm electronic payment cheque, this prompting is initiated on first SIM card that first mobile device comprises.Therefore, avoided being not intended to produce money transfer.Checking of establishment to electronic payment cheque preferably includes input PIN-RSA numbering.PIN-RSA numbering is the PIN code of 4 figure places, and it is used to obtain the access right to key file on the SIM card.

According to the present invention, the electronic payment cheque of encryption transmits via Message Agent, and the electronic payment cheque agency of encryption is switched to SMS point-to-point data download message, is sent to second SIM card that second mobile device is comprised then.Message Agent is the integration section of central hub.

Message Agent in the central hub is suitable for specific messages is sent to the SIM card that comprises in the mobile device from banking institution via the bank's application that is also contained in usually the BDC.The BDC territory can comprise some banks territory, promptly be linked to some banks of the service in BDC territory, and uses identical BDC to handle transaction.The BDC territory can be divided into a BDC and some banks zone.Part of functions that may be common between BDC is in charge of in bank, as internet bank.

Other claim is described other preferred embodiment of the present invention.

Term cellular phone and " travelling carriage " synonym, and be used for defining mobile phone, it is divided into two logical blocks: " mobile device " and " subscriber identity module (SIM) ".Mobile device has the repertoire that carries out radio communication with digital mobile telephone system.Therefore, mobile device equals travelling carriage with SIM.Do not have SIM, mobile device can only carry out urgent call.SIM card is a smart card, and it is used to store the relevant information of subscribing.

Below in conjunction with the example of preferred embodiment and with reference to accompanying drawing, the present invention more completely is described, wherein:

Fig. 1 a and 1b represent to carry out the overview of the each several part of method of the present invention,

Fig. 2 is the schematic diagram of the data flow between some part of carrying out method of the present invention, and

Fig. 3 a and 3b are respectively the general introductions of digital signature calculating and digital signature authentication.

In each accompanying drawing, identical reference number is represented similar elements.

Fig. 1 a represents to carry out the example of overview of the each several part of method of the present invention.These parts are expressed as in the territory 100 that is included in the user respectively, network operator's territory 200, central hub 300, bank data processing center (BDC territory) 400 and the banking institution 500.Shown is the mobile phone 101 and 102 of working in digital mobile telephone system 100, and wherein mobile phone 101 is senders of electronic payment cheque, and mobile phone 102 is its recipients.This digital mobile telephone system 100 can be global system for mobile communications (GSM) or U.S.'s digital cellular phone service (D-AMPS).

In this explanation, term " recipient " is used to represent send to it mobile phone 102 of electronic payment cheque, and term " sender " is used to represent the mobile phone 101 from wherein sending electronic payment cheque.But, term " recipient " and " sender " also can represent respectively to its send electronic payment cheque mobile phone 102 the user and from the user of the mobile phone 101 that wherein sends electronic payment cheque.

As mentioned above, term cellular phone and " travelling carriage " synonym, and be used for defining mobile phone 101,102, it is divided into two logical blocks: " mobile device " 101b, 102b and " subscriber identity module (SIM) " 101a, 102a.Mobile device 101b, 102b have the repertoire that is used for carrying out with digital mobile telephone system radio communication.Therefore, mobile device 101b, 102b equal travelling carriage 101,102 respectively with SIM 101a, 102a.In this explanation, the application program of carrying out method of the present invention is arranged on the SIM card; For ease of reading this explanation, this not necessarily offers some clarification on.

In order to use method of the present invention, promptly to activate application program, the user must register in banking institution 500 by internet bank usually, will illustrate below.After registration, the user receives new SIM card 101a, 102a as the subscriber from network operator 200.This SIM card 101a, 102a comprise the application program of sending and receiving of the electronic payment cheque that is used to support the method according to this invention.SIM card 101a, 102a preferably pass through personalization, so that allow the remote update of aerial (OTA).Activation must be by successful execution before can using the service of carrying out the method according to this invention, and after this, the user can use SIM card 101a, the 102a of mobile device and customization.Application program on SIM card 101a, the 102a is responsible for signing electronic payment cheque and and user interactions.

Send specific messages from bank's application 402 to mobile phone 101,102 by SMS-C201 and carry out the OTA renewal via SMS gateway/proxy 401 in the BDC territory 400 and network operator.Application message transmits as the user data in the short message, and utilizes mobile initiation and mobile-terminated short message to transmit between mobile phone 101,102 and SMS-C 201.

Thereby BDC territory 400 has the interface of the gsm environment to central hub 300 to the network operator.SMS gateway 401 is responsible for communicating by letter via central hub 300 and network operator territory 200 interior SMS-C 201.Bank in the BDC territory 400 uses 402 and utilizes XML interface and SMS gateway/proxy 401 to communicate.By this interface, can allow BDC 200 ask the OTA of the application message on SIM card 101a, the 102a to upgrade.The XML interface comprises recipient's telephone number and as ordinary text message or be sent to the character string that the application message of SIM application program sends.XML document utilizes HTTP method POST to send between bank's application 402 and SMS gateway/proxy 401.

SMS gateway/proxy 401 also has the service of initiating message of moving of monitoring.This service processing is from the entire message of mobile phone 101,102 (is to move the request of initiation or irrelevant to the mobile terminating request responding with it), and message is sent to the territory of banking institution 500 as XML document.

For the information that is sent to SMS gateway/proxy 401 from bank's application 402, bank uses 402 as the HTTP client computer, and SMS gateway/proxy 401 is as http server.Use 402 information for be sent to bank from SMS gateway/proxy 401, use opposite process, promptly SMS gateway/proxy 401 is used as the HTTP client computer, and bank uses 402 as http server.

By short message service (SMS), carry out the sender 101 of electronic payment cheque and the information exchange as shown by arrows between the recipient 102 by means of the SMS gateway/proxy server 401 in the BDC territory 400 of central hub 300 and sender bank and via the SMS central SMS-C 201 in network operator's the territory 200.SMS gateway/proxy server 401 is used 302 by the bank that communicates with banking institution 500 and is supported.BDC territory 400 can be positioned within the banking institution 500 or near, but this is optional, as long as BDC territory 400 and banking institution 500 can communicate.

It is transparent that communicating by letter between SMS gateway/proxy 401, central hub 300 and the SMS-C 201 uses 402 to bank.SMS gateway/proxy 401 in the BDC territory 400 is utilized the SMS-C agreement, is connected to network operator's SMS-C 201 as SMPP.SMS-C 201 is responsible for sending SMS message to mobile phone when sending request from SMS gateway/proxy 401, and the short message of initiating from mobile phone is forwarded to SMS gateway/proxy 401.Mobile originated short message at specific SME address, be so-called big account.SMS-C the SME map addresses to the address of SMS gateway/proxy 401, and the SMS gateway/proxy 401 of forwards in the BDC territory 400 Message, be that the transmit leg of the MSISDN of mobile phone must be delivered to SMS gateway/proxy 401 from SMS-C 201, use 402 so that further be sent to bank.

Hereinbefore, abbreviation SME represents " Short Message Entity ", and it is the entity that can receive and/or send SMS message.For example, SME can be arranged in travelling carriage or fixed network.Abbreviation MSISDN represents " travelling carriage International ISDN number ", and it is the standard international telephone number that is used to identify given user.This number is based on ITU-T (International Telecommunications Union-telecommunication standardization sector) standard E.164.At last, abbreviation SMPP represents " reciprocity short message ", and wherein " equity " is a kind of traffic model, and wherein each side has identical ability, and the either party all can initiate communication session.

Therefore, application message transmits as the user data in the short message, and utilizes mobile initiation and mobile-terminated short message to transmit between mobile phone and SMS-C 201.SMS gateway 401 also has the service of initiating message of moving of monitoring.This service processing is from the entire message of mobile phone 101,102 (is to move the request of initiation or irrelevant to the mobile terminating request responding with it), and message is sent to banking institution 500 as XML document.The SMS gateway/proxy is functional must to send to another to the message that is encoded to SMS point-to-point data download message from a mobile phone.

Be described in more detail requirement below to SMS gateway/proxy 401.SMS gateway/proxy 401 must be able to be proofreaded the entire message of initiating from travelling carriage 101,102.According to type of message, SMS gateway/proxy 401 should be routed to message banking institution 500 or forwards is arrived another mobile phone 101,102.Shown in Figure 1 from or the message that is sent to mobile phone comprise electronic payment cheque 10, move and initiate application

message 20 and mobile terminating application message 30.Certainly, send to another short message of 102 (SM) from a mobile phone 101 and generally can comprise text message; But they do not have shown in Figure 1, because they are not focus of the present invention

About send and be forwarded to the message of another mobile phone 102 from a mobile phone 101.SMS gateway/proxy 401 should be carried out following steps:

From move initiation application message 20, extract recipient 102 telephone number, and it is put into the SM head as destination address.

Initiate the address from moving to initiate to extract the SM head, and it is put into the parameter of application message as the telephone number of transmit leg (sender).

Preferably the actual date from the gateway/proxy server is appended to application message as parameter.Therefore, electronic payment cheque has been equipped with the check opening date, and check effective option in the limited period that bank sets is provided.The effective time of check then can be from time that check sends, to be it begin to calculate through date of the SMS gateway/proxy server 401 of sender's banking institution 500.

Is the mobile terminating message coding that SMS point-to-point data are downloaded (SMS PP DD) message.This makes mobile device be forwarded to SIM to short message pellucidly.

The element of Fig. 1 b presentation graphs 1a is respectively in conjunction with the territory 350 of recipient's network operator's territory 250, electronic payment cheque recipient's bank data processing center (BDC territory) and recipient's banking institution 550.Network operator's territory 250 comprises SMS central SMS-C 251, and the BDC territory 350 of recipient's banking institution comprises that SMS gateway/proxy server 351 and bank use 352.Fig. 1 a and hollow arrow among the 1b express possibility and certain takes place communicate by letter, but further do not specify this communication

When recipient 102 had received electronic payment cheque, he can deposit it in his bank account of banking institution 550.For this reason, the recipient uses 452 to the SMS from mobile phone 102 via SMS-C 251, hub 300, SMS gateway/proxy server 451 and bank and sends to its banking institution 550.This SMS comprises electronic payment cheque 10 and check deposits request 40 in.After receiving that check deposits request 40 in, banking institution 550 beginning and sender's banking institution 500 communicates by letter, thus the account transfer of the amount of money that indicates in the realization electronic payment cheque from sender's account to recipient's account.The details of this communication is described below.

Recipient 102 has received electronic payment cheque, wherein has the telephone number that receives mobile phone 102, will transfer into the digital signature of the application program generation on the SIM of recipient's the amount of money and the sender account that should therefrom withdraw deposit and mobile phone 101 from the sender; In addition, the additional automatically MSISDN that sends mobile phone 101 of SMS gateway/proxy 301.Therefore, the sender of electronic payment cheque can be offered like clockwork and be received mobile phone 102.SMS gateway/proxy 301 is also added dater, provides date issued to electronic payment cheque.

The recipient begins to adopt second digital signature to sign electronic payment cheque, and adopting the such signed electronic payment cheque of first and second digital signature to be sent to central hub 300 from second travelling carriage 102.Hub 300 is carried out following the processing:

The part of the check of second user, 102 signatures is sent to second user's 102 banking institution 550.Banking institution's 550 certifying signatures of second user 102, and return corresponding account number according to GSM number of second user 102 and account's index.

The actual account number that central hub 300 receives the banking institution 550 from second user 102 appends to the part of the transaction of first user, 101 signatures.These data are sent to first user's 101 banking institution 500.First user's banking institution 500 checking is from first user's signature, and determines whether there are enough funds among the account that telephone number (for example GSM number) and account's index by first user 101 show.If there are enough funds in first user's 101 account, then first user's 101 500 second users of beginning in secondary bank mechanism 550 of banking institution account transfers accounts.First user's 101 banking institution 500 is to central hub 300 return responses.Be rejected if this is replied, then central hub 300 sends SMS message to first and second users 101,102, wherein has expression and has refused the information of transferring accounts.If reply to confirming that then central hub 300 sends application type SMS to second user 102, this application type SMS eliminates the check from second user's 102 SIM card.

No matter reply refusal or affirmation to the allocation of the funds, the recipient of electronic payment cheque all can have notice and not postpone basically.Equally, the recipient of electronic payment cheque can receive about the notice of this reception and the not delay when receiving basically.

Though only represented two users, BDC, two banking institution, should be appreciated that any amount of basically usefulness in the user domain can be carried out method of the present invention per family.In addition, a plurality of BDC, banking institution, SMS center can be used in the present invention's realization.

The application program support that is used to realize method of the present invention on user's the SIM card is sent check from a plurality of accounts of different banking institution; The user is for example starting the service that realizes this method in 5 different banks, so that use 10 accounts altogether.

Fig. 2 is the schematic diagram of the data flow between some part of carrying out method of the present invention.Fig. 2 represents that check sender data 50 send to the recipient's of electronic payment cheque second mobile phone 102 from sender's mobile phone 101.Check sender data 50 comprise electronic payment cheque at least, receive the telephone number of mobile phone 102, will transfer into recipient's the amount of money and the sender account that should therefrom withdraw deposit from the sender.Check sender data also comprise the digital signature that application program generated on the SIM of mobile phone 101.Therefore, check sender data 50 were confirmed and signature by the sender before sending, and are sent via SMS.Check sender data 50 send via sender's SMS gateway/proxy 301 (not shown among Fig. 2), and wherein the SMS gateway/proxy receives SM, to its recompile and be forwarded to and receive mobile phone 102.

When recipient 102 wishes that when receiving check and deposit bank account in, it also can carry out via SMS.Recipient 102 enters the appropriate application on the SIM card of mobile phone 102 via the suitable menu entries in the services menu, and has been provided all and has received the tabulation of check.In the next one was mutual, recipient 102 selected the check that deposit in, if do not set default account, then also selected the account that should deposit in, and he imports individual service PIN code, PIN-RSA, thereby allowed the signature transaction.

Sending from recipient 102 before check deposits request 51 in, show the general introduction of collected information to recipient 102.Shown information is the amount of money, account's pet name, date and Ref. No..Shown Ref. No. is the transaction identifiers that is connected with signature identifiers.The user confirms and with digital form signature general introduction, and deposits check in request 51 and send to central hub 300.Therefore, check deposits in and asks 51 to comprise check recipient's signature and check sender's signature.

The data communication 52 of central hub 300 initiations and second user's 102 banking institution 550.Central hub 300 sends to the part of the check of second user, 102 signatures second user's 102 banking institution 550 in transfer of data 52, and banking institution's 550 certifying signatures of second user 102, and, return corresponding account number to central hub 300 according to GSM number of second user 102 and account's index.

The actual account number that central hub 300 receives the banking institution 550 from second user 102 appends to the part of the transaction of first user, 101 signatures.These data are sent to first user's 101 banking institution 500 in transfer of data 53.First user's banking institution 500 checking is from first user's signature,

and determines whether there are enough funds among the account that telephone number (for example GSM number) and account's index by first user 101 show.If there are enough funds in first user's 101 account, then first user's 101 banking institution 500 initiates the account's of second user in secondary bank mechanism 550 account transfer (not shown).

First user's 101 banking institution 500 is to central hub 300 return responses 54.Be rejected if reply 54, then central hub 300 sends SMS message 55,56 to first and second users 101,102 respectively, wherein has to have refused the information of transferring accounts.If reply to confirming that then central hub 300 sends application type SMS 55 to second user 102, the check that application type SMS 55 eliminates from second user's 102 SIM card.

It is well-known that the right asymmetric cryptosystem of asymmetric key that comprises private key and PKI by employing generates digital signature itself, but it will be described with reference to Fig. 3 a and 3b below with of the present invention being used in combination.

Asymmetric cryptosystem system or PKI system adopt two different keys, promptly are used for the PKI 4b and the private key 4a of encryption and decryption.Two key 4a, 4b are relative to each other, and it is right to form the unique key of individual, but can not be according to the understanding of a key is calculated another.PKI or private key can be used for encrypting.Key is then adopted in deciphering, and right corresponding secret key is carried out.For example, adopt the message of recipient's public key encryption can only adopt same recipient's private key to be decrypted.(Adleman) algorithm is the actual standard that is used for the PKI system now to RSA for Rivest, Shamir.

Hashing algorithm 2 is used for creating the eap-message digest of digital finger-print or certain segment information.Even the minimum change in the origination message document also produces diverse digital finger-print.MAC (authentication of message sign indicating number) is the ashed information that adopts symmetric key encryption.MAC provides integrality for message, does not abandon but do not have.SHA-1 is the hashing algorithm of using always.It produces the 20 byte message summary of any input message.

Digital signature is created in the following manner:

Origination message 1 adopts hashing algorithm 2 (for example SHA-1) to carry out shuffling, and the digital finger-print 3 of creating origination message.

Fingerprint 3 adopts the private key 4a of transmit leg to encrypt.

The result is a digital signature 5, and it is unique for each combination of message 1 and private key 4a.Message 1 and digital signature 5 form entity 6.

After receiving, digital signature 5 is verified in the following manner:

Comprise origination message in the entity 6 of origination message 1 and digital signature 5 through being used to create the hashing algorithm 2 of digital signature 5, thereby digital finger-print 3 ' is provided.

Signature 5 adopts the PKI 4b of transmit leg to be decrypted, and the digital finger-print 3 of deciphering is provided ".

The digital finger-print 3 of digital finger-print 3 ' and deciphering " compare ?.If they are identical, then digital signature 5 is effective.

Digital signature provides the following:

The checking of the identity of transmit leg.

The assurance of any variation of notification message (integrality).

Transmit leg can't refuse to send the assurance (nothing is abandoned) of message.

in the method for the invention, above-mentioned notion is used for creating Secure Transaction.

The activation of the service that will describe below, be used for carrying out method of the present invention, it is right to generate RSA key on SIM card.Private key is stored in the tamperproof zone on the SIM card, and PKI outputs to server the BDC territory from mobile phone.Server sends to mobile phone with the RSA PKI of itself again.The open index that all RSA keys (end user and BDC key) have 1024 moduluses and are set to 2^16+1 (=65537).

In order to allow the transmit leg that server can verification public key, the user receives one-time password (otp) by the autonomous channel (for example via internet bank) of safety from server in advance.Application program on the SIM card utilizes SHA-1 to calculate eap-message digest.Input is all information of transmission in message (comprising PKI) and the connection string of OTP.The eap-message digest that generates is 20 bytes, but is truncated to preceding 8 bytes, so that create identifying code.

PKI is output to the BDC territory with out of Memory and identifying code.The total length of message is 139 bytes (1 byte message types+1 byte protocol version+1 byte SIM application version+128 byte PKIs+8 byte identifying codes), and it can send in a SM

Server then can calculate identifying code with the same manner according to known OTP and received information.If with the comparison success of the identifying code that receives, it is destroyed to think that then PKI does not have in transmittance process, and it comes from described user really.If accept user's PKI, then server sends the PKI that belongs to this BDC territory, and it will be used for server authentication in subsequent operation.Message comprises new identifying code, and this makes the application program on the SIM card can verify that this message comes from correct source.It also comprises BDC identifier BDC-ID, and BDC-ID is used for PKI is linked to correct BDC (under the situation of a plurality of BDC) by phone.Identifying code is preceding 8 bytes of utilizing the eap-message digest of SHA-1 calculating equally.Input is all information of transmission in message (comprising PKI) and the connection string of OTP.

PKI is sent to mobile phone with out of Memory and identifying code.The total length of message is 138 bytes (1 byte message types+1 byte BDC-ID+128 byte PKI+8 byte identifying codes), and it can send in a SM.Application program on the SIM card then can be calculated identifying code with the same manner according to known OTP and the information that is received.If with the comparison success of Receipt Validation sign indicating number, it is destroyed to think that then PKI does not have in transmittance process, and it comes from this BDC really.

For the OTA that mobile phone can be trusted from the BDC territory upgrades and request, need a kind of mechanism that is used for server authentication.According to public key cryptography standards, adopt RSA and BDC private key to encrypting from all information in the message of server.This creates signature, and it makes the application program on the SIM card can carry out server authentication when receiving message.Except application message, the message of signature also comprises type of message, BDC identifier and sequence number

Notice that type of message and BDC identifier are not also had cryptographically sends to mobile phone, because the SIM application program needs them before the message that checking (deciphering) is signed.How type of message is used for determining processing messages.The BDC identifier is used for selecting being used for the PKI to decrypt messages.

Sequence number is 3 byte integer that BDC generates, and it must add one to each new operation of specific user's request to BDC, and promptly each user adopts independently counter.Before cryptographic operation, information must be filled into 128 bytes.Owing to do not calculate the hash of message, therefore will not comprise the hashing algorithm identifier.Fill and carry out in the following manner basically:

The string of filling character that structure is made of (byte lengths of the data that 128-[will sign]-3) eight bit byte with hexadecimal value FF.

Connect the string of filling character, message and delimiter to be signed, thereby form filling message.

BDC signs filling message by the private key that adopts BDC to information encryption then.When receiving this message, the SIM application program is carried out following steps:

Utilize RSA to pass through the BDC PKI to decrypt messages.Which PKI BDC-D is used for selecting be used for decrypt messages.

Check is filled character, so that authorization information does not change after signature, deletes the data of filling character and being signed to recover then.For obtaining added security, BDCID in the signed message and type of message also can compare with BDCID and the type of message that unencryption just sends, so that authorization information does not change as yet.

Sequence number and the sequence number that receives with last OTA request are compared, so that prevent the attempt of resetting.This numbering must add one to each new OTA request by server.

The Client-initiated move transaction is signed, and can list following every:

Send check (via SMS)

Deposit check (via SMS) in

Sign transaction according to public-key encryption standard, employing RSA.

Be summarized in parameter and order thereof when signing in the process of exchange below The SHA-1 hash is calculated according to the following connection data in each transaction.

Send check

MSISDN_receiver (20 byte)

BDCID_issuer (1 byte)

AccountID_issuer (1 byte)

ChequeAmount (15 byte)

Cheque ID (3 byte)

The form of recipient's telephone number, MSISDN-receiver are complete international telephone number when signature, by user's input, do not have "+" or " 00 " character string the preceding.

Deposit check in

BDCID_receiver (1 byte)

AccountID_receiver (1 byte)

SignID (3 byte)

ChequeIssueDate (8 byte)

Signature_issuer (128 byte)

In transaction is summed up, show 7 reference numbers (RefNo) to the user.4 transaction identifiers (TrxID) that RefNo normally is connected with 3 signature identifiers (SignID) of user.But in depositing check trading in, generation and Cashier's is not mutual, therefore may not receive TrxID.For the form that allows RefNo that the user is consistent, in this operation, adopt unsigned pseudo-value (" 0000 ") to replace TrxID.

In signature calculation, 20 byte results of above-mentioned SHA-1 computing are filled into 128 bytes, and encrypt by user's private key, employing RSA.

Filling according to EMSA-PKCS1-V1_5 coding computing carry out.Fill and carry out in the following manner basically:

Utilize SHA-1 to come shuffling message.

Utilize DER (special coding rule) to construct SHA-1 hashing algorithm identifier.This produces following eight bit byte character string:

30?21?30?09?06?05?2b?0e?03?02?1a?05?00?04?14

The string of filling character that structure is made of 90 eight bit bytes with hexadecimal value FF.

Connect fill character string, algorithm identifier, shuffling message and delimiter, fill message thereby form.

00 || 01 || FF FF[...86xFF...] FF FF || 00 || 30 21 30 09 06 05 2b 0e03,02 1a, 05 00 04 14 || [shuffling message]

Signature verification is carried out in the following manner:

Utilize the original transaction of SHA-1 shuffling, and use above-mentioned filling.

The PKI that utilizes RSA and user is to the signature deciphering.

Transaction and decrypted signature after shuffling and the filling are compared.If their couplings, then signature is effective

User's registration is described below, is the activation of the application program on the SIM card.Described registration is carried out via internet bank.Suppose that the

user has received new SIM card and has been instructed to from the network operator and activate the service be used to carry out method of the present invention by internet bank.Therefore suppose impliedly that the user is the registered user of internet bank and thereby has had a trusting relationship between user and bank.In addition, suppose that the user has registered the service of carrying out method of the present invention via internet bank, and after this bank sends request so that provide and distribution support is used to carry out the new SIM card of the application program of method of the present invention to the user to the network operator.In addition, suppose that mobile phone starts shooting, and inserted new SIM card.

The user selects the menu option in the internet bank, so that activate the service that is used to carry out method of the present invention.Then, on screen, show 8 one-time password (otp)s to the user.This information is used for the SIM application program, user rs authentication is provided and initiates key to generate.Indication user choice menus option is so that activate the service that is used to carry out method of the present invention on mobile phone.

Select " Service Activation " option in the menu of user on mobile phone, and input OTP.Input OTP triggering generates RSA key on SIM card right.Private key is stored in the tamperproof memory cell of SIM card.Application computes identifying code on the SIM card.All information in the message that input is with OTP is connected, i.e. type of message, OTA protocol version, SIM application version and user's PKI.The 8 byte identifying codes that generate then in SM other parameter be sent to the BDC territory

Note, on SIM card, need SME address (telephone number), so that send message to the BDC territory.The SME address can be pre-configured on SIM card, but in a plurality of BDC environment, the SME address preferably can show to the user with OTP on computer screen, be transfused to mobile phone then after OTP.

Accepting before PKI is used for the BDC territory, the identifying code according to the local calculating of identical parameters the identifying code that receives from mobile phone and the BDC territory compares.If relatively be successful, storage of public keys then.

If accept user's PKI, then the PKI of himself is exported in the BDC territory, and this PKI will be used for server authentication in subsequent operation.Message comprises new identifying code, and this makes the application program on the SIM card can verify that this message comes from correct source.It also comprises BDC-ID, and this BDC-ID is used for PKI is linked to correct BDC (under the situation of a plurality of BDC) by phone.

Calculate identifying code, all information in the message that input is with OTP is connected, the i.e. PKI of type of message, BDCID and BDC.The 8 byte identifying codes that generate then in SM other parameter be sent to mobile phone.

When receiving message, the application program on the SIM card will compare according to the local identifying code that calculates of identical parameters in identifying code and the mobile phone, thus the authentication sign indicating number.If be proved to be successful, storage of public keys then, and to this result of BDC field notice.

Then, the BDC territory sends message to mobile phone, wherein comprises the required information of configuration of the application program on the SIM card.This packets of information adopted the private key of BDC to sign before sending to mobile phone (encryption).This makes the SIM application program can carry out server authentication when receiving message.

Except application message, the message of signature also comprises type of message, BDC-ID and sequence number.Type of message and BDC-ID are not had to encrypt yet to be sent, because the SIM application program needs these parameters so that processing messages.Message is signed " mistake then! Do not find reference source ".

When receiving this message, SIM application program verification signed message, and checking sequence number.BDC-ID is used for selecting be used to verify the PKI of message.

If be proved to be successful, storing applied data then, and to this result of BDC field notice.The sequence number that receives in the request from BDC is returned in response, and can be used for results link to corresponding request at server end.

The request user selects the PIN code of 4 figure places, and it will be used for obtaining the access right to the key file on the SIM card.This PIN code is called PIN-RSA in this article.At last, notify the user by text message on display screen of mobile telephone, the service that is used to carry out method of the present invention is activated.

Can by central hub provide useful functional be to handle checkbook via Web server.When the user sent to another user with check, this transmission was through central hub and SMS server.When central hub register check, it can send " check sends " message to Web server Telephone number, account's index, check that " check sends " message comprises sender and recipient identify, treat transfer amount and date.Web server writes the checkbook table to these data.

When the recipient of electronic payment cheque deposits check in, this will carry out via central hub.When central hub reception was confirmed from the account transfer of sender's banking institution, central hub sent " check is paid " message to Web server.This " check is paid " message comprise check sign, sender and recipient telephone number, treat transfer amount and date.Web server is put into " check is paid " table to this check.Here, sender and recipient automatically have the renewal checkbook of having sent and having received check.

Via web interface, user's (being sender and/or recipient) can be connected to Web server, and checks and all sent check.For example, may there be following five kinds of possibilities: " all checks ", " paid settled check ", " having sent check ", " having received check ", and " cashing check ".

" all checks " explicit user sends and/or receives, has the tabulation of all checks of its state (depositing or do not deposit in the account of banking institution in)." paid settled check " explicit user sends, the tabulation of the check that deposits in of the side of being received.The explicit user that " sent check " has sent but the tabulation of the check that deposits in of the side of not being received as yet.The explicit user that " received check " has received but the tabulation of the check that do not deposit in as yet, and " cashed check " explicit user has received and deposited in the account's of banking institution the tabulation of check.The possibility that instrument " paid settled check " provides definite check whether to be deposited in reciprocal account for the user, this claims under the situation of not receiving check the recipient and is suitable for.If the recipient claims do not receive and send check, then can retransmit this check.The fail safe of this re-transmission is that the check of any repetition will be refused by banking institution.

In addition, the service of this checkbook can comprise general strobe utility, make the user can select only to check in the selected time interval, to have sent and/or received, from and/or be sent to the check of selected telephone number or the like.

Check will expire after given number of days.When closing on the validity date of " not cashing " check, Web server can be notified user under it by short message.

Illustrated that more than message can send as short message via the SMS business.But, because bulk information and signature in the check must send as two short messages from the check that the sender left and sent to the recipient.First user's signature is divided into two parts, and check then sends as two SM, has the part of signature in each.For can be once more in recipient's one side with message relating, each message must comprise quoting the other parts of message; This parameter

is called MessageReference, is a byte counter unique to each user.Two kinds of message must comprise recipient's telephone number (MSISDN), so that allow the SMS agency that forwards is arrived the recipient.The second portion that sends to recipient's check from the sender comprises the second portion of signature.

As described above in detail, sender's depositing in of check of sending and sending in recipient's banking institution the recipient can start by the short message that sends from the recipient.Equally, because bulk information and comprise the sender and the needs of recipient's signature, request message must send as three short messages.The one SM comprises check information, and back two short messages comprise recipient and sender's signature respectively.For can be once more in recipient's one side with message relating, each message must comprise quoting the other parts of message; This parameter is called MessageReference, is a byte counter unique to each user.

Use be equipped with IrDA, fast the mobile phone of IrDA or bluetooth facility to withdraw deposit from ATM (ATM) be well-known.If the electronic payment cheque service realizes that in the SIM card of the mobile phone with IrDA, quick IrDA or bluetooth facility then mobile phone can be used for by the amount of money in the ATM extraction electronic payment cheque.In addition, the user can select to extract from ATM the part of the amount of money that shows the electronic payment cheque, and the remainder of the amount of money is deposited in the account.

In general, be noted that the point to point link between a travelling carriage (mobile phone) and another travelling carriage also can be according to IrDA or quick IrDA standard, bluetooth standard, Wi-Fi standard and/or any other short-range communication standard.

Patent Citations (7)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US5511121A *	1994-02-23	1996-04-23	Bell Communications Research, Inc.	Efficient electronic money
US5677955A *	1995-04-07	1997-10-14	Financial Services Technology Consortium	Electronic funds transfer instruments
US5907801A *	1995-09-22	1999-05-25	At&T Wireless Services, Inc.	Apparatus and method for optimizing wireless financial transactions
US6067529A *	1998-08-12	2000-05-23	Ericsson Inc.	System and method for sending a short message containing purchase information to a destination terminal
AT442746T *	1998-09-10	2009-09-15	Swisscom Ag	PROCEDURE FOR BUYING GOODS OR SERVICES WITH A MOBILE PHONE
IL134741A *	2000-02-27	2003-11-23	Adamtech Ltd	Mobile transaction system and method
DE10028028A1 *	2000-06-08	2001-12-13	Ernst Forster	Use of mobile telephone and SMS messaging with credit card or account to make transaction

* Cited by examiner, † Cited by third party

Cited By (103)

Publication number	Priority date	Publication date	Assignee	Title
CN101926147A *	2007-12-27	2010-12-22	意大利电信股份公司	Method for enjoying service through mobile telephone terminal and subscriber identification card for implementing it
WO2011044740A1 *	2009-10-13	2011-04-21	国民技术股份有限公司	Method and system for mobile payment
CN102034177A *	2009-09-29	2011-04-27	国际商业机器公司	Method and device for realizing effective mobile ticket transfer
CN101511074A *	2009-03-30	2012-03-07	宇龙计算机通信科技(深圳)有限公司	Selection method, system, server and terminal for mobile terminal paying account
CN102799660A *	2012-09-04	2012-11-21	南京天溯自动化控制系统有限公司	Data checking method and data checking device
Family To Family Citations				
WO2004004199A1 *	2002-06-26	2004-01-08	Telefonaktiebolaget Lm Ericsson (Publ)	Method of controlling a network entity and a mobile station
US20050097046A1	2003-10-30	2005-05-05	Singfield Joy S.	Wireless electronic check deposit scanning and cashing machine with web-based online account cash management computer application system
GB2417813A *	2003-12-18	2006-03-08	Veritas Mobile Solutions Pte L	System and method for facilitating payment via a communications network using value accredited to a customer of the communications network
EP1733340A1 *	2004-03-22	2006-12-20	Philips Intellectual Property & Standards GmbH	Electronic payment of content
WO2005119607A2 *	2004-06-03	2005-12-15	Tyfone, Inc.	System and method for securing financial transactions
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card

US7797250B2 *	2005-11-18	2010-09-14	Pitney Bowes Inc.	Method for electronically endorsing check images
KR20070077569A *	2006-01-24	2007-07-27	삼성전자주식회사	One time password service system using portable phone and certificating method using the same
US7633916B2 *	2006-01-24	2009-12-15	Sony Corporation	System and method for providing data to a wireless communication device
CN101064603A *	2006-04-27	2007-10-31	国际商业机器公司	Short message forwarding method and system, server and short message receiving and transmitting apparatus
US7559461B2 *	2006-06-02	2009-07-14	First Data Corporation	ATM systems and methods for cashing checks
US9332009B2 *	2006-09-29	2016-05-03	Telecom Italia S.P.A.	Use, provision, customization and billing of services for mobile users through distinct electronic apparatuses
US8799147B1	2006-10-31	2014-08-05	United Services Automobile Association (Usaa)	Systems and methods for remote deposit of negotiable instruments with non-payee institutions
US7876949B1	2006-10-31	2011-01-25	United Services Automobile Association	Systems and methods for remote deposit of checks
US7885451B1	2006-10-31	2011-02-08	United Services Automobile Association (Usaa)	Systems and methods for displaying negotiable instruments derived from various sources
US8708227B1	2006-10-31	2014-04-29	United Services Automobile Association (Usaa)	Systems and methods for remote deposit of checks
US7873200B1	2006-10-31	2011-01-18	United Services Automobile Association (Usaa)	Systems and methods for remote deposit of checks
US8351677B1	2006-10-31	2013-01-08	United Services Automobile Association (Usaa)	Systems and methods for remote deposit of checks
FI121323B *	2007-02-09	2010-09-30	Hsl Helsingin Seudun Liikenne	Procedure, ticket processing device, computer software product and product platform for an electronic ticket security mechanism
US8959033B1	2007-03-15	2015-02-17	United Services Automobile Association (Usaa)	Systems and methods for verification of remotely deposited checks
DE102007015788B3 *	2007-03-30	2008-10-23	Fm Marketing Gmbh	Multimedia device and method for data transmission in a multimedia device
US8538124B1	2007-05-10	2013-09-17	United Services Auto Association (USAA)	Systems and methods for real-time validation of check image quality
US8433127B1	2007-05-10	2013-04-30	United Services Automobile Association (Usaa)	Systems and methods for real-time validation of check image quality
US8070057B2	2007-09-12	2011-12-06	Devicefidelity, Inc.	Switching between internal and external antennas
US20090070691A1	2007-09-12	2009-03-12	Devicefidelity, Inc.	Presenting web pages through mobile host devices
US9304555B2	2007-09-12	2016-04-05	Devicefidelity, Inc.	Magnetically coupling radio frequency antennas
US9311766B2	2007-09-12	2016-04-12	Devicefidelity, Inc.	Wireless communicating radio frequency signals
US8915447B2	2007-09-12	2014-12-23	Devicefidelity, Inc.	Amplifying radio frequency signals
US9058512B1	2007-09-28	2015-06-16	United Services Automobile Association (Usaa)	Systems and methods for digital signature detection
HU230695B1 *	2007-10-20	2017-09-28	Andras Vilmos	Method of preparing storing and method of storing single user access information into safe storage unit of a communication device
US8358826B1	2007-10-23	2013-01-22	United Services Automobile Association (Usaa)	Systems and methods for receiving and orienting an image of one or more checks
US9892454B1	2007-10-23	2018-02-13	United Services Automobile Association (Usaa)	Systems and methods for obtaining an image of a check to be deposited
US9898778B1	2007-10-23	2018-02-20	United Services Automobile Association (Usaa)	Systems and methods for obtaining an image of a check to be deposited
US9159101B1	2007-10-23	2015-10-13	United Services Automobile Association (Usaa)	Image processing
US7996315B1	2007-10-30	2011-08-09	United Services Automobile Association (Usaa)	Systems and methods to modify a negotiable instrument
US8001051B1	2007-10-30	2011-08-16	United Services Automobile Association (Usaa)	Systems and methods to modify a negotiable instrument
US7996314B1	2007-10-30	2011-08-09	United Services Automobile Association	Systems and methods to modify a negotiable instrument

			(Usaa)	
US8046301B1	2007-10-30	2011-10-25	United Services Automobile Association (Usaa)	Systems and methods to modify a negotiable instrument
US7996316B1	2007-10-30	2011-08-09	United Services Automobile Association	Systems and methods to modify a negotiable instrument
US8290237B1	2007-10-31	2012-10-16	United Services Automobile Association (Usaa)	Systems and methods to use a digital camera to remotely deposit a negotiable instrument
US8320657B1	2007-10-31	2012-11-27	United Services Automobile Association (Usaa)	Systems and methods to use a digital camera to remotely deposit a negotiable instrument
US7900822B1	2007-11-06	2011-03-08	United Services Automobile Association (Usaa)	Systems, methods, and apparatus for receiving images of one or more checks
US7896232B1	2007-11-06	2011-03-01	United Services Automobile Association (Usaa)	Systems, methods, and apparatus for receiving images of one or more checks
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US20090164373A1 *	2007-12-21	2009-06-25	Mastercard International, Inc.	System and Method of Preventing Password Theft
US10380562B1	2008-02-07	2019-08-13	United Services Automobile Association (Usaa)	Systems and methods for mobile deposit of negotiable instruments
US8214298B2 *	2008-02-26	2012-07-03	Rfinity Corporation	Systems and methods for performing wireless financial transactions
US20090307140A1 *	2008-06-06	2009-12-10	Upendra Mardikar	Mobile device over-the-air (ota) registration and point-of-sale (pos) payment
US8543091B2	2008-06-06	2013-09-24	Ebay Inc	Secure short message service (SMS) communications
US8351678B1	2008-06-11	2013-01-08	United Services Automobile Association (Usaa)	Duplicate check detection
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US7698222B1 *	2008-09-02	2010-04-13	United Services Automobile Association (Usaa)	Systems and methods of check re-presentment deterrent
US7620604B1 *	2008-09-02	2009-11-17	United Services Automobile Association (Usaa)	Systems and methods of check re-presentment deterrent
US8422758B1	2008-09-02	2013-04-16	United Services Automobile Association (Usaa)	Systems and methods of check re-presentment deterrent
US10504185B1	2008-09-08	2019-12-10	United Services Automobile Association (Usaa)	Systems and methods for live video financial deposit
US7885880B1	2008-09-30	2011-02-08	United Services Automobile Association (Usaa)	Atomic deposit transaction
US8275710B1	2008-09-30	2012-09-25	United Services Automobile Association (Usaa)	Systems and methods for automatic bill pay enrollment
US7974899B1	2008-09-30	2011-07-05	United Services Automobile Association (Usaa)	Atomic deposit transaction
US7962411B1	2008-09-30	2011-06-14	United Services Automobile Association (Usaa)	Atomic deposit transaction
EP2175454B1 *	2008-10-13	2012-12-12	Vodafone Holding GmbH	Method and terminal for providing controlled access to a memory card
US8391599B1	2008-10-17	2013-03-05	United Services Automobile Association (Usaa)	Systems and methods for adaptive binarization of an image
US7949587B1	2008-10-24	2011-05-24	United States Automobile Association (USAA)	Systems and methods for financial deposits by electronic message
US7970677B1	2008-10-24	2011-06-28	United Services Automobile Association (Usaa)	Systems and methods for financial deposits by electronic message
US8452689B1	2009-02-18	2013-05-28	United Services Automobile Association (Usaa)	Systems and methods of check detection
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
US10956728B1	2009-03-04	2021-03-23	United Services Automobile Association (Usaa)	Systems and methods of check processing with background removal

US8332329B1 *	2009-04-22	2012-12-11	United Services Automobile Association (Usaa)	Virtual check
US8542921B1	2009-07-27	2013-09-24	United Services Automobile Association (Usaa)	Systems and methods for remote deposit of negotiable instrument using brightness correction
US9779392B1	2009-08-19	2017-10-03	United Services Automobile Association (Usaa)	Apparatuses, methods and systems for a publishing and subscribing platform of depositing negotiable instruments
US8977571B1	2009-08-21	2015-03-10	United Services Automobile Association (Usaa)	Systems and methods for image monitoring of check during mobile deposit
US8699779B1	2009-08-28	2014-04-15	United Services Automobile Association (Usaa)	Systems and methods for alignment of check during mobile deposit
MX2009009454A *	2009-09-03	2011-03-11	Compracel S A De C V Star	Payment methods using electronic devices.
JP4905577B2 *	2010-04-22	2012-03-28	株式会社デンソー	Communication system, transmitter, receiver, transceiver
US9129340B1	2010-06-08	2015-09-08	United Services Automobile Association (Usaa)	Apparatuses, methods and systems for remote deposit capture with enhanced image detection
KR20120040880A *	2010-10-20	2012-04-30	삼성전자주식회사	Device and method for controlling gprc charge payment in wireless terminal
KR101807764B1 *	2010-12-31	2018-01-19	주식회사 케이티	Method and system for providing financial service
US20130046698A1 *	2011-08-16	2013-02-21	Icertify Llc	System and method of creating and authenticating a secure financial instrument
JP5824977B2 *	2011-08-31	2015-12-02	株式会社リコー	Key pair management program, key pair management method, and image forming apparatus
EP2613287B1 *	2012-01-04	2017-12-06	Barclays Bank PLC	Computer system and method for initiating payments based on cheques
US10380565B1	2012-01-05	2019-08-13	United Services Automobile Association (Usaa)	System and method for storefront bank deposits
CN102903044A *	2012-09-03	2013-01-30	中国工商银行股份有限公司	Banking mobile terminal data signature device, banking mobile terminal data signature method and safety authentication system
US10552810B1	2012-12-19	2020-02-04	United Services Automobile Association (Usaa)	System and method for remote deposit of financial instruments
US11138578B1	2013-09-09	2021-10-05	United Services Automobile Association (Usaa)	Systems and methods for remote deposit of currency
GB2519076A *	2013-10-08	2015-04-15	A Men Technology Corp	Point transaction system and method for mobile communication device
US9286514B1	2013-10-17	2016-03-15	United Services Automobile Association (Usaa)	Character count determination for a digital image
WO2016074124A1 *	2014-11-10	2016-05-19	Hong Kong R & D Centre for Logistics and Supply Chain Management Enabling Technologies Limited	A system and method for facilitating a financial transaction between a payer and a payee
WO2016076807A1	2014-11-12	2016-05-19	Kkb-Kredi Kayit Burosu Anonim Sirketi	Management system for payment by electronic cheque and a method thereof
US10402790B1	2015-05-28	2019-09-03	United Services Automobile Association (Usaa)	Composing a focused document image from multiple image captures or portions of multiple image captures
US10715583B2	2016-02-12	2020-07-14	Visa International Service Association	Network topology
US10693658B2 *	2016-02-12	2020-06-23	Visa International Service Association	Methods and systems for using digital signatures to create trusted digital asset transfers
US11108566B2	2016-02-12	2021-08-31	Visa International Service Association	Methods and systems for using digital signatures to create trusted digital asset transfers
US20180025344A1 *	2016-07-25	2018-01-25	Ca, Inc	Communicating authentication information between mobile devices
US10484178B2 *	2016-10-26	2019-11-19	Black Gold Coin, Inc.	Systems and methods for providing a universal decentralized solution for verification of users with cross-verification features
US10749681B2	2016-10-26	2020-08-18	Black Gold Coin, Inc.	Systems and methods for providing a universal decentralized solution for verification of users with cross-verification features
US11030752B1	2018-04-27	2021-06-08	United Services Automobile Association (Usaa)	System, computing device, and method for document detection

SE1951426A1 *	2019-12-11	2021-06-12	Trust Anchor Group ipr Ab	Method for performing an offline transaction
WO2021150218A1 *	2020-01-22	2021-07-29	Visa International Service Association	System and method for revocable peer-to-peer payments

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
CN1653751A	2005-08-10	A method of processing an electronic payment cheque
CN100539747C	2009-09-09	Authentication and check SMS method for communicating
US8166299B2	2012-04-24	Secure messaging
US7245902B2	2007-07-17	Secure messaging via a mobile communications network
US7634280B2	2009-12-15	Method and system for authenticating messages exchanged in a communications system
US10158491B2	2018-12-18	Qualified electronic signature system, method and mobile processing terminal for qualified electronic signature
EP1387239B1	2018-04-04	Secure messaging
RU2411670C2	2011-02-10	Method to create and verify authenticity of electronic signature
US20060053280A1	2006-03-09	Secure e-mail messaging system
CN1744489A	2006-03-08	Providing certificate matching in a system and method for searching and retrieving certificates
US20070168432A1	2007-07-19	Use of service identifiers to authenticate the originator of an electronic message
CN1764922A	2006-04-26	Message settings selection
CN1700699A	2005-11-23	Method of providing a signing key for digitally signing verifying or encrypting data and mobile terminal
TWI555383B	2016-10-21	Method for recording and certifying the reception of e-mail
CN1977559A	2007-06-06	Method and system for protecting information exchanged during communication between users
CN106921639A	2017-07-04	Mobile digital certificate application method and device
KR20200077512A	2020-06-30	Platform and method for authenticating electronic announcements for electronic identity verification and authentication services (EIDAS)
TW200806002A	2008-01-16	Message authentication system and message authentication method
KR20200076674A	2020-06-29	Platform and method for authenticating electronic contracts for electronic identity verification and authentication services (EIDAS)
GB2384396A	2003-07-23	Authentication messaging in a mobile communications network
EP2378800B1	2018-02-14	Secure communication system
WO2011030352A2	2011-03-17	System and method for mobile phone resident digital signing and encryption/decryption of sms
Nyaketcho	2014	STK implementation in SMS banking in M-pesa-Kenya, exploits and feasible solutions
CN1905442A	2007-01-31	System and method for processing messages being composed by a user
EP2079208A1	2009-07-15	Systems and methods for server aided processing of a signed receipt

Priority And Related Applications

Priority Applications (2)

Application	Priority date	Filing date	Title
DKPA200200387		2002-03-13	
DKPA200200387		2002-03-13	

Legal Events

Date	Code	Title	Description
2005-08-10	P801	Publication	

2005-08-10	C06	Publication	
2005-10-05	SE01	Entry into force of request for substantive examination	
2005-10-05	C10	Entry into substantive examination	
2008-02-06	TA01	Transfer of patent application right	**Effective date of registration:** 20080104 **Address after:** Aarhus **Applicant after:** Encryption solutions, Limited by Share Ltd **Address before:** Denmark and Rupp **Applicant before:** Beamtrust AS
2008-02-06	ASS	Succession or assignment of patent right	**Owner name:** ENCRYPTED SOLUTION STOCK CO., LTD. **Free format text:** FORMER OWNER: BEAM TRUST CO., LTD. **Effective date:** 20080104
2008-02-06	C41	Transfer of patent application or patent right or utility model	
2010-07-14	WD01	Invention patent application deemed withdrawn after publication	**Open date:** 20050810
2010-07-14	C02	Deemed withdrawal of patent application after publication (patent law 2001)	

About Send Feedback Public Datasets Terms Privacy Policy

Patents CH690048

Safety device controlling access to a computer or a network terminal.

Classifications

G07F7/1008 Active credit-cards provided with means to personalise their use, e.g. with PIN-introduction/comparison system

View 6 more classifications

CH690048A5
Switzerland

Download PDF Find Prior Art Similar

Other languages: French

Inventor: Yvan Korshun

Worldwide applications

1995 CH 1996 AT EP DE US

Application CH03375/95A events

1995-11-28 Application filed by C Sam S A En Formation C O Jue

1995-11-28 Priority to CH03375/95A

2000-03-31 Publication of CH690048A5

Info: Patent citations (15), Cited by (137), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (9)

Hide Dependent

1. Security device controlling access to a computer or to a network terminal provided with means allowing its use only using an access code, characterized in that said access code is carried by a portable support intended to be placed in the presence of a detector connected to said computer or network terminal, the authorized user, carrying said code support, not necessarily having to know the latter.

2. Security device according to claim 1, characterized in that the code support comprises means for reading or detecting biometric characters of the authorized user.

3. Security device according to claim 1, characterized in that the access code is contained in the memory of a computer chip card constituting said portable code carrier.

4.

Security device according to claim 1, characterized in that the access code detector is mounted on an element external to the computer or the network terminal, but connected to it.

5. Security device according to claim 4, characterized in that the detector of the access code is carried by a mouse connected to the computer or to the network terminal.

6. Security device according to claim 4, characterized in that the access code detector is carried by a keyboard connected to the computer or to the network terminal.

7. Security device according to claim 1, characterized in that the access code detector is mounted on the computer or on the network terminal itself.

8

Security device according to claim 1, characterized in that the access code detector comprises an antenna so that the reading can be carried out without necessarily having any physical contact between the support of the code access and said reader.

9. Security device according to claim 1, characterized in that the detector of the access code and the support thereof both include conductive areas so that the reading of the code access can only be made when the respective conductive areas are in contact with each other.

Description

The present invention relates to a security device controlling access to a computer or to a network terminal provided with means allowing its use only using an access code.

Such safety devices are known per se. In these known devices, the user of the computer or of the network terminal who is authorized knows the access code and enters it into the computer or the network terminal using the keyboard provided with the latter. .

This operational mode does not exclude abusive uses due, in particular, to indiscretions that the authorized user could commit.

The object of the present invention is to remedy this drawback by providing means so that the access code can be entered into the computer or the network terminal without the authorized user even having to know this code.

In practice, it will be the rule that, precisely, the user does not know this code.

This object is achieved by the means defined in claim 1.

The drawing represents, by way of example, an embodiment of the subject of the invention.

Fig. 1 is a perspective view of a personal computer.
Fig. 2 is a view of a detail, and
Fig. 3 schematically illustrates the operational principle of this computer.

The personal computer (PC) shown in fig. 1 is generally designated by 1. It is surmounted by its display screen 2. A program diskette ready to be engaged in computer 1 has been represented at 3. A mouse, connected to computer 1 by a cable 4, is represented at 5. This mouse is provided with an antenna 6 and with an information reader or detector 7 connected to said antenna (fig. 2)

The installation also includes a set of smart cards 8, the memory of which contains a computer access code 1.

The installation diagram illustrated in fig. 3, where the elements appear in the form of blocks, comprises a peripheral 9 representing all the usual peripherals of a personal computer (hard disk, programs, files, networks), a set 10, comprising a basic input-output system (basic input-output system BIOS) 11, a memory 12 and a microprocessor (au P) 13. The program diskette 3 is also visible in this figure as well as the mouse 5 and two user chip cards 8.

The present installation is used as follows: each authorized user will be provided with a smart card 8 which he will present, when he wishes to use the computer 1, next to the mouse 5. The access code contained in the memory of the smart card 8 will be detected by the antenna 6 of the mouse 5 and transmitted by the driver 4 to the computer 1. The latter will compare the access code of the card 8 with the access code contained in its memory 12 and, if there is identity, will release the blockage produced by its security device so that it can then be used.

The user (s) will not have to know and, in principle, will not have to know the access code, which will prevent indiscretions from being committed.

In order to increase security, the user cards 8 may be provided with means for detecting biometric characters of each of the users, for example the fingerprint of their index. Each user will then have to place their index on said detection means so that the access code can be recognized by the computer. Thus, any misuse of user cards by unauthorized persons will be excluded.

In order to ensure great flexibility in the use of this installation, any data relating to the access code or the personal biometric code of the users may be entered into the computer memory by presenting new access cards to the mouse 5 while inserting a master card into the computer without which the data contained in the computer memory could not be modified.

The media of the access code may not consist of user cards but by any other portable means such as badges, watches, electronic agendas, or the like.

In the example described and shown, the detector of the access code is carried by the mouse, which has the advantage that the computer itself does not have to undergo modifications so that the device according to the invention can be applied to it, especially since the conductor 4 connecting the mouse to the computer will be the ordinary conductor that the mice contain. It will suffice that the reader 7 of the mouse comprises switching means such that as soon as a user card is presented to the mouse, it is the information relating to the access code which is transmitted to the computer whereas, as soon as the user card is no longer located in the area of influence of the antenna 6, it is the ordinary information provided by the usual mice, produced by their rotating sphere, which is transmitted to the computer.

The means of detecting or reading the access code may also be mounted on other elements separate from the computer than the mouse, for example on a keyboard for entering data into the computer, on a printer controlled by the computer or a modem, for example. These reading means can also be integrated into the computer itself.

Similarly, in the example described and shown, the reading is carried out remotely, without material contact between the reader and the portable medium of the access code, by means of an antenna. But it could also be envisaged that the support of the access code and the detection means comprise conductive zones which will have to be brought into material contact so that the access code can be read.

It should be noted that the data contained in the access code carriers may not be all identical, but may include information elements specific to each user in such a way that they are not all able to access all the functions of the computer or of the network terminal, and that access is thus "selective".

Provision may be made for the computer or the network terminal to be arranged in such a way that the user is obliged to represent his access card during the operations he performs in order to prevent an unauthorized user from replacing himself, to the authorized user during use.

The present invention will include a very large number of applications: Telebanking, Videotex, Internet databases, etc. It can be applied to any equipment comprising an integrated computer, such as a photocopier, any machine or other.

Patent Citations (15)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
SE4257048B *	1981-03-18	1982-10-25	Loefberg Bo	DATABERARE
JPS62251963A *	1986-04-25	1987-11-02	Casio Comput Co Ltd	Certificating system for ic card
IS3386A7 *	1987-10-02	1988-11-28	Ranjit Senanayake Daya	Human identification system
JPH025195A *	1988-06-23	1990-01-10	Omron Tateisi Electron Co	Ic card
US5187352A *	1989-01-03	1993-02-16	William Blair	Microprocessor controlled security system for computers
US4901068A *	1989-01-17	1990-02-13	Moneyfax, Inc.	Identification apparatus for operating secure equipment
US5130519A *	1990-01-16	1992-07-14	George Bush	Portable pin card
DE4015482C1 *	1990-05-14	1991-07-25	Competence Center Informatik Gmbh, 4470 Meppen, De	User authenticating system for data processing terminal - contactlessly interrogates identification disc worn by user
DE59209256D1 *	1991-01-22	1998-05-07	Skidata Ag	Device for authorizing the operation of a device with an actuation unit
AU3777593A *	1992-02-26	1993-09-13	Paul C. Clark	System for protecting computers via intelligent tokens or smart cards

JP2746801B2 *	1992-08-27	1998-05-06	三菱電機株式会社	IC card and password verification method for IC card
US5355414A *	1993-01-21	1994-10-11	Ast Research, Inc.	Computer security system
FR2717931B1 *	1994-03-23	1996-05-31	Gemplus Card Int	Identity verification system.
DE19508288A1 *	1995-03-09	1995-10-05	Peter Prof Dr Ing Lieli	Prevention of unauthorised access to computer system
US5724027A *	1995-09-28	1998-03-03	Intel Corporation	Method and apparatus for providing system security to personal computer systems using transparent system interrupt

* Cited by examiner, † Cited by third party

Cited By (137)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US10361802B1	1999-02-01	2019-07-23	Blanding Hovenweep, Llc	Adaptive pattern recognition based control system and method
KR19990012099A *	1997-07-26	1999-02-25	윤종용	User verification method using e-resident card
US6087928A	1997-11-13	2000-03-14	Imageworks Manufacturing, Inc.	System and method for providing restrained, streamlined access to a computerized information source
GB2333619A *	1998-01-07	1999-09-22	Ian David Evans	Security system detects user proximity to computer apparatus
US6615189B1	1998-06-22	2003-09-02	Bank One, Delaware, National Association	Debit purchasing of stored value card for use by and/or delivery to others
US7809642B1	1998-06-22	2010-10-05	Jpmorgan Chase Bank, N.A.	Debit purchasing of stored value card for use by and/or delivery to others
US6360953B1 *	1998-07-15	2002-03-26	Magnex Corporation	Secure print sensing smart card with on-the-fly-operation
US6032136A	1998-11-17	2000-02-29	First Usa Bank, N.A.	Customer activated multi-value (CAM) card
US7660763B1	1998-11-17	2010-02-09	Jpmorgan Chase Bank, N.A.	Customer activated multi-value (CAM) card
US6792464B2 *	1999-02-18	2004-09-14	Colin Hendrick	System for automatic connection to a network
USD433413S *	1999-04-09	2000-11-07	Biolink Technologies International, Inc.	Biometric scanning aperture for a computer input device
US6282304B1	1999-05-14	2001-08-28	Biolink Technologies International, Inc.	Biometric system for biometric input, comparison, authentication and access control and method therefor
US6882984B1	1999-06-04	2005-04-19	Bank One, Delaware, National Association	Credit instrument and system with automated payment of club, merchant, and service provider fees
US7058817B1	1999-07-02	2006-06-06	The Chase Manhattan Bank	System and method for single sign on process for websites with multiple applications and services
WO2001033477A2	1999-11-04	2001-05-10	Jpmorgan Chase Bank	System and method for automated financial project management
US10275780B1	1999-11-24	2019-04-30	Jpmorgan Chase Bank, N.A.	Method and apparatus for sending a rebate via electronic mail over the internet
US8571975B1	1999-11-24	2013-10-29	Jpmorgan Chase Bank, N.A.	System and method for sending money via E-mail over the internet
WO2001041032A1	1999-11-30	2001-06-07	David Russell	Methods, systems, and apparatuses for secure interactions
US8799160B2	1999-12-07	2014-07-29	Steve Sorem	System and method for processing transactions
US6564998B1 *	2000-01-25	2003-05-20	Hewlett-Packard Development Company	Card enabled latch for a portable computer
US6686778B1	2000-02-15	2004-03-15	Bank One, Delaware, National Association	System and method for generating graphical user interfaces
US6941279B1	2000-02-23	2005-09-06	Banke One Corporation	Mutual fund card method and system
GB2360610A *	2000-03-22	2001-09-26	Newmark Technology Group Plc	Computer access control and security system
US20030172027A1 *	2001-03-23	2003-09-11	Scott Walter G.	Method for conducting a credit transaction using biometric information
WO2001088859A2 *	2000-05-18	2001-11-22	Stefaan De Schrijver	Smartchip biometric device

AU6177501A *	2000-05-18	2001-11-26	Stefaan De Schrijver	Apparatus and method for secure object access
AU6179501A *	2000-05-22	2001-12-03	Stefaan De Schrijver	Electronic cartridge writing instrument
US7426530B1	2000-06-12	2008-09-16	Jpmorgan Chase Bank, N.A.	System and method for providing customers with seamless entry to a remote server
AU7358401A *	2000-06-16	2001-12-24	Stefaan De Schrijver	Piezo sensor peripheral device
US10185936B2	2000-06-22	2019-01-22	Jpmorgan Chase Bank, N.A.	Method and system for processing internet payments
US7831508B1	2000-06-23	2010-11-09	Jpmorgan Chase Bank, N.A.	System and method for implementing a consolidated application process
WO2002011019A1	2000-08-01	2002-02-07	First Usa Bank, N.A.	System and method for transponder-enabled account transactions
US7747866B1	2000-08-24	2010-06-29	Jpmorgan Chase Bank, N.A.	System and method providing improved error detection related to transmission of data over a communication link
US8335855B2	2001-09-19	2012-12-18	Jpmorgan Chase Bank, N.A.	System and method for portal infrastructure tracking
AU736796B3 *	2000-09-27	2001-08-02	Comgeer Pty Ltd	Computer-type peripherals
US6631849B2	2000-12-06	2003-10-14	Bank One, Delaware, National Association	Selectable multi-purpose card
US6985873B2	2001-01-18	2006-01-10	First Usa Bank, N.A.	System and method for administering a brokerage rebate card program
WO2007044600A2	2005-10-06	2007-04-19	C-Sam, Inc.	Transactional services
US20140089120A1	2005-10-06	2014-03-27	C-Sam, Inc.	Aggregating multiple transaction protocols for transacting between a plurality of distinct payment acquiring devices and a transaction acquirer
US10176476B2	2005-10-06	2019-01-08	Mastercard Mobile Transactions Solutions, Inc.	Secure ecosystem infrastructure enabling multiple types of electronic wallets in an ecosystem of issuers, service providers, and acquires of instruments
US7181017B1	2001-03-23	2007-02-20	David Felsher	System and method for secure three-party communications
US8849716B1	2001-04-20	2014-09-30	Jpmorgan Chase Bank, N.A.	System and method for preventing identity theft or misuse by restricting access
US7313546B2	2001-05-23	2007-12-25	Jp Morgan Chase Bank, N.A.	System and method for currency selectable stored value instrument
AU2002312381A1	2001-06-07	2002-12-16	First Usa Bank, N.A.	System and method for rapid updating of credit information
WO2003001363A1	2001-06-25	2003-01-03	Jp Morgan Chase Bank	Electronic vouchers and a system and method for issuing the same
US7266839B2	2001-07-12	2007-09-04	J P Morgan Chase Bank	System and method for providing discriminated content to network users
AU2002327922A1	2001-07-24	2003-02-17	First Usa Bank, N.A.	Multiple account card and transaction routing
US7809641B2	2001-07-26	2010-10-05	Jpmorgan Chase Bank, National Association	System and method for funding a collective account
US7311244B1	2001-08-13	2007-12-25	Jpmorgan Chase Bank, N.A.	System and method for funding a collective account by use of an electronic tag
US8800857B1	2001-08-13	2014-08-12	Jpmorgan Chase Bank, N.A.	System and method for crediting loyalty program points and providing loyalty rewards by use of an electronic tag
US8020754B2	2001-08-13	2011-09-20	Jpmorgan Chase Bank, N.A.	System and method for funding a collective account by use of an electronic tag
US7103576B2	2001-09-21	2006-09-05	First Usa Bank, Na	System for providing cardless payment
US20030229811A1 *	2001-10-31	2003-12-11	Cross Match Technologies, Inc	Method that provides multi-tiered authorization and identification
EP1444568A4	2001-11-01	2005-11-09	Bank One Delaware Nat Ass	System and method for establishing or modifying an account with user selectable terms
US7987501B2	2001-12-04	2011-07-26	Jpmorgan Chase Bank, N.A.	System and method for single session sign-on
US7941534B2	2002-02-19	2011-05-10	Jpmorgan Chase Bank, N.A.	System and method for single sign-on session management without central server
JP4137468B2 *	2002-02-27	2008-08-20	富士通株式会社	Program usage authentication method
US8392301B1	2002-03-08	2013-03-05	Jpmorgan Chase Bank,	Financial system for isolated economic environment

			N.A.	
US7756896B1	2002-03-11	2010-07-13	Jp Morgan Chase Bank	System and method for multi-dimensional risk analysis
US7204425B2	2002-03-18	2007-04-17	Precision Dynamics Corporation	Enhanced identification appliance
US20180165441A1	2002-03-25	2018-06-14	Glenn Cobourn Everhart	Systems and methods for multifactor authentication
US7899753B1	2002-03-25	2011-03-01	Jpmorgan Chase Bank, N.A	Systems and methods for time variable financial authentication
US20040210498A1	2002-03-29	2004-10-21	Bank One, National Association	Method and system for performing purchase and other transactions using tokens with multiple chips
AU2003230751A1	2002-03-29	2003-10-13	Bank One, Delaware, N.A.	System and process for performing purchase transaction using tokens
WO2004008282A2 *	2002-07-12	2004-01-22	Privaris, Inc.	Personal authentication software and systems for travel privilege assignation and verification
US8229804B1	2002-07-29	2012-07-24	Jpmorgan Chase Bank, N.A.	Method and system for providing pre-approved targeted products
CA2494299C	2002-08-06	2013-10-08	Privaris, Inc.	Methods for secure enrollment and backup of personal identity credentials into electronic devices
CZ2005209A3 *	2002-09-10	2005-12-14	Ivi Smart Technologies, Inc.	Safe biometric verification of identity
US7809595B2	2002-09-17	2010-10-05	Jpmorgan Chase Bank, Na	System and method for managing risks associated with outside service providers
US7058660B2	2002-10-02	2006-06-06	Bank One Corporation	System and method for network-based project management
JP2004132890A *	2002-10-11	2004-04-30	Fujitsu Component Ltd	Noncontact ic card reader/writer apparatus, noncontact ic card, input apparatus, and noncontact method for computing position of ic card
US20040122736A1	2002-10-11	2004-06-24	Bank One, Delaware, N.A.	System and method for granting promotional rewards to credit account holders
AU2003280369A1 *	2002-10-14	2004-05-04	Volker Budde	Access card for testing access authorisation to a security system
US8301493B2	2002-11-05	2012-10-30	Jpmorgan Chase Bank, N.A.	System and method for providing incentives to consumers to share information
US9818136B1	2003-02-05	2017-11-14	Steven M. Hoffberg	System and method for determining contingent relevance
WO2004109455A2	2003-05-30	2004-12-16	Privaris, Inc.	An in-circuit security system and methods for controlling access to and use of sensitive data
US8306907B2	2003-05-30	2012-11-06	Jpmorgan Chase Bank N.A.	System and method for offering risk-based interest rates in a credit instrument
US6983882B2 *	2003-09-02	2006-01-10	Cheng-Fu Weng	Portable wireless anti-theft USB disc
US7953663B1	2003-09-04	2011-05-31	Jpmorgan Chase Bank, N.A.	System and method for financial instrument pre-qualification and offering
DE20314722U1 *	2003-09-23	2005-02-10	Scm Microsystems Gmbh	Device for secure access to digital media content, virtual multi-interface driver and system for secure access to digital media content
US8239323B2	2003-09-23	2012-08-07	Jpmorgan Chase Bank, N.A.	Method and system for distribution of unactivated bank account cards
US8190893B2	2003-10-27	2012-05-29	Jp Morgan Chase Bank	Portable security transaction protocol
US7742997B1	2004-04-23	2010-06-22	Jpmorgan Chase Bank, N.A.	System and method for management and delivery of content and rules
US8918900B2 *	2004-04-26	2014-12-23	Ivi Holdings Ltd.	Smart card for passport, electronic passport, and method, system, and apparatus for authenticating person holding smart card or electronic passport
WO2005119607A2 *	2004-06-03	2005-12-15	Tyfone, Inc.	System and method for securing financial transactions
US20050269401A1 *	2004-06-03	2005-12-08	Tyfone, Inc.	System and method for securing financial transactions
US7392222B1	2004-08-03	2008-06-24	Jpmorgan Chase Bank, N.A.	System and method for providing promotional pricing
US20060181243A1 *	2005-02-11	2006-08-17	Nortel Networks Limited	Use of location awareness to facilitate clinician-charger interaction in a healthcare environment
US8929528B2 *	2005-02-11	2015-01-06	Rockstar Consortium Us Lp	Method and system for enhancing collaboration

US8050939B2 *	2005-02-11	2011-11-01	Avaya Inc.	Methods and systems for use in the provision of services in an institutional setting such as a healthcare facility
US7966008B2 *	2005-02-11	2011-06-21	Avaya Inc.	Use of location awareness to control radio frequency interference in a healthcare environment
US7676380B2 *	2005-02-11	2010-03-09	Nortel Networks Limited	Use of location awareness to establish and suspend communications sessions in a healthcare environment
US7707044B2 *	2005-02-11	2010-04-27	Avaya Inc.	Use of location awareness to transfer communications sessions between terminals in a healthcare environment
US7801743B2 *	2005-02-11	2010-09-21	Avaya Inc.	Use of location awareness of establish communications with a target clinician in a healthcare environment
US8180065B2 *	2005-02-11	2012-05-15	Avaya Inc.	Use of location awareness to request assistance for a medical event occurring in a healthcare environment
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
US8630898B1	2005-02-22	2014-01-14	Jpmorgan Chase Bank, N.A.	Stored value card provided with merchandise as rebate
EP1861807B1	2005-03-24	2012-11-07	Privaris, Inc.	Biometric identification device with smartcard capabilities
US20060226217A1 *	2005-04-07	2006-10-12	Tyfone, Inc.	Sleeve for electronic transaction card
US7401731B1	2005-05-27	2008-07-22	Jpmorgan Chase Bank, Na	Method and system for implementing a card product with multiple customized relationships
US8185877B1	2005-06-22	2012-05-22	Jpmorgan Chase Bank, N.A.	System and method for testing applications
US8847794B2 *	2005-07-15	2013-07-02	Tyfone, Inc.	Symmetric cryptography with user authentication
US8139788B2 *	2005-07-15	2012-05-29	Tyfone, Inc.	Hybrid symmetric/asymmetric cryptography with user authentication
US7805615B2 *	2005-07-15	2010-09-28	Tyfone, Inc.	Asymmetric cryptography with user authentication
CN101213559B *	2005-08-05	2012-02-29	夏普株式会社	Communication device and communication system
US8583926B1	2005-09-19	2013-11-12	Jpmorgan Chase Bank, N.A.	System and method for anti-phishing authentication
US8874477B2	2005-10-04	2014-10-28	Steven Mark Hoffberg	Multifactorial optimization system and method
US8408456B1	2006-02-08	2013-04-02	Jpmorgan Chase Bank, N.A.	System and method for granting promotional rewards to both customers and non-customers
US7753259B1	2006-04-13	2010-07-13	Jpmorgan Chase Bank, N.A.	System and method for granting promotional rewards to both customers and non-customers
US7784682B2	2006-02-08	2010-08-31	Jpmorgan Chase Bank, N.A.	System and method for granting promotional rewards to both customers and non-customers
US8793490B1	2006-07-14	2014-07-29	Jpmorgan Chase Bank, N.A.	Systems and methods for multifactor authentication
US7991158B2	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
JP2010516002A	2007-01-09	2010-05-13	ビザ ユー．エス．エー．インコーポレイテッド	Contactless transaction
US20080222573A1 *	2007-03-06	2008-09-11	Simon Abeckaser	Computer mouse with cursor finding function and faster screen privacy function
US20100131414A1 *	2007-03-14	2010-05-27	Gavin Randall Tame	Personal identification device for secure transactions
US8347378B1	2007-05-17	2013-06-25	Jpmorgan Chase	Systems and methods for managing digital certificates
US8676642B1	2007-07-05	2014-03-18	Jpmorgan Chase Bank, N.A.	System and method for granting promotional rewards to financial account holders
TWI617986B	2007-09-24	2018-03-11	蘋果公司	Embedded authentication systems in an electronic device
US8417601B1	2007-10-18	2013-04-09	Jpmorgan Chase Bank, N.A.	Variable rate payment card
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
US8321682B1	2008-01-24	2012-11-27	Jpmorgan Chase Bank, N.A.	System and method for generating and managing administrator passwords

USD635186S1	2008-06-30	2011-03-29	Jpmorgan Chase Bank, N.A.	Metal transaction device
US9305292B1	2008-07-03	2016-04-05	Jpmorgan Chase Bank, N.A.	Systems and methods for providing an adaptable transponder device
USD636021S1	2008-07-17	2011-04-12	Jpmorgan Chase Bank, N.A.	Eco-friendly transaction device
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
US9608826B2	2009-06-29	2017-03-28	Jpmorgan Chase Bank, N.A.	System and method for partner key management
US8582829B2	2010-11-03	2013-11-12	Gary S. Shuster	Online identity verification
IN2014KN00998A	2011-10-12	2015-09-04	C Sam Inc	
US10007906B2	2011-11-17	2018-06-26	Abdolreza Behjat	Using a mobile device in a commercial transaction
GB2509495A *	2013-01-02	2014-07-09	Knightsbridge Portable Comm Sp	Device and system for user authentication to permit access to an electronic device
US9419957B1	2013-03-15	2016-08-16	Jpmorgan Chase Bank, N.A.	Confidence-based authentication
US10148726B1	2014-01-24	2018-12-04	Jpmorgan Chase Bank, N.A.	Initiating operating system commands based on browser cookies
USD776664S1 *	2015-05-20	2017-01-17	Chaya Coleena Hendrick	Smart card
US10868672B1	2015-06-05	2020-12-15	Apple Inc.	Establishing and verifying identity using biometrics while protecting user privacy
US11140171B1	2015-06-05	2021-10-05	Apple Inc.	Establishing and verifying identity using action sequences while protecting user privacy

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
EP0777171A1	1997-06-04	Security device for controlling access to a computer or a network terminal
AU2006307996B2	2011-05-19	Method and system for secure password/PIN input via mouse scroll wheel
US6509847B1	2003-01-21	Pressure password input device and method
US20070128899A1	2007-06-07	System and method for improving the efficiency, comfort, and/or reliability in Operating Systems, such as for example Windows
US20050240756A1	2005-10-27	System and method for improving the efficiency, comfort, and/or reliability in Operating Systems, such as for example Windows
EP0395749A1	1990-11-07	Method and device for the protection and universalization of a software
US20140115723A1	2014-04-24	System and Method for Digital Media Distribution
Kershner et al.	1994	An experimental sound-based hierarchical menu navigation system for visually handicapped use of graphical user interfaces
FR2834366A1	2003-07-04	SELF-LOCKING CHIP CARD, DEVICE FOR SECURING SUCH A CARD AND RELATED METHODS
WO2002039394A1	2002-05-16	Computer system for offering for sale and selling articles of a shop
Drumm et al.	1997	The Cybermobile: A Gateway for Public Access to Network-Based Information.
EP0946918B1	2002-10-09	Portable electronic device with display screen along several directions
WO2003040984A1	2003-05-15	Universal mobile interactive information equipment that is used, in particular, to monitor dependent elderly people
FR2738070A1	1997-02-28	Mouse type pointer for use as peripheral with computer
WO2000014655A3	2000-06-02	Function key for computer data handling
Cox	1997	Applying design metrics to object-oriented systems
Rhonemus	1998	Reagents for protein analysis and modification
Doyle	1991	A guide for the selection and maintenance of computer peripherals

Hass	1978	Bloc voting in black precincts in Muncie and its political impact during the 1967, 1971 and 1975 mayoral primary and general elections
Schoen	1980	Interactive IMGRID, direct communication with a geographic information system
Smith	1996	Water table fluctuation in an East Central Indiana toposequence
Smigielski et al.	1996	A systematic satellite approach for estimating central surface pressures of mid-latitude cold season oceanic cyclones
Guidry	1992	Individual and structural explanations of inequality: the Black view
Jessup	1987	Eli Lilly and Conner Prairie
Mansfield	2002	Integrated thematic units for middle school ESL

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
CH03375/95A	1995-11-28	1995-11-28	Safety device controlling access to a computer or a network terminal.

Applications Claiming Priority (5)

Application	Filing date	Title
CH03375/95A	1995-11-28	Safety device controlling access to a computer or a network terminal.
EP96118144A	1996-11-13	Security device for controlling access to a computer or a network terminal
AT96118144T	1996-11-13	SECURITY DEVICE FOR CONTROLLING ACCESS TO A COMPUTER OR NETWORK TERMINAL
DE69613545T	1996-11-13	Security device for controlling access to a computer or network terminal
US08/752,575	1996-11-21	Security device for controlling the access to a personal computer or to a computer terminal

Legal Events

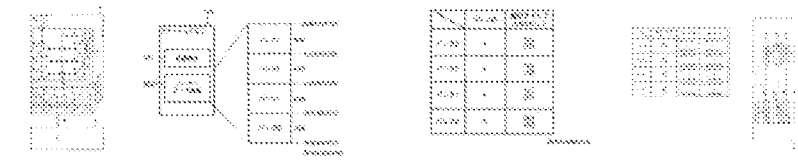
Date	Code	Title	Description
2002-07-15	PL	Patent ceased	

Data provided by IFI CLAIMS Patent Services

Patents JP4515793

Memory card device and memory card control method

Images (15)



Classifications

G06F12/0623 Address space extension for memory modules

View 2 more classifications

JP4515793B2
Japan

Download PDF Find Prior Art Family

Other languages: Japanese

Inventor: 大志 詰山, 哲也 高瀬, 昭雄 矢沢

Worldwide applications

2004 JP US

Application JP2004069424A events

2004-03-11 Application filed by 株式会社東芝, 東芝デジタルメディアエンジニアリング株式会社

2004-03-11 Priority to JP2004069424A

2005-09-22 Publication of JP2005258804A

2010-08-04 Application granted

2010-08-04 Publication of JP4515793B2

Status Expired - Fee Related

2024-03-11 Anticipated expiration

Info: Patent citations (12), Cited by (21), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (4)

Hide Dependent

1. In a memory card device that can be removably connected to a host device,
A host interface unit for executing a communication with the host device and receiving a command group including a memory access command with a memory address of a specific bit width transmitted from the host device;
A nonvolatile semiconductor memory having a storage area larger than the maximum memory size addressable by the memory address of the specific bit width,
Bank identification number management means for dividing the storage area of the nonvolatile semiconductor memory into a plurality of banks and managing a plurality of bank identification numbers corresponding to the plurality of banks, and
Bank designation means for designating one of the plurality of banks as an access target bank according to a bank identification number included in a bank designation command transmitted from the host device;
Memory control means for accessing one of the specified plurality of banks in response to the memory access command transmitted from the host device and accompanied by a memory address of the specific bit width ;
Card address generation means for generating a card address for identifying the memory card device in response to a card address generation command transmitted from the host device and transmitting the card address to the host device;
The bank identification number management means is generated by the card address generation means so that a bank identification number equal to the value of the generated card address is assigned to a specific one of the plurality of banks. A bank identification number corresponding to each of the plurality of banks is generated from the card address,
The bank designation command is a card selection command which is transmitted from the host device and changes the operation mode of the memory card device designated by the card address to a data transfer mode capable of executing data transfer with the host device. A memory card device characterized by the above.

2. In a memory card device that can be removably connected to a host device,
A host interface unit for executing a communication with the host device and receiving a command group including a memory access command with a memory address of a specific bit width transmitted from the host device,
A nonvolatile semiconductor memory having a storage area larger than the maximum memory size addressable by the memory address of the specific bit width;
Bank identification number management means for dividing the storage area of the nonvolatile semiconductor memory into a plurality of banks and managing a plurality of bank identification numbers corresponding to the plurality of banks, and
Bank designation means for designating one of the plurality of banks as an access target bank according to a bank identification number included in a bank designation command transmitted from the host device,
Memory control means for accessing one of the specified plurality of banks in response to the memory access command transmitted from the host device and accompanied by a memory address of the specific bit width,
The bank identification number management means is configured to generate a bank identification number corresponding to each of the plurality of banks from a card

address for identifying the memory card device.
The bank designation command includes a bank identification number generated from the card address transmitted from the host device, and a data transfer mode capable of executing data transfer between the operation mode of the memory card device and the host device. is a card selection command to transition to
The memory card device, wherein the bank designating unit is configured to designate one of the plurality of banks as an access target bank according to a bank identification number included in the card selection command.

3. In a memory card device that can be removably connected to a host device.
Communication with the host device is performed, and at least a card address generation command for requesting generation of a card address for identifying the memory card device, which is transmitted from the host device, and the memory card device are identified. A card selection command that includes a value generated from the card address for the bank identification number as a bank identification number and changes the operation mode of the memory card device to a transfer mode capable of executing data transfer with the host device, and a specific bit width A host interface unit for receiving a command group including a memory access command with a memory address;
A nonvolatile semiconductor memory having a storage area larger than the maximum memory size addressable by the memory address of the specific bit width;
In response to the card address generation command, card address generation means for generating the card address and transmitting it to the host device;
A bank that divides a storage area of the nonvolatile semiconductor memory into a plurality of banks, and manages values generated from the card addresses generated by the card address generation means as the bank identification numbers respectively corresponding to the plurality of banks An identification number management means;
Bank designation means for designating one of the plurality of banks as an access target bank in accordance with a bank identification number included in the card selection command;
Memory control means for accessing one of the designated plurality of banks in response to the memory access command transmitted from the host device and accompanied by the memory address having the specific bit width. Memory card device.

4. A memory card control method for controlling the operation of a memory card device detachably connectable to a host device.
Executing a communication with the host device and receiving a command group including a memory access command with a memory address of a specific bit width transmitted from the host device;
The storage area of the nonvolatile semiconductor memory having a storage area larger than the maximum memory size that can be addressed by the memory address of the specific bit width is divided into a plurality of banks, and the card address for identifying the memory card device is used. Generating a plurality of bank identification numbers assigned to each of the plurality of banks;
A card selection that includes a value generated from the card address transmitted from the host device as a bank identification number and changes the operation mode of the memory card device to a transfer mode capable of performing data transfer with the host device. In accordance with a command, a bank specifying step of specifying one of the plurality of banks as an access target bank;
Accessing one of the specified banks in response to the memory access command transmitted from the host device and accompanied by a memory address of the specific bit width. Card control method.

Description

The present invention relates to a memory card device that can be detachably connected to a host device and a control method thereof

In recent years, with the digitization of content data such as music and video, digital devices have been actively developed. Many of these digital devices include a storage device such as a compact disk drive or a hard disk drive for recording content data.

Recently, digital devices have been miniaturized. For example, in digital devices such as music players, products having a size of several centimeters square have appeared. In such a small digital device, it is necessary to reduce the size of the recording medium. As a small recording medium, a memory card incorporating a nonvolatile semiconductor memory has attracted attention.

As one type of such memory card, a memory card having a copyright protection function is known (for example, see Patent Document 1). This memory card has a revocation function for eliminating unauthorized devices as one of copyright protection functions.

An SD (Secure Digital) memory card is a memory card having a copyright protection function, and is equipped with a NAND flash EEPROM. This NAND flash EEPROM is a kind of nonvolatile semiconductor memory and can be electrically rewritten. NAND flash EEPROM is classified as flash memory. In the flash memory, the lowest area that can be erased by one erase operation is defined as an erase block, and data is always erased in units of erase blocks. Therefore, the flash memory is more suitable for recording a large-capacity file than a random access application in which data is frequently updated.
JP 2000-357126 A

However, in an SD memory card, there is an addressing method (hereinafter referred to as a byte unit addressing method) in which an access position is designated in byte units using a 32-bit width memory address attached to a memory access command from a host device. It's being used. Therefore, the upper limit of the memory size of the SD memory card is limited $^{2\,32}$ bytes, that is 4GB.

If an addressing method (hereinafter referred to as a block unit addressing method) in which an access position is specified in units of blocks in which a plurality of bytes are grouped instead of a byte unit addressing method is used, even if a 32-bit width memory address is used. Even in such a case, a memory address space of 4 GB or more can be accessed.

However, when the block unit addressing method is simply used, there arises a problem that compatibility with an existing host device that does not support the block unit addressing method cannot be maintained. That is, when data is written using the block unit addressing method, data groups constituting one file may be distributed and written in a memory address space exceeding 4 GB due to file fragmentation. This is because, for example, a memory card with an overall memory size of 8 GB is taken as an example, although a part of data constituting a file A exists in a position in the lower 4 GB in the memory space of 8 GB. In this situation, the data of the remaining part of the file A exists at a position in the upper 4 GB. As described above, when a data group constituting one file is distributed in a memory address space exceeding 4 GB, the existing host device that does not support the block unit addressing method but supports only the byte unit addressing method. Can no longer read the file correctly. This is because the maximum memory space accessible by the byte unit addressing method is 4 GB. Therefore, it is necessary to realize a new mechanism for expanding the memory space of the memory card.

The present invention has been made in consideration of the above-described circumstances, and it is possible to expand an accessible memory address space while maintaining compatibility with an existing host device that does not support the block unit addressing method. An object of the present invention is to provide a memory card device and a control method thereof.

in order to solve the above-described problem, the present invention provides at least a specific bit width transmitted from the host device by executing communication with the host device in a memory card device detachably connectable to the host device. A host interface unit that receives a command group including a memory access command accompanied by a memory address of the memory, a nonvolatile semiconductor memory having a storage area larger than a maximum memory size addressable by the memory address of the specific bit width, and the nonvolatile memory Bank identification number management means for dividing the storage area of the semiconductor memory into a plurality of banks and managing a plurality of bank identification numbers corresponding to the plurality of banks, and a bank included in the bank designation command transmitted from the host device One of the plurality of banks is assigned according to the identification number. Bank designation means for designating a bank to be accessed and one of the designated banks are accessed in response to the memory access command transmitted from the host device and accompanied by a memory address having the specific bit width. A memory control unit, and a card address generation unit that generates a card address for identifying the memory card device in response to a card address generation command transmitted from the host device and transmits the card address to the host device; The bank identification number management means is generated by the card address generation means so that a bank identification number equal to the value of the generated card address is assigned to a specific one of the plurality of banks. Bank identification corresponding to each of the plurality of banks The bank designation command executes the data transfer with the host device in the operation mode of the memory card device designated by the card address, which is transmitted from the host device. It is a card selection command for making a transition to a possible data transfer mode.

According to the present invention, an accessible memory address space can be expanded while maintaining compatibility with an existing host device that does not support the block unit addressing method.

Hereinafter, embodiments of the present invention will be described with reference to the drawings.

(Embodiment 1)

FIG. 1 is a block diagram showing a configuration of a memory card according to the first embodiment of the present invention. The memory card 101 is a memory card that can be detachably connected to the host device 10, and is realized, for example, as an SD (Secure Digital) memory card. The SD memory card 101 is a removable card that is detachably mounted in a memory card mounting slot (SD card slot) provided in the host device 10 such as a personal computer, a PDA (Personal Digital Assistants), a camera, or a mobile phone. It is a storage device. All communications between the host device 10 and the SD memory card 101 are controlled by commands from the host device 10.

A bus (SD bus) 20 connecting the host device 10 and the SD memory card 101 includes six communication lines (data DAT0-3, command CMD, clock CLK) and three power supply lines (VDD, GND, GND). Correspondingly, the SD memory card 101 has four data pins [DAT0-3] 109, 110, 102, 103, a command pin [CMD] 104, and a clock signal pin [CLK] 107 as shown in the figure. The power supply pin [VDD] 106 and two ground pins [GND] 105 and 108 are provided. The functions of the six communication lines (data DAT0-3, command CMD, clock CLK) are as follows.

DAT0-3: Each data line is a bidirectional signal line used for data transfer between the host device 10 and the SD memory card 101. Each of the host device 10 and the SD memory card 101 operates in the push-pull mode.

CMD: The command signal line is a bidirectional signal line. It is used to transfer commands from the host device 10 to the SD memory card 101 and to transfer responses from the SD memory card 101 to the host device 10. Each memory access command, such as a read command and a write command, includes a 32-bit wide memory address as its command argument.

CLK: The clock signal line is a signal line for transmitting the clock signal CLK from the host device 10 to the SD memory card 101. The command transfer from the host device 10 to the SD memory card 101 and the data transfer between the host device 10 and the SD memory card 101 are synchronized with the clock signal CLK supplied from the host device 10 to the SD memory card 101. Executed.

The SD memory card 101 is provided with a card controller 114 and a flash memory 116. The flash memory 116 is an electrically erasable and writable nonvolatile semiconductor memory, and includes, for example, one or more NAND flash EEPROM chips. In the present embodiment, the flash memory 116 includes a storage area having a memory size larger than the maximum memory size (4 GB) that can be addressed by a 32-bit wide memory address.

The storage area of the flash memory 116 is composed of a large number of erase blocks. The size of each erase block is, for example, 8 KB, 16 KB, or 32 KB. Each erase block is composed of a plurality of pages. One page is usually composed of 528 (512 + 16) bytes. 512 bytes are used as a data storage area, and 16 bytes are used as a redundant area for storing an error correction code and the like. If the size of the erase block is 8 KB, one erase block is composed of 16 pages. If the size of the erase block is 16 KB, one erase block is composed of 32 pages. If the size of the erase block is 32 KB, one erase block is composed of 64 pages. For example, a 64 MB flash EEPROM is composed of 528 bytes × 32 pages × 4096 erase blocks.

In the SD memory card 101, the user data area can only read and write a normal command manages separately flash memory 116 to the user data area and the protected area. In order to access the protected area, a predetermined authentication process is required. This method uses the mechanism of CPRM (Content Protection for Recordable Media: http://www.4centity.com/tech/cprm/). This mechanism realizes a function for suppressing access by unauthorized devices.

The card controller 114 is a controller that accesses the flash memory 116 in response to a command from the host device 10. The card controller 114 includes an I / O interface unit (I / O I / F) 111, a ROM 112, an SRAM 113, a memory interface (memory I / F) 115, a register 117, a bank ID generation unit 118, a bank designation unit 119, and An MPU 120 is provided.

An I / O interface unit (I / O I / F) 111 is a host interface unit for executing communication with the host device 10. The ROM 112 stores a program (firmware) executed by the MPU 120. The memory interface 115 is a memory control unit that accesses the flash memory 116 in accordance with a memory access command from the host device 10 under the control of the MPU 120. The register 117 is used to hold various information regarding the SD memory card 101. The bank ID generation unit 118 is a bank identification number management unit that divides the storage area of the flash memory 116 into a plurality of banks (a plurality of storage areas) and manages a plurality of bank identification numbers corresponding to the plurality of banks. . The bank ID generation unit 118 generates a plurality of bank identification numbers (bank IDs) to be assigned to each of the plurality of banks. The bank designating unit 119 is a bank designating unit that designates one of a plurality of banks as an access target bank according to the transmission bank identification number transmitted from the host device 10. The MPU 120 is a processor that controls the operation of the SD memory card 101, and executes firmware loaded from the ROM 112 to the SRAM 113. The MPU 120 manages the storage area of the flash memory 116 by dividing the storage area of the flash memory 116 into a plurality of banks by using the bank ID generation unit 118 and the bank specification unit 119, and the bank specified by the bank identification number from the host device 10. The memory device is accessed according to a memory access command (write command, read command, etc.) from the host device 10. Addressing (addressing) for each bank is performed using a byte unit addressing method in order to maintain compatibility with existing host devices that do not support the block unit addressing method.

Next, a configuration example of the flash memory 116 will be described with reference to FIG.

As shown in FIG. 2, the storage area of the flash memory 116 is divided into a protection area 201 and a user data area 202. The memory size of the user data area 202 is a memory size larger than the maximum memory size that can be addressed by a 32-bit wide memory address attached as a command argument to the memory access command, for example, 16 GB. The user data area 202 is managed by the bank ID generation unit 118 by being divided into four banks of bank 0 to bank 3. That

is, banks 0, 1, 2, and 3 are allocated in order from the lower address side to the 16 GB memory address space of the user data area 202 (the space of 000000000000 to 3FFFFFFFF in hexadecimal notation). The memory size of each of the bank 0 to bank 3 is a maximum memory size of 4 GB or less that can be addressed by a 32-bit memory address. In this embodiment, the memory size of each bank is 4 GB.

FIG. 3 shows an example of a bank ID table managed by the bank ID generation unit 118. This bank ID table is a table that defines the relationship between the bank ID corresponding to each of bank 0 to bank 3 and the upper 2 bits of the absolute address corresponding to each bank. The absolute address is a 34-bit memory address capable of addressing a 16 GB memory address space (a space of 000000000000 to 3FFFFFFFF in hexadecimal notation) included in the user data area 202. The bank specifying unit 119 obtains the upper 2 bits of the absolute address corresponding to the bank ID specified from the host device 20 with reference to the bank ID table of FIG. An absolute memory address of 34 bits can be generated from the upper 2 bits and a memory address of 32 bits provided as a command argument of the memory address command from the host device 20.

FIG. 4 shows the relationship between the upper 2 bits of the absolute address corresponding to each bank, the command argument (32-bit width memory address), and the 34-bit width absolute address.

As described above, the memory address having a 32-bit width is given as an argument of the command together with the memory access command from the host device 10. The maximum value of a 32-bit memory address is FFFFFFFF in hexadecimal notation.

If the bank ID designated by the host device 20 is 0, the bank designating unit 119 selects a bank 0 in response to a 32-bit width memory address accompanying the memory access command from the host device 10. By adding the upper 2 bits "00", an absolute memory address having a 34-bit width for accessing the bank 0 is generated. If the bank ID designated by the host device 20 is 1, the bank designating unit 119 selects a bank 1 with respect to a 32-bit width memory address attached to the memory access command from the host device 10. By adding the upper 2 bits "01", an absolute memory address having a 34-bit width for accessing the bank 1 is generated. If the bank ID designated by the host device 20 is 2, the bank designating unit 119 selects a bank 2 in response to a 32-bit wide memory address associated with the memory access command from the host device 10. By adding the upper 2 bits "10", an absolute memory address having a 34-bit width for accessing the bank 2 is generated. If the bank ID designated by the host device 20 is 3, the bank designating unit 119 selects a bank 3 in response to a 32-bit width memory address

accompanying the memory access command from the host device 10. Thus, by adding the upper 2 bits "11", an absolute memory address having a 34-bit width for accessing the bank 3 is generated.

Next, the operation of the SD memory card 101 will be described with reference to FIG. Here, it is assumed that the write data from the host device 10 is written to the bank.

In step 501, the host device 10 transmits an initialization command to the SD memory card 101 via a command (CMD) line. The card controller 114 of the SD memory card 101 performs a predetermined initialization process in step 502, and transmits a response indicating the end of the initialization process to the host apparatus 10 via a command (CMD) line in step 503. In step 504, the host apparatus 10 receives the response and confirms the end of the initialization process.

In step 505, the host device 10 transmits a bank designation command including a bank identification number (bank ID) that designates a bank to be accessed to the SD memory card 101 via a command (CMD) line. In step 506, the card controller 114 of the SD memory card 101 uses the bank ID table described above as the bank designation process to set the bank ID value included in the bank designation command from the host device 10 to the upper two absolute addresses. A process of converting to bits is executed, and the value of the upper 2 bits is held. In step 507, the card controller 114 of the SD memory card 101 transmits a response indicating the end of the bank designation process to the host device 10 via the command (CMD) line. In step 508, the host apparatus 10 receives the response and confirms the end of the bank designation process.

In step 509, the host device 10 transmits a write command to the SD memory card 101 via a command (CMD) line. A memory address value having a 32-bit width is added to the write command as a command argument. When the card controller 114 of the SD memory card 101 receives the write command, in step 510, the card controller 114 obtains a 32-bit width memory address value from the command argument attached to the write command, and for this 32-bit width memory address value, An absolute address having a 34-bit width is generated by extending the stored upper 2 bits. In the following step 511, the card controller 114 of the SD memory card 101 designates write data transmitted from the host device 10 via the data (DAT0-3) line following the write command by an absolute address having a 34-bit width. The writing process for writing to the storage location in the flash memory 116 is executed. In the writing process, the absolute address, the write data, and its control signal are supplied to the flash memory 116 via the memory I / F 115. The write target bank is determined by the value of the upper 2 bits, and to which storage position in the write target bank the data is written is determined by the 32-bit width memory address value associated with the write command. When a write command is received from an existing host device that does not have a bank designation function, that is, when a write command is received without receiving a bank designation command, the card controller 114 of the SD memory card 101 always has a bank. 0 is selected as an access target bank.

In the following step 512, the card controller 114 of the SD memory card 101 transmits a response indicating the completion of the writing process to the host device 10 via the command (CMD) line. In step 513, the host apparatus 10 receives the response and confirms the completion of writing.

In the case where the write access to the same bank is executed a plurality of times, the host device 10 only needs to send the bank designation command once before sending the first write command. It is only necessary to transmit a write command without transmitting.

As the bank ID value, any value that can uniquely identify each bank can be used. Furthermore, the bank designation command including the bank ID does not necessarily have to be a dedicated bank designation command. If the command can include the value of the bank ID as a command argument, various existing commands can be used as the bank designation command.

As described above, in this embodiment, an access target bank is first designated by the bank ID from the host device 10, and a write access to the designated access target bank is executed in accordance with a write command from the host device 10. Therefore, the host device 10 can access a memory address space larger than a memory address space accessible by a 32-bit width memory address (byte unit address) only by changing the access target bank. Therefore, it is possible to expand the accessible memory address space while maintaining compatibility with an existing host device that does not support the block unit addressing method. Further, at the time of writing the file, several write accesses for writing the data group constituting the file are executed for the designated bank while a certain bank is designated. For this reason, even if file fragmentation occurs, it is possible to prevent the occurrence of a situation where data groups constituting the same file are stored across different banks. Therefore, even for an existing host device that does not have a bank designation function, for a file existing in bank 0, all data groups constituting the file can be read correctly.

Data reading is also executed in the same procedure as in FIG. Further, the bank 0-3 may be composed of four flash EEPROM chips. In this case, for example, by supplying a chip enable signal to one of the four flash EEPROM chips according to the value of the upper 2 bits of the absolute memory address, one of the four flash EEPROM chips is designated as an access target bank. Is done. Then, an access to the designated flash EEPROM chip is executed according to a memory access command including a 32-bit width memory address.

Next, a case where a card selection command (CMD7) is used as the bank designation command will be described.

The card selection command (CMD7) is a command for changing the operation mode of the SD memory card 101 to a data transfer mode capable of executing data transfer with the host device. The card selection command (CMD7) includes a card address for identifying the SD memory card 101, which is referred to as RCA (relative card address). When the SD memory card 101 receives a card selection command including its own RCA, the SD memory card 101 shifts the operation mode of the SD memory card 101 to the data transfer mode. When transitioning to the data transfer mode, the SD memory card 101 can normally accept a memory access command (read command, write command, etc.) from the host device 10. Therefore, normally, when performing read access and write access to the SD memory card 101, the SD memory card 101 is made to have data by issuing a card selection command to the SD memory card 101 before issuing the memory access command. It is necessary to set the transfer mode.

Therefore, if a card selection command (CMD7) including an RCA and a bank ID is transmitted to the SD memory card 101, an instruction to transition to the data transfer mode and an access target bank can be specified with a single command. .

FIG. 6 shows a procedure of processing for designating an access target bank using a card selection command (CMD7).

In step 601, the host apparatus 10 transmits an RCA generation command (CMD3) to the SD memory card 101 via a command (CMD) line. The RCA generation command (CMD3) is a command for requesting the SD memory card 101 to generate an RCA (also referred to as issuing an RCA). In step 602, the card controller 114 of the SD memory card 101 itself generates an RCA, and in step 603, returns the RCA as a response to the host apparatus 10 via a command (CMD) line. In step 604, the host apparatus 10 receives a response from the SD memory card 101 and obtains an RCA. Next, in step 605, the host device 10 transmits a card selection command (CMD 7) to the SD memory card 101. This card selection command (CMD7) includes an RCA of the SD memory card 101 and a bank ID for designating an access target bank. Note that the card selection command (CMD7) does not necessarily include the RCA and the bank ID separately, and the RCA value included in the card selection command (CMD7) can also be used as the bank ID.

In step 606, the card controller 114 of the SD memory card 101 changes the operation mode of the SD memory card 101 to the data transfer mode, and as a bank designation process, the bank ID value included in the card selection command (CMD7) is absolute. A process of converting the upper 2 bits of the address is executed, and the value of the upper 2 bits is held. In step 607, the card controller 114 of the SD memory card 101 returns a response indicating that the data transfer mode has been changed to the host device 10. The host device 10 receives the response in step 608 and confirms that the SD memory card 101 has been changed to the data transfer mode.

In step 604, when the host device 10 wants to change the RCA value obtained from the SD memory card 101, the host device 10 repeats steps 601 to 604 again, so that a new RCA value is obtained from the SD memory card 101. Can be received.

In addition, when the RCA value included in the card selection command (CMD7) is used as the bank ID instead of including the RCA and the bank ID in the card selection command (CMD7), the bank ID generation unit 118 A bank ID corresponding to each of the banks 0-3 is generated from the RCA value issued to the host device 10.

FIG. 7 shows an example of a bank ID table when a value generated from RCA is used as a bank ID. In FIG. 7, the RCA value itself is used as the bank ID corresponding to the bank 0. The bank ID corresponding to the bank 1 is RCA + 1, the bank ID corresponding to the bank 2 is RCA + 2, and the bank ID corresponding to the bank 3 is RCA + 3.

FIG. 7 shows a case where the RCA value transmitted from the SD memory card 101 to the host device 10 is 0x1100, and the bank IDs of bank 0, bank 1, bank 2, and bank 3 are 0x1100, 0x1101, 0x1102, 0x1103. In the bank ID table of FIG. 7, the value of the upper 2 bits of the absolute address is associated with each of RCA, RCA + 1, RCA + 2, and RCA + 3.

In this way, bank IDs of bank 0, bank 1, bank 2, and bank 3 are generated from the RCA values, and these bank IDs and values of the upper 2 bits of the absolute address are associated with each other using the bank ID table. By holding this, the host device 10 can designate a desired bank only by issuing a card selection command including the following values as command arguments.

When designating bank 0, the host device 10 issues a card selection command including the RCA obtained from the SD memory card 101 as a command argument. The existing host device 10 that does not have the bank designation function always issues a card selection command including the RCA obtained from the SD memory card 101 as a command argument. For this reason, when the SD memory card 101 is mounted on an existing host device 10 that does not have a bank designation function, bank 0 can be automatically selected as an access target bank.

When designating bank 1, the host device 10 issues a card selection command including RCA + 1, that is, a value obtained by adding +1 to the value of RCA obtained from the SD memory card 101 as a command argument. When designating bank 2, the host device 10 issues a card selection command including RCA + 2, that is, a value obtained by adding +2 to the value of RCA obtained from the SD memory card 101 as a command argument. When designating bank 3, the host device 10 issues a card selection command including RCA + 3, that is, a value obtained by adding +3 to the value of RCA obtained from the SD memory card 101 as a command argument.

In the above description, the bank ID values corresponding to banks 0, 1, 2, and 3 are generated by adding 0, 1, 2, and 3, respectively, to RCA. Add 4 values other than 0, 1, 2, 3 respectively, subtract 0, 1, 2, 3 respectively from RCA, or bit-invert the value of RCA to RCA It may be generated by performing other operations such as.

The command argument of the card selection command has a 32-bit width size, but its upper 16-bit portion is used to indicate RCA, and the lower 16-bit portion is a reserved bit. Therefore, instead of changing the RCA value to be set in the command argument of the card selection command to RCA, RCA + 1, RCA + 2, RCA + 3, RCA is always set in the upper 16 bits and set in the reserved bits. The value may be changed to 0, 1, 2, 3, or RCA, RCA + 1, RCA + 2, RCA + 3. In this case, the bank designating unit 119 acquires the bank ID from the reserved bits included in the command argument of the card selection command, and refers to the bank ID table to convert the acquired bank ID into upper bits of the absolute address. That's fine. In addition to a card selection command, any command that includes RCA as a command argument can be used as a bank designation command.

In this way, by using a method of designating a bank using a card selection command, it is possible to designate a bank to be accessed without using a bank designation dedicated command. In particular, by making the bank ID value assigned to bank 0 equal to RCA, any existing host device can normally access bank 0.

In the above-described example, the procedure for generating the bank ID has been described on the assumption that the host device 10 and the SD memory card 101 determine in advance. However, the bank ID corresponding to each bank is assigned to the SD memory card. It is also possible to notify the host apparatus 10 from 101. For example, the SD memory card 101 can transmit an RCA corresponding to each of the banks 0-3 to the host device 10 and use these RCAs as bank IDs corresponding to the respective banks 0-3. For example, the SD memory card 101 may issue an RCA for the next bank when an RCA generation command (CMD3) is issued a predetermined number of times. If the predetermined number is, for example, 3 times, the SD memory card 101 generates an RCA for bank 0 in response to the RCA generation commands from the first time to the third time, and generates RCA from the fourth time to the sixth time. An RCA for bank 1 is generated for the command, an RCA for bank 2 is generated for the RCA generation commands from the seventh to the ninth time, and an RCA generation command for the tenth to twelfth times is generated. Generates an RCA for bank 3.

When the value of the command argument included in the received RCA generation command is not 0, or when the command argument included in the received RCA generation command indicates an already generated RCA, the SD memory card 101 You may make it issue RCA for banks. In this case, the host device 10 first transmits an RCA generation command including 0 as a command argument to the SD memory card 101, thereby obtaining an RCA for bank 0. Next, the host device 10 transmits an RCA generation command including the RCA for bank 0 as a command argument to the SD memory card 101, thereby obtaining the RCA for bank 1. Next, the host device 10 transmits an RCA generation command including the RCA for bank 1 as a command argument to the SD memory card 101, thereby obtaining the RCA for bank 2. Finally, the host device 10 transmits an RCA generation command including the RCA for bank 2 as a command argument to the SD memory card 101, thereby obtaining the RCA for bank 3.

In the first embodiment described above, the case where the user data area of the flash memory 116 is divided into four banks has been described. However, the number of banks is not limited to four, and the user data area may be divided into more banks. good.

(Embodiment 2)
Next, an SD memory card 101 according to the second embodiment of the present invention will be described.

In the first embodiment, the example in which the 16 GB storage area is divided into four banks each having a memory size of 4 GB has been described. However, in the second embodiment, the 16 GB storage area is divided into the lower 4 GB bank. It is divided into two banks, 0 and bank 12 of the upper 12 GB. Addressing for bank 0 is performed using a byte unit addressing method, and addressing for bank 1 is performed using a block unit addressing method. The host device 10 designates the bank by the same method as in the first embodiment, and then addresses the lower 4 GB using the above-described byte unit addressing method, and the above-mentioned block unit for the upper 12 GB. Address using addressing method.

FIG. 8 is a block diagram showing a configuration of the SD memory card 101 according to the second embodiment. The card controller 114 of the SD memory card 101 is provided with a byte address conversion unit 801 in addition to the configuration of FIG. The firmware stored in the ROM 112 is configured to selectively use the byte unit addressing method and the block unit addressing method. The other parts are the same as in FIG

The bank ID generation unit 118 generates a bank identification number (bank ID) for managing the storage area of the flash memory 116 by dividing it into two banks. The bank designation unit 119 designates a bank to be accessed according to a bank identification number (bank ID) from the host device 10. When the block addressing method is used, the byte address converter 801 converts a block memory address associated with a memory access command transmitted from the host device 10 into a byte address. For example, when one block is 512 bytes, the byte address conversion unit 801 actually accesses the storage area of the flash memory 116 with the memory address value of the block unit by multiplying the memory address value of the block unit by 512. To a memory address value in bytes.

The storage location that can be specified by the memory address in units of blocks is discrete for each block, that is, every 512 bytes. For example, 0x00000000
depending on the memory address in block units
0x00000001
0x00000002
When converting to a byte unit address,
0x00000000
0x00000100
0x00000400
It becomes.

The ROM 112 stores firmware that has been changed to interpret the block unit addressing method. Since the MPU 120 executes this firmware, block unit addressing can be interpreted.

Next, a configuration example of the flash memory 116 will be described with reference to FIG.

As shown in FIG. 9, the storage area of the flash memory 116 is divided into a protection area 201 and a user data area 202. The memory size of the user data area 202 is, for example, 16 GB. The user data area 202 is divided into two banks, bank 0 and bank 1, for management. That is, the banks 0 and 1 are assigned in order from the lower address side to the 16 GB memory address space of the user data area 202 (the space of 000000000000 to 3FFFFFFFF in hexadecimal notation). The memory size of bank 0 is 4 GB, and the memory size of bank 1 is 12 GB.

FIG. 10 shows an example of a bank ID table managed by the bank ID generation unit 118. The bank ID table is a table that defines bank IDs corresponding to the bank 0 and the bank 1, respectively. Here, the bank ID corresponding to the bank 0 is set to 0 and the bank ID corresponding to the bank 1 is set to 1. However, as in the first embodiment, RCA may be used as the bank ID.

FIG. 11 shows the relationship between a command argument (32-bit width memory address) corresponding to each bank and an absolute address of 34-bit width.

As described above, the memory address having a 32-bit width is given as an argument of the command together with the memory access command from the host device 10. The 32-bit width memory address corresponding to bank 0 is a byte unit address, and the 32-bit width memory address corresponding to bank 1 is a block unit address.

If the bank ID designated by the host device 10 is 0, the bank designating unit 119 determines the upper 2 bits for the 32-bit width memory address (byte unit address) attached to the memory access command from the host device 10. By adding bit "00", a 34-bit absolute memory address (byte unit address) for accessing bank 0 is generated. If the bank ID designated by the host device 20 is 1, the bank designation unit 119 multiplies the 32-bit width memory address (block unit address) associated with the memory access command from the host device 10 by 512. A 34-bit absolute memory address (byte unit address) for accessing bank 1 is generated.

Next, the operation of the SD memory card 101 will be described with reference to FIG. Here, it is assumed that the write data from the host device 10 is written to the bank. FIG. 12 differs from FIG. 5 in that steps 901 to 906 are added. Other parts are the same as those in FIG.

In step 501, the host device 10 transmits an initialization command to the SD memory card 101. The card controller 114 of the SD memory card 101 performs a predetermined initialization process in step 502, and transmits a response indicating the end of the initialization process to the host device 10 in step 503. In step 504, the host apparatus 10 receives the response and confirms the end of the initialization process.

In step 505, the host device 10 transmits a bank designation command including a bank identification number (bank ID) for designating a bank to be accessed to the SD memory card 101. Instead of the bank designation command, a card selection command including a bank ID may be used. In step 506, the card controller 114 of the SD memory card 101 executes bank designation processing. In this bank designation process, the card controller 114 of the SD memory card 101 holds "00" as the value of the upper 2 bits of the absolute address if bank 0 is designated by the bank designation command. If bank 1 is specified by the command, the value of the upper 2 bits is

not held at all. In step 507, the card controller 114 of the SD memory card 101 transmits a response indicating the end of the bank designation process to the host device 10. In step 508, the host apparatus 10 receives the response and confirms the end of the bank designation process.

When accessing the bank 1, the host device 10 transmits to the SD memory card 101 an address mode change command indicating that the address mode of the SD memory card 101 is switched to the block unit address mode in step 901. The block unit address mode is an address mode capable of receiving an address in block units. On the other hand, when accessing the bank 0, the host device 10 transmits an address mode change command indicating that the address mode of the SD memory card 101 is switched to the byte unit address mode to the SD memory card 101 in step 901. The byte unit address mode is an address mode for accepting addresses in byte units.

In step 902, the card controller 114 of the SD memory card 101 changes its own address mode from the byte unit address mode to the block unit address mode or from the block unit address mode to the byte unit address mode in response to the address mode change command. change. In step 903, the card controller 114 of the SD memory card 101 transmits a response indicating completion of the address mode change to the host device 10. The host device 10 receives the response in step 904 and confirms that the SD memory card 101 has changed the address mode. Note that the default address mode of the SD memory card 101 is the byte unit address mode, and the SD memory card 101 operates in the byte unit address mode until an address mode change command is received from the host device.

In step 509, the host device 10 transmits a write command to the SD memory card 101. A memory address having a 32-bit width is added to the write command as a command argument. This 32-bit memory address is a byte unit address if the bank to be accessed is bank 0, and a block unit address if the bank to be accessed is bank 1. In step 905, the card controller 114 of the SD memory card 101 determines whether the current address mode is the block unit address mode or the byte unit address mode.

If the current address mode is the block unit address mode, the card controller 114 of the SD memory card 101 proceeds to step 906. In step 906, the card controller 114 of the SD memory card 101 obtains a 32-bit width memory address value from the command argument attached to the write command, and the memory address value is converted from the block unit address to the byte unit address (34 bit width) (Absolute address). In the following step 511, the card controller 114 of the SD memory card 101 writes the write data transmitted from the host device 10 following the write command to the storage location in the flash memory 116 designated by the byte unit address. Execute. In the writing process, the absolute address, the write data, and its control signal are supplied to the flash memory 116 via the memory I / F 115.

On the other hand, if the current address mode is the byte unit address mode, the card controller 114 of the SD memory card 101 proceeds to step 510. In step 510, the card controller 114 of the SD memory card 101 obtains a 32-bit width memory address value from the command argument attached to the write command, and holds the upper address stored for the 32-bit width memory address value. By expanding the 2-bit value, a 34-bit wide absolute address is generated. In the following step 511, the card controller 114 of the SD memory card 101 performs a writing process of writing the write data transmitted from the host device 10 following the write command to the storage location in the flash memory 116 designated by the absolute address. Execute.

In subsequent step 512, the card controller 114 of the SD memory card 101 transmits a response indicating completion of the writing process to the host device 10. In step 513, the host apparatus 10 receives the response and confirms the completion of writing.

When a write command is received from an existing host device that does not support the bank designation function and the block unit address mode, the card controller 114 of the SD memory card 101 always accesses bank 0 in the byte unit address mode. Good. As a result, the existing host device can also access bank 0 correctly.

(Embodiment 3)
Next, an SD memory card 101 according to the third embodiment of the present invention will be described.

In addition to the configuration of the first embodiment, the SD memory card 101 according to the third embodiment has an access control function that permits access to each bank only when a predetermined condition is satisfied.

FIG. 13 is a block diagram showing a configuration of the SD memory card 101 according to the third embodiment. The card controller 114 of the SD memory card 101 is provided with a bank access control unit 901 in addition to the configuration of FIG. The other points are the same as in FIG. The bank access control unit 901 is provided to realize an access control function, and determines whether or not access by the host device 10 is permitted for each bank.

FIG. 14 shows an access control table that defines conditions for permitting access. This access control table associates a bank number for which access is permitted with the number of receptions of the bank designation command. The bank access control unit 901 counts the number of receptions of the bank designation command

from the host device 10, and accesses the host device 10 by referring to the access control table using the counted number of receptions of the bank designation command as an index. Decide which banks should be allowed. For example, in the access control table of FIG. 14, access to bank 0 is permitted when the number of receptions of the bank designation command is three or more. Similarly, access to the bank 1 is permitted when the number of receptions of the bank designation command is 5 or more, and access to the bank 2 is permitted when the number of receptions of the bank designation command is 7 or more. Is permitted when the number of received bank designation commands is 9 or more.

Next, the operation of the SD memory card 101 will be described with reference to FIG. Here, it is assumed that the write data from the host device 10 is written to the bank. In this example, step 505 to step 508 in FIG. 5 are changed from step 1101 to step 1105.

In step 501, the host device 10 transmits an initialization command to the SD memory card 101. The card controller 114 of the SD memory card 101 performs a predetermined initialization process in step 502, and transmits a response indicating the end of the initialization process to the host device 10 in step 503. In step 504, the host apparatus 10 receives the response and confirms the end of the initialization process.

In step 1101, the host device 10 transmits a bank designation command including a bank identification number (bank ID) for designating a bank to be accessed to the SD memory card 101. Instead of the bank designation command, a card selection command including a bank ID may be used. When the card controller 114 of the SD memory card 101 receives the bank designation command in step 1102, it increments the value indicating the number of receptions of the bank designation command by +1. When the bank designation command is received for the first time after the initialization process, the number of receptions of the bank designation command is 1. In step 1102, the card controller 114 of the SD memory card 101 determines an accessible bank number by the above-described method. In the subsequent step 1103, if the access target bank designated by the bank designation command is an accessible bank, the card controller 114 of the SD memory card 101 uses a bank designation command from the host device 10 as a bank designation process. A process of converting the included bank ID value into the upper 2 bits of the absolute address is executed, and the value of the upper 2 bits is held. If the access target bank designated by the bank designation command is not an accessible bank, the bank designation process is not executed. In step 1104, the card controller 114 of the SD memory card 101 transmits a response indicating the end of bank designation to the host device 10. This response can include information indicating the success or failure of the bank designation process. In step 1105, the host apparatus 10 receives the response and confirms whether the bank designation process has been successful. The host device 10 executes step 1101 again as necessary to access the desired bank. Accordingly, step 1102, step 1103, and step 1104 are executed again in the same procedure.

Here, as an example of bank access control, a state when a bank designation command is received three times will be described. in a state where the bank designation command is received three times, it is determined that bank 0 is accessible with reference to the access control table of FIG. If the bank designated by the bank designation command is 0, as the bank designation process, a process of converting the bank ID corresponding to bank 0 into the upper 2 bits of the absolute address corresponding to bank 0 is performed. As a result, bank 0 can be accessed. However, when the bank designated by the bank designation command is 1, the bank designation process is not executed. As a result, access to bank 1 is prohibited. As a method of prohibiting access to bank 1, in addition to a method that does not perform bank designation processing, for example, a method of converting to a higher-order bit of a memory address of a nonexistent bank, or a specific bank such as bank 0 is supported. For example, there is a method in which a specific bank is always set as an access target bank by converting it into upper 2 bits of the absolute address.

In step 1104, when the host device 10 receives the response and recognizes that the designated bank is accessible, the host device 10 performs the processing from step 509 onward to write data. In step 509, the host device 10 transmits a write command to the SD memory card 101. A memory address value having a 32-bit width is added to the write command as a command argument. When the card controller 114 of the SD memory card 101 receives the write command, in step 510, the card controller 114 obtains a 32-bit width memory address value from the command argument attached to the write command, and for this 32-bit width memory address value, An absolute address having a 34-bit width is generated by extending the stored upper 2 bits. In the subsequent step 511, the card controller 114 of the SD memory card 101 transfers the write data transmitted from the host device 10 following the write command to the storage location in the flash memory 116 specified by the 34-bit width absolute address. Execute the writing process to write. In the writing process, the absolute address, the write data, and its control signal are supplied to the flash memory 116 via the memory I / F 115. In subsequent step 512, the card controller 114 of the SD memory card 101 transmits a response indicating completion of the writing process to the host device 10. In step 513, the host apparatus 10 receives the response and confirms the completion of writing.

In the above bank access control, a table indicating banks that are permitted to be accessed is referred to, and the corresponding bank can be accessed when the number of received bank designation commands is reached. However, the present invention is not limited to this. Can be used to restrict access to each bank.

In each of the above embodiments, the user data area of the SD memory card is divided into a plurality of banks. However, the present invention is not limited to the user data area, and the protection area may be divided into a plurality of banks. Good. However, in this case, it is necessary to use the above-described CPRM mechanism in order to access the protection area. Moreover, although each above-mentioned embodiment demonstrated and demonstrated the SD memory card, the structure of the

bank control of each embodiment is applicable to the various memory cards which can be connected to a host device removably. A memory card is a generic name for a removable storage device and does not limit the physical shape of the memory card.

Further, the present invention is not limited to the above-described embodiments as they are, and can be embodied by modifying the constituent elements without departing from the scope of the invention in the implementation stage. In addition, various inventions can be formed by appropriately combining a plurality of constituent elements disclosed in the embodiment. For example, some components may be deleted from all the components shown in the embodiment. Furthermore, constituent elements over different embodiments may be appropriately combined.

1 is a block diagram showing a configuration of a memory card according to a first embodiment of the present invention. The figure which shows the bank structure of the non-volatile semiconductor memory provided in the memory card of FIG. The figure which shows the example of the bank ID table used in the memory card of FIG. The figure which shows the relationship between the upper 2 bits of the absolute address corresponding to each bank in the memory card of FIG. 1, the command argument, and the absolute address of 34 bits width. 3 is a flowchart showing the operation of the memory card of FIG. 3 is a flowchart for explaining an operation of designating a bank using a card selection command in the memory card of FIG. 1. The figure which shows the other example of the bank ID table used in the memory card of FIG. The block diagram which shows the structure of the memory card based on 2nd Embodiment of this invention. The figure which shows the bank structure of the non-volatile semiconductor memory provided in the memory card of FIG. The figure which shows the example of the bank ID table used in the memory card of FIG. The figure which shows the relationship between the command argument corresponding to each bank in the memory card | curd of FIG. 8, and the absolute address of 34 bit width. 9 is a flowchart showing the operation of the memory card of FIG. The block diagram which shows the structure of the memory card based on 3rd Embodiment of this invention. The figure which shows the example of the access control table used in the memory card of FIG. 14 is a flowchart showing the operation of the memory card of FIG

Explanation of symbols

DESCRIPTION OF SYMBOLS 10 ... Host device, 101 ... SD memory card, 111 ... I / O interface, 120 ... MPU, 115 ... Memory interface, 116 ... Flash memory, 118 ... Bank ID production | generation part, 119 ... Bank designation | designated part, 801 ... Byte address conversion Part, 901 ... Bank access control part.

Patent Citations (12)

Publication number	Priority date	Publication date	Assignee	Title
JP2001051897A *	1999-08-11	2001-02-23	Toshiba Corp	Semiconductor storage device
JP2004038643A *	2002-07-04	2004-02-05	Matsushita Electric Ind Co Ltd	Composite input and output device
JP2004086503A *	2002-08-26	2004-03-18	Toshiba Corp	Memory card recognizing system, memory card host equipment, memory card, storage area switching method, and storage area switching program
JP2004514962A *	2000-08-17	2004-05-20	サンディスク コーポレイション	Multiple removable non-volatile memory cards that communicate sequentially with the host
WO2005045680A1 *	2003-11-07	2005-05-19	Matsushita Electric Industrial Co., Ltd.	Information recording medium and its control method
JP2006524405A *	2003-04-23	2006-10-26	コーニンクレッカ フィリップス エレクトロニクス エヌヴィ	Partition selection for universal storage
JP2007518188A *	2004-01-09	2007-07-05	サンディスク コーポレイション	Memory card that supports file system interoperability

Family To Family Citations

US4473877A *	1981-04-16	1984-09-25	Tulk Ronald K	Parasitic memory expansion for computers
US5630098A *	1991-08-30	1997-05-13	Ncr Corporation	System and method for interleaving memory addresses between memory banks based on the capacity of the memory banks
JPH06274412A	1993-03-19	1994-09-30	Fujitsu Ltd	Memory controller
JP4621314B2	1999-06-16	2011-01-26	株式会社東芝	Storage medium
US6430648B1 *	2000-01-05	2002-08-06	International Business Machines Corporation	Arranging address space to access multiple memory banks

* Cited by examiner, † Cited by third party

Cited By (21)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
FI117489B *	2003-02-07	2006-10-31	Nokia Corp	A method for indicating a memory card, a system using a memory card, and a memory card
JP2005275907A *	2004-03-25	2005-10-06	Toshiba Corp	Electronic apparatus, and method for controlling storage medium unit of the apparatus
JP4817836B2	2004-12-27	2011-11-16	株式会社東芝	Card and host equipment
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
JP2007257345A *	2006-03-23	2007-10-04	Nec Corp	Electronic tag
KR100888261B1	2007-02-22	2009-03-11	삼성전자주식회사	Memory subsystem capable of using bank identification and method thereof
JP4473900B2 *	2007-08-22	2010-06-02	株式会社東芝	Semiconductor memory device
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
CN101282347B *	2008-05-15	2011-04-06	普天信息技术研究院有限公司	Method for controlling intelligent storing card
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US20100033310A1 *	2008-08-08	2010-02-11	Narendra Siva G	Power negotation for small rfid card
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
JP5129691B2 *	2008-08-22	2013-01-30	株式会社バッファロー	Memory card, memory card control device, and memory card control method
US8473964B2 *	2008-09-30	2013-06-25	Microsoft Corporation	Transparent user mode scheduling on traditional threading systems
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
US20110173458A1 *	2010-01-13	2011-07-14	Bonica Richard T	Secure portable data storage device
JP5549432B2 *	2010-07-02	2014-07-16	富士通株式会社	Storage apparatus and access control program
CN102169459B *	2010-11-29	2013-04-24	北京握奇数据系统有限公司	Method, device and intelligent card for accessing data
TWI474253B *	2011-08-18	2015-02-21		
US8856063B1 *	2012-11-09	2014-02-18	Ralink Technology Corp.	Method of detecting addressing mode and electronic system thereof
US10235103B2 *	2014-04-24	2019-03-19	Xitore, Inc.	Apparatus, system, and method of byte addressable and block addressable storage and retrival of data to and from non-volatile storage memory

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
JP4515793B2	2010-08-04	Memory card device and memory card control method

EP1189139B1	2007-12-12	Recording system, data recording device, memory device, and data recording method
US8291155B2	2012-10-16	Data access method, memory controller and memory storage system
KR100483643B1	2005-04-18	Memory device
US8054686B2	2011-11-08	Flash memory storage apparatus, flash memory controller, and switching method thereof
JP4059002B2	2008-03-12	Memory device
KR20080091203A	2008-10-09	Portable data storage device incorporating multiple flash memory units
JP2005267628A	2005-09-29	Memory card using nand flash memory, and operation method thrurfor
JP2006092019A	2006-04-06	Controller, memory card and its control method
US8127072B2	2012-02-28	Data storage device and method for accessing flash memory
US20100011154A1	2010-01-14	Data accessing method for flash memory and storage system and controller using the same
JP2009510584A	2009-03-12	Portable data storage device using SLC and MLC flash memory
US6996663B1	2006-11-15	Continuous arrangement of data clusters across multiple storages
KR20080084082A	2008-09-19	Memory card and memory system including the same and operating method thereof
TW201027555A	2010-07-16	Semiconductor storage device and storage controlling method
JPWO2005083573A1	2007-11-29	Semiconductor memory device
WO2009096180A1	2009-08-06	Memory controller, nonvolatile storage device, and nonvolatile storage system
JP2010146326A	2010-07-01	Storage device, method of controlling same, and electronic device using storage device
TW200540690A	2005-12-16	Memory card that supports file system interoperability
JP2009245278A	2009-10-22	Semiconductor storage device
JP2006195565A	2006-07-27	Control method for semiconductor storage device, memory card, and host apparatus
JPWO2007105688A1	2009-07-30	Memory controller, nonvolatile storage device, and nonvolatile storage system
JP4575410B2	2010-11-04	Semiconductor memory device and operation method thereof
JP4308780B2	2009-08-05	Semiconductor memory device, memory controller, and data recording method
KR20080033649A	2008-04-17	Flash memory system and managing method for the system capable of merging data less frequently

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
JP2004069424A	2004-03-11	2004-03-11	Memory card device and memory card control method

Applications Claiming Priority (2)

Application	Filing date	Title
JP2004069424A	2004-03-11	Memory card device and memory card control method
US10/930,872	2004-09-01	Memory card device, and memory card control method for controlling the device

Legal Events

Date	Code	Title	Description
2006-11-02	A621	Written request for application examination	**Free format text**: JAPANESE INTERMEDIATE CODE: A621 **Effective date**: 20061101
2009-12-28	A977	Report on retrieval	**Free format text**: JAPANESE INTERMEDIATE CODE: A971007 **Effective date**: 20091228

2010-01-06	A131	Notification of reasons for refusal	**Free format text:** JAPANESE INTERMEDIATE CODE: A131 **Effective date:** 20100105
2010-03-09	A521	Written amendment	**Free format text:** JAPANESE INTERMEDIATE CODE: A523 **Effective date:** 20100308
2010-04-09	TRDD	Decision of grant or rejection written	
2010-04-14	A01	Written decision to grant a patent or to grant a registration (utility model)	**Free format text:** JAPANESE INTERMEDIATE CODE: A01 **Effective date:** 20100413
2010-04-15	A01	Written decision to grant a patent or to grant a registration (utility model)	**Free format text:** JAPANESE INTERMEDIATE CODE: A01
2010-05-20	A61	First payment of annual fees (during grant procedure)	**Free format text:** JAPANESE INTERMEDIATE CODE: A61 **Effective date:** 20100513
2010-05-21	R150	Certificate of patent or registration of utility model	**Free format text:** JAPANESE INTERMEDIATE CODE: R150
2010-05-24	FPAY	Renewal fee payment (event date is renewal date of database)	**Free format text:** PAYMENT UNTIL: 20130521 **Year of fee payment:** 3
2013-05-21	LAPS	Cancellation because of no payment of annual fees	

Data provided by IFI CLAIMS Patent Services

About Send Feedback Public Datasets Terms Privacy Policy

Patents AUPP411098A0

Communication method and apparatus improvements

Classifications

H04B1/40 Circuits

View 9 more classifications

AUPP411098A0

Australia

Find Prior Art Similar

Current Assignee : NEWCOM TECHNOLOGIES Pty Ltd

Worldwide applications

1998 AU 1999 DK GN GB PL GA JP WO KR IL NO HU EE BR NZ AT SE ID PT EP 2000 US FR IS NO 2001 ZA BG 2002 HK 2006 US

Application AUPP4110A events

1998-06-15	Application filed by NEWCOM TECHNOLOGIES Pty Ltd
1998-06-15	Priority to AUPP4110A
1998-07-09	Publication of AUPP411098A0
1999-06-11	Priority claimed from AU42516/99A
2007-07-27	First worldwide family litigation filed
Status	Abandoned

Info: Patent citations (31), Cited by (64), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Patent Citations (31)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
BE794977A *	1972-02-05	1973-05-29	Siemens Ag	SWITCHING DEVICE FOR REMOTE-CONTROLLED ELECTRICAL USERS
US4677653A *	1986-06-16	1987-06-30	B/W Investments	Cellular mobile phone with a plurality of accessing telephone numbers for allowing access to the mobile phone by any one of the telephone numbers
DE3721889A1	1987-07-02	1989-01-12	Standard Elektrik Lorenz Ag	COMPUTER CONTROLLED SUBSCRIBER DEVICE FOR OPERATION IN TELECOMMUNICATION NETWORKS, IN PARTICULAR MOBILE RADIO NETWORKS, WITH DIFFERENT SYSTEM TECHNOLOGY
CA2064646A1	1991-04-02	1992-10-03	Kipling W. Fyfe	Automatic number assignment module selection for mobile telephone
SE9101105L	1991-04-12	1992-08-03	Comvik Gsm Ab	PHONE SYSTEM PROCEDURES
FI98183C *	1992-02-14	1997-04-25	Nokia Mobile Phones Ltd	Arrangement for connecting a data adapter to a GSM cellular telephone
FI90298C	1992-02-18	1994-01-10	Nokia Mobile Phones Ltd	The card reader device
GB2269512B *	1992-08-03	1996-08-14	Nokia Mobile Phones Uk	Radio arrangement
SE470041B	1992-10-01	1993-10-25	Nordictel Ab	Digital mobile telephone system in which each subscription is assigned a subscriber number and multiple subscriber cards (SIM)
DE69324445T2 *	1992-11-27	1999-09-30	Denso Corp	Portable electronic device
DE4307122A1 *	1993-03-06	1994-09-08	Sel Alcatel Ag	Smart card
JPH07123262B2	1993-03-19	1995-12-25	日本電気株式会社	Mobile phone

US5548485A *	1993-04-12	1994-09-20	Electronic Retailing Systems Int'l Inc.	Electronic price display system with vertical rail
FR2711866B1	1993-10-26	1996-05-24	Alcatel Mobile Comm France	Installation of digital radio-telephone with mobile terminals.
EP0690645B1	1994-06-30	2006-08-02	Casio Computer Co., Ltd.	Radio communication apparatus having a plurality of identification codes
FI981780 *	1994-04-19	1997-04-25	Nokia Mobile Phones Ltd	Card reading device for mobile phone
FI103313B1	1994-05-13	1999-05-31	Sonera Oy	A method for calling a terminal of a mobile communication system, such as a card-controlled mobile station
US5764730A *	1994-10-05	1998-06-09	Motorola	Radiotelephone having a plurality of subscriber identities and method for operating the same
US6012634A *	1995-03-06	2000-01-11	Motorola, Inc.	Dual card and method therefor
FR2740291B1 *	1995-10-20	1997-12-12	Sagem	DUAL FUNCTION RADIOTELEPHONE, PARTICULARLY FINANCIAL TRANSACTION AND METHOD FOR ESTABLISHING A COMMUNICATION BETWEEN THE RADIOTELEPHONE AND THE RADIOTELEPHONE NETWORK
AUPN755196A0	1996-01-15	1996-02-08	Benson, Keith	Improvements relating to mobile phones
US5915226A *	1996-04-19	1999-06-22	Gemplus Card International	Prepaid smart card in a GSM based wireless telephone network and method for operating prepaid cards
US5815426A *	1996-08-13	1998-09-29	Nexcom Technology, Inc.	Adapter for interfacing an insertable/removable digital memory apparatus to a host data part
US5884168A *	1996-08-30	1999-03-16	Ericsson, Inc.	Multiple cellular systems with limited sim card information
US5894597A *	1996-09-24	1999-04-13	Motorola, Inc.	Communication device for different sized cards
GB2319438A *	1996-11-13	1998-05-20	Int Maritime Satellite Organiz	User Terminal for Multiple Services
NL1005601C2 *	1997-03-21	1998-09-22	Koninkl Kpn Nv	Telecommunication system
US6185436B1 *	1997-03-27	2001-02-06	Siemens Information And Communication Networks, Inc.	Wireless communication system
US6138010A *	1997-05-08	2000-10-24	Motorola, Inc.	Multimode communication device and method for operating a multimode communication device
US5987325A *	1997-05-19	1999-11-16	Motorola, Inc.	Multiple smart card phone and method
US6250557B1	1998-08-25	2001-06-26	Telefonaktiebolaget Lm Ericsson (Publ)	Methods and arrangements for a smart card wallet and uses thereof

* Cited by examiner, † Cited by third party

Cited By (64)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
AU726580B3 *	1998-06-15	2000-11-09	Newcom Holdings Pty Ltd	Communication method and apparatus improvements
US7376583B1	1999-08-10	2008-05-20	Gofigure, L.L.C.	Device for making a transaction via a communications link
FI112427B *	1999-11-05	2003-11-28	Nokia Corp	A method for determining the capabilities of a wireless terminal in a multimedia messaging service, a multimedia messaging service, and a multimedia terminal
GB2362774B	2000-05-26	2004-08-18	Nokia Mobile Phones Ltd	Radiotelephone
GB2371445A *	2000-07-14	2002-07-24	Funge Systems Internat Ltd	Interrogatable communication apparatus
ES2182642B1 *	2000-07-17	2004-08-16	Imbros Corporation	REMOTE COMMUNICATIONS DEVICE.
FI112307B *	2000-08-02	2003-11-14	Nokia Corp	communication Server
FR2815500B1 *	2000-10-17	2003-03-07	Sagem	PORTABLE TELEPHONES WITH MULTIMEDIA FILE PLAYER
DE10064546C1 *	2000-12-22	2002-07-04	Huf Huelsbeck &	Locking system for motor vehicles

			Fuerst Gmbh	
WO2002071727A2 *	2001-03-05	2002-09-12	Quasar Communication Systems Ltd.	Cellular telephone protocol extension adapter
US20030186722A1 *	2002-03-28	2003-10-02	Comverse, Ltd.	Method and device for real time GSM user device profile interrogation and registration
UA9124U *	2002-06-20	2005-09-15		Playing system for remote gaming activities for gambling
US7280847B2	2002-07-26	2007-10-09	Way Systems Inc	System and method for mobile transactions using the bearer independent protocol
WO2004088641A2	2003-03-26	2004-10-14	Way Systems, Inc.	System and method for securely storing, generating, transferring and printing electronic prepaid vouchers
US20040230489A1 *	2002-07-26	2004-11-18	Scott Goldthwaite	System and method for mobile payment and fulfillment of digital goods
US20040127256A1 *	2002-07-30	2004-07-01	Scott Goldthwaite	Mobile device equipped with a contactless smart card reader/writer
US7720762B1	2002-10-03	2010-05-18	Gofigure Payments, Llc	System and method for electronically processing commercial transactions based upon threshold amount
US7336973B2	2002-10-30	2008-02-26	Way Systems, Inc	Mobile communication device equipped with a magnetic stripe reader
KR100769741B1 *	2003-05-29	2007-10-23	교세라 가부시키가이샤	Radio communication system, radio communication apparatus, radio communication terminal and mobile radio communication apparatus
JP4629579B2	2003-10-14	2011-02-09	テレコム・イタリア・エッセ・ピー・アー	Resource control method and system via mobile terminal, related network and computer program product therefor
US20050133589A1 *	2003-12-18	2005-06-23	Chuang Guan Technology Co., Ltd.	Network connection apparatus
DE602004020684D1	2004-03-19	2009-05-28	Nokia Corp	NO METHOD FOR IMPROVING TERMINAL OPERATION
US20110071949A1 *	2004-09-20	2011-03-24	Andrew Petrov	Secure pin entry device for mobile phones
US20060064391A1 *	2004-09-20	2006-03-23	Andrew Petrov	System and method for a secure transaction module
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
CN1804338530 *	2006-01-24	2006-07-19	华为技术有限公司	Remote-inquiring-information method and communication terminal
US20070184858A1 *	2006-02-09	2007-08-09	Agere Systems Inc.	Method of attaching mobile communication tasks to a Subscriber Information Module card and mobile communication device incorporating the same
US7873573B2 *	2006-03-30	2011-01-18	Obopay, Inc.	Virtual pooled account for mobile banking
US20070244811A1 *	2006-03-30	2007-10-18	Obopay Inc.	Mobile Client Application for Mobile Payments
US20090319425A1 *	2007-03-30	2009-12-24	Obopay, Inc.	Mobile Person-to-Person Payment System
US8532282B2 *	2006-03-30	2013-09-10	Obopay, Inc.	Data communications over voice channel with mobile consumer communications devices
US20080032741A1 *	2006-03-30	2008-02-07	Obopay	Programmable Functionalities for Mobile Consumer Communications Devices with Identification-Modules
US20070255653A1 *	2006-03-30	2007-11-01	Obopay Inc.	Mobile Person-to-Person Payment System
US20070255662A1 *	2006-03-30	2007-11-01	Obopay Inc.	Authenticating Wireless Person-to-Person Money Transfers
US8249965B2 *	2006-03-30	2012-08-21	Obopay, Inc.	Member-supported mobile payment system
US7392946B2 *	2006-06-12	2008-07-01	Sony Ericsson Mobile Communications Ab	Mobile radio terminal having a multiple form factor memory card reader
US20080064442A1 *	2006-09-11	2008-03-13	Utstarcom, Inc.	Identity and payment modem module for handsets
US7848980B2	2006-12-26	2010-12-07	Visa U.S.A. Inc.	Mobile payment system and method using alias
US9940627B2	2006-12-26	2018-04-10	Visa U.S.A. Inc.	Mobile coupon method and system
US8615426B2	2006-12-26	2013-12-24	Visa U.S.A. Inc.	Coupon offers from multiple entities
CN101595491A	2006-12-26	2009-12-02	维萨美国股份有限公司	Mobile vending purchasing
US8170527B2	2007-09-26	2012-05-01	Visa U.S.A. Inc.	Real-time balance on a mobile phone

US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
WO2009114876A2 *	2008-03-14	2009-09-17	Obopay, Inc.	Network-based viral payment system
EP2114098A1	2008-04-29	2009-11-04	Koninklijke KPN N.V.	Subscriber identity module transceiver
US9715709B2	2008-05-09	2017-07-25	Visa International Services Association	Communication device including multi-part alias identifier
US9542687B2	2008-06-26	2017-01-10	Visa International Service Association	Systems and methods for visual representation of offers
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US8348112B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
US10706402B2	2008-09-22	2020-07-07	Visa International Service Association	Over the air update of payment transaction data stored in secure memory
US9824355B2	2008-09-22	2017-11-21	Visa International Service Association	Method of performing transactions with contactless payment devices using pre-tap and two-tap operations
US8977567B2	2008-09-22	2015-03-10	Visa International Service Association	Recordation of electronic payment transaction information
US8851386B2	2009-01-20	2014-10-07	Mastercard International Incorporated	Removably securing small contactless payment card via removable accessory to electronic device
EP2401708A4	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
US9235831B2	2009-04-22	2016-01-12	Gofigure Payments, Llc	Mobile payment systems and methods
US8195236B2	2010-06-16	2012-06-05	On Track Innovations Ltd.	Retrofit contactless smart SIM functionality in mobile communicators
US8424757B2	2010-12-06	2013-04-23	On Track Innovations Ltd.	Contactless smart SIM functionality retrofit for mobile communication device
AU2011338191A1 *	2010-12-09	2013-07-11	Keith Benson	Hand-held self-provisioned pin red communicator
US20130212399A1 *	2011-08-17	2013-08-15	Geoffrey I. Cairns	Travel Vault
US8646698B2 *	2012-02-15	2014-02-11	Tennrich International Corp.	Protective cover of mobile electronic product
US8925817B2	2012-11-04	2015-01-06	Id Tech	Card reader and method of use thereof
EP3085230A1	2014-12-19	2016-06-22	Cardiab ApS	A method and an assembly for generating a magnetic field
CN107209846A	2014-12-19	2017-09-26	卡德賓博私人有限公司	Method for generating the method and component in magnetic field and manufacturing component
EP3082071A1	2015-04-17	2016-10-19	Cardiab ApS	Device for and method of outputting a magnetic field

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
AUPP411098A0	1998-07-09	Communication method and apparatus improvements
EP1039752A4	2007-05-02	Communication apparatus and method
AU9375898A	1999-03-22	Method and apparatus for securing communications
AU3126400A	2000-07-03	Apparatus and method for wireless communications
AU5263700A	2000-12-18	Method and apparatus for secure communication
AU3087500A	2000-07-12	Method and means for telecom
AU3970899A	1999-12-06	Ferrographic method and apparatus
GB9823629D0	1998-12-23	Communication method and apparatus
AU5701100A	2001-01-22	Communication methods and apparatus
AU2895295A	1996-03-04	Communication apparatus and method

AU5288099A	2000-02-21	Communication system and method therefor
AU7083494A	1996-01-25	Communication method and apparatus therefor
GB9814412D0	1998-09-02	Communications method and apparatus
AU8469798A	1999-03-29	Apparatus and method for radio communication
GB2329556B	1999-12-08	Communication method and apparatus
AUPP754398A0	1999-01-07	Method and apparatus for composting
AU7234094A	1995-08-29	Communication method and apparatus
AU7528630	2003-10-16	Communication device and method of operation
AU5976300A	2001-03-26	Method and apparatus for establishing communication
AU5297098A	1998-08-13	Data communication method and data communication apparatus
AU8924297A	1998-04-02	Method and apparatus for message communication
AU7959700A	2001-05-14	Communication apparatus and communication method
AU1877500A	2000-07-31	Communications system and apparatus
AU1818497A	1997-09-02	Arrangement and method for communication
AU3101799A	1999-10-11	Method and system for wireless telecommunications

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
AUPP4110A	1998-06-15	1998-06-15	Communication method and apparatus improvements

Applications Claiming Priority (29)

Application	Filing date	Title
AUPP4110A	1998-06-15	Communication method and apparatus improvements
BR9911309-0A	1999-06-11	Remote communication device, and, arrangement.
DE69933863T	1999-06-11	COMMUNICATION PROCESS AND DEVICE
IDW20010120A	1999-06-11	METHODS AND EQUIPMENT FOR IMPROVING COMMUNICATIONS
DK99957131T	1999-06-11	Method and device for communication
NZ509305A	1999-06-11	Communication method and apparatus improvements
EP99957131A	1999-06-11	Communication method and apparatus
ES99957131T	1999-06-11	APPARATUS AND COMMUNICATION METHOD.
CNB99809367XA	1999-06-11	Communication method and apparatus improvements
CA002335147A	1999-06-11	Communication method and apparatus improvements
PCT/AU1999/000455	1999-06-11	Communication method and apparatus improvements
PL99346269A	1999-06-11	Communication method and apparatus improvements
IL14031199A	1999-06-11	Communication method and apparatus improvements
AT99957131T	1999-06-11	COMMUNICATION PROCESS AND DEVICE
KR1020007014293A	1999-06-11	Communication method and apparatus improvements
PT99957131T	1999-06-11	Communication method and apparatus
GB0017365A	1999-06-11	Communication method and apparatus improvements
JP2000555459A	1999-06-11	Communication method and communication device

HU0102642A	1999-06-11	Communication apparatus and arrangement
RU2001101520/09A	1999-06-11	ADVANCED COMMUNICATION METHOD AND DEVICE
AU42518/99A	1999-06-11	Communication method and apparatus improvements
US09/594,016	2000-06-15	Communication method and apparatus improvements
FR0009330A	2000-07-17	IMPROVEMENTS TO COMMUNICATION METHODS AND APPARATUS
NO20006397A	2000-12-14	communication device
IS5770A	2000-12-14	Improvements in telecommunications method and equipment
ZA200100311A	2001-01-11	Communication method and apparatus improvements.
BG105146A	2001-01-12	Communication device
HK02108566.5A	2002-11-27	Communication method and apparatus improvements
US11/448,117	2006-06-07	Communication method and apparatus improvements

Legal Events

Date	Code	Title	Description
2000-03-16	NAA1	Application designating australia and claiming priority from australian document	**Ref document number:** 4251899 **Country of ref document:** AU

Data provided by IFI CLAIMS Patent Services

STRUCTURE COMPRISING AN ELECTRONIC DEVICE, IN PARTICULAR FOR THE MANUFACTURE OF A SECURITY OR VALUE DOCUMENT

Abstract

The present invention relates to a structure (1) for the manufacture of a security document or value, comprising: - an electronic device (8), - an at least partially fibrous interlayer (2) with a window (4) wherein at least partially extends the electronic device (8), - an adhesive layer (6) in contact with the intermediate layer.

Classifications

» G06K19/07722 Physical layout of the record carrier the record carrier being multilayered, e.g. laminated sheets

View 7 more classifications

FR2868987A1

France

Find Prior Art Similar

Other languages: French

Inventor: Sandrine Rancien, Frederic Vicentini

Current Assignee : ArjoWiggins SAS

Worldwide applications

2004 FR 2005 PL KR MX EP WO AR EP EP EP BR SA US 2010 SG

Application FR0403908A events

2004-04-14 Application filed by ArjoWiggins SAS

2004-04-14 Priority to FR0403908A

2005-10-21 Publication of FR2868987A1

2007-02-16 Application granted

2007-02-16 Publication of FR2868987B1

Status Active

2024-04-14 Anticipated expiration

Info: Patent citations (65), Cited by (45), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Patent Citations (65)

Publication number	Priority date	Publication date	Assignee	Title
US4428997A *	1979-12-26	1984-01-31	Polaroid Corporation	Protective coatings for documents
WO2002082126A1 *	2001-04-05	2002-10-17	Arjo Wiggins Security Sas	Self-adhesive document incorporating a radiofrequency identification device
WO2002089062A1 *	2001-04-26	2002-11-07	Arjo Wiggins Security Sas	Cover incorporating a radio frequency identification device
Family To Family Citations				
US3922424A *	1972-05-22	1975-11-25	Monsanto Co	Non-woven fibrous material bonded with ethylene/vinyl chloride interpolymers
DE2919649A1	1979-05-16	1980-11-20	Bbc Brown Boveri & Cie	SECURITY PAPER
FR2509767A1	1981-07-20	1983-01-21	Arjomari Prioux	NEW, LIGHTWEIGHT SYNTHETIC PRINTING PAPER AND PROCESS FOR PREPARING THE SAME
US4551909A *	1984-03-29	1985-11-12	Gte Laboratories Incorporated	Method of fabricating junction field effect transistors
US5216269A *	1989-03-31	1993-06-01	U.S. Philips Corp.	Electrically-programmable semiconductor memories with buried injector region
GB9211123D0	1992-05-26	1992-07-08	Amblehurst Ltd	Holographic device
GB9222460D0	1992-10-26	1992-12-09	Hughes Microelectronics Europa	Radio frequency baggage tag
GB2279907B	1993-07-02	1996-11-06	Gec Avery Ltd	An integrated circuit card

CA2122168A1 *	1993-12-16	1995-06-17	David P. Hultman	Polymer-reinforced paper having improved cross-direction tear
DE9422424U1	1994-02-04	2002-02-21	Giesecke & Devrient Gmbh	Chip card with an electronic module
DE4416697A1 *	1994-05-11	1995-11-16	Giesecke & Devrient Gmbh	Data carrier with integrated circuit
US5528222A *	1994-09-09	1996-06-18	International Business Machines Corporation	Radio frequency circuit and memory in thin flexible package
DE19601358C2	1995-01-20	2000-01-27	Fraunhofer Ges Forschung	Integrated circuit paper
DE19602821C1	1996-01-26	1997-06-26	Siemens Ag	Method for producing a data card
US6233818B1	1996-02-12	2001-05-22	David Finn	Method and device for bonding a wire conductor
DE19654902C2	1996-03-15	2000-02-03	David Finn	Smart card
US5786626A *	1996-03-25	1998-07-28	Ibm Corporation	Thin radio frequency transponder with leadframe antenna structure
FR2746939B1 *	1996-03-26	1998-05-22	Schlumberger Ind Sa	DEVICE FOR TRANSFERRING INFORMATION BETWEEN A PORTABLE OBJECT AND A READER
AU3433697A	1996-07-11	1998-02-09	David Finn	Method and device for manufacturing a chip card as well as chip card
US5895557A *	1996-10-03	1999-04-20	Kimberly-Clark Worldwide, Inc.	Latex-saturated paper
WO1998015916A1 *	1996-10-09	1998-04-16	Pav Card Gmbh	Method and connection arrangement for producing a smart card
US6111506A *	1996-10-15	2000-08-29	Iris Corporation Berhad	Method of making an improved security identification document including contactless communication insert unit
SE509570C2 *	1996-10-21	1999-02-08	Ericsson Telefon Ab L M	Temperature compensating means and procedure for mounting electronics on a circuit board
FR2768443B1	1997-09-15	1999-10-15	Arjo Wiggins Papiers Couches	COATED PAPER HAVING A WATCH-LIKE MARK AND MANUFACTURING METHOD
EP0905657B1	1997-09-23	2003-05-28	STMicroelectronics S.r.l.	Currency note comprising an integrated circuit
FR2769109B1 *	1997-09-26	1999-11-19	Gemplus Sca	DISPOSABLE CHIP ELECTRONIC DEVICE AND MANUFACTURING METHOD
FR2775533B1	1998-02-27	2003-02-14	Gemplus Sca	ELECTRONIC DEVICE WITH NON-CONTACT ELECTRONIC MEMORY, AND METHOD FOR MANUFACTURING SUCH A DEVICE
FR2776153B1	1998-03-10	2000-07-28	Ordicam Rech Et Dev	METHOD FOR SECURITY IDENTIFICATION OF A PERSON AND PORTABLE DEVICE FOR IMPLEMENTING THE METHOD
EP0950537A2 *	1998-04-13	1999-10-20	ARKWRIGHT Incorporated	A transparent recording sheet having an image-receptive coating, an anti-static coating, and a removable opaque anti-static adhesive strip
NL1008929C2 *	1998-04-20	1999-10-21	Vhp Ugchelen Bv	Substrate made of paper provided with an integrated circuit.
US6064855A *	1998-04-27	2000-05-16	Ho; Frederick Pak Wai	Voice book system
US6100804A	1998-10-29	2000-08-08	Intecmec Ip Corp.	Radio frequency identification system
DE19850853C1	1998-11-02	2000-03-16	David Finn	Identification label for surface fixture or wrap-around fixture to object comprises multi-layer structure with identification layer for optical designation, reinforcement layer
NL1010841C2	1998-12-18	2000-06-20	Enschede Sdu Bv	Method for manufacturing a booklet, booklet manufactured according to the method and booklet.
US6262692B1	1999-01-13	2001-07-17	Brady Worldwide, Inc.	Laminate RFID label and method of manufacture
AT198239T	1999-02-10	2001-01-15	Sihl Gmbh	RFID TRANSPONDER WITH PRINTABLE SURFACE
EP1049043A1 *	1999-04-30	2000-11-02	Siemens Aktiengesellschaft	Chip carrier structure
FR2796183B1	1999-07-07	2001-09-28	A S K	CONTACTLESS ACCESS TICKET AND MANUFACTURING METHOD THEREOF
US6395124B1	1999-07-30	2002-05-28	3M Innovative Properties Company	Method of producing a laminated structure
JP4588139B2	1999-08-31	2010-11-24	リンテック株式会社	IC card manufacturing method
FR2801707B1 *	1999-11-29	2002-02-15	A S K	METHOD FOR MANUFACTURING A CONTACT-FREE CONTACT HYBRID CHIP CARD WITH AN ANTENNA SUPPORT OF FIBROUS MATERIAL

FR2802684B1	1999-12-15	2003-11-28	Gemplus Card Int	DISPOSABLE INTEGRATED CIRCUIT CHIP DEVICE AND METHOD FOR MANUFACTURING SUCH A METHOD
ES2215152T3 *	2000-07-11	2004-10-01	X-Ident Technology Gmbh	LABEL OR SAFETY MARBETE WITH RFID TRANSPONDER.
EP1179811B1 *	2000-08-11	2008-10-15	European Central Bank	Security document and process for producing a security document
CN1208742C *	2000-12-04	2005-06-29	王子油化合成纸株式会社	Identifying mark and label with the identifying mark
FR2826154B1 *	2001-06-14	2004-07-23	A S K	CHIP CARD WITHOUT CONTACT WITH AN ANTENNA SUPPORT AND CHIP SUPPORT OF FIBROUS MATERIAL
US6894615B2 *	2001-10-09	2005-05-17	3M Innovative Properties Company	Article with retroreflective and radio frequency-responsive features
CA2652104C *	2001-12-24	2012-02-14	Digimarc Id Systems, Llc	Contact smart cards having a document core, contactless smart cards including multi-layered structure, pet-based identification document, and methods of making same
US6951596B2 *	2002-01-18	2005-10-04	Avery Dennison Corporation	RFID label technique
US6914747B2	2002-03-20	2005-07-05	Hitachi Global Storage Technologies Netherlands B.V.	Disk drive having electrostatic discharge path defined between disk assembly and base
JP2003331242A *	2002-05-10	2003-11-21	Konica Minolta Holdings Inc	Ic card
FR2840431B1 *	2002-05-29	2004-09-03	Francois Trantoul	METHOD AND DEVICE FOR PROTECTING READING INSTRUCTIONS
US20040069861A1 *	2002-10-09	2004-04-15	Teileen Jon B.	Removably attachable security devices
FI20022094A0	2002-11-25	2002-11-25	Rafsec Oy	Transponder and method for its manufacture
DE102004008841A1	2003-03-12	2004-09-23	Bundesdruckerei Gmbh	Security insert, to prevent forgery or tampering, at a book document e.g. a passport, has an integrated data carrier with a microchip which can be scanned without contact
WO2004080726A2	2003-03-12	2004-09-23	Bundesdruckerei Gmbh	Method for the production of a book cover insert and book-type security document and book cover insert and book-type security document
DE10338444B4 *	2003-08-18	2019-11-28	Smartrac Ip B.V.	Transponder inlay for a document for personal identification and method for its production
EP1517267A1	2003-09-19	2005-03-23	Axalto S.A.	Dual interface card
WO2005062246A1	2003-12-19	2005-07-07	Axalto Sa	Identification document
WO2005034031A1	2003-10-01	2005-04-14	Axalto Sa	Identification document
FR2863083B1	2003-12-02	2006-03-03	A S K	IDENTITY BOOKLET WITH RADIOFREQUENCY INDENTIFICATION DEVICE
WO2005104065A2 *	2004-03-29	2005-11-03	Avery Dennison Corporation	Security label, secured article and method for making the label and article

* Cited by examiner, † Cited by third party

Cited By (45)

Publication number	Priority date	Publication date	Assignee	Title
FR2895118A1 *	2005-12-15	2007-06-22	Arjowiggins Security Soc Par A	FILM FILM INCORPORATING A CHIP
FR2916558A1 *	2007-05-21	2008-11-28	Fasver Soc Par Actions Simplif	FLEXIBLE ADHESIVE SAFETY VIGNETTE WITH AT LEAST ONE CONTACTLESS MICROCIRCUIT FOR OFFICIAL DOCUMENT
FR2916559A1 *	2007-05-21	2008-11-28	Fasver Soc Par Actions Simplif	Flexible safety vignette for e.g. passport, has peripheral reinforcement chip comprising recess for receiving microcircuit, where chip is extended around microcircuit according to format lower than that of flexible support
FR2937162A1 *	2008-10-15	2010-04-16	Fasver	FLEXIBLE SAFETY VIGNETTE COMPRISING AT LEAST ONE MICROCIRCUIT
FR2965511A1 *	2010-10-05	2012-04-06	Oberthur Technologies	SECURITY DOCUMENT COMPRISING A NEAR FIELD COMMUNICATION DEVICE SUCH AS A PASSPORT
WO2017013313A1 *	2015-07-20	2017-01-26	Smart Packaging Solutions (S.P.S.)	Insert for a security document, in particular for a passport

Family To Family Citations

WO2004080726A2 *	2003-03-12	2004-09-23	Bundesdruckerei Gmbh	Method for the production of a book cover insert and book-type security document and book cover insert and book-type security document
DE102005021477B4 *	2004-10-14	2020-04-02	Pav Card Gmbh	Process for producing a laminate for a pass-inlay and identification document
US7581678B2	2005-02-22	2009-09-01	Tyfone, Inc.	Electronic transaction card
WO2007117261A2 *	2005-07-26	2007-10-18	Digimarc Corporation	Forensic feature for secure documents
JP2008009584A *	2006-06-28	2008-01-17	Matsushita Electric Ind Co Ltd	Touch panel
KR101478810B1 *	2006-07-28	2015-01-02	가부시키가이샤 한도오따이 에네루기 켄큐쇼	Power storage device
US8232621B2 *	2006-07-28	2012-07-31	Semiconductor Energy Laboratory Co., Ltd.	Semiconductor device
US7838976B2 *	2006-07-28	2010-11-23	Semiconductor Energy Laboratory Co., Ltd.	Semiconductor device having a semiconductor chip enclosed by a body structure and a base
PL2047414T3 *	2006-08-03	2014-03-31	Smart Packaging Solutions Sps	Secure document, in particular electronic passport with enhanced security
DE102006036286A1 *	2006-08-03	2008-02-14	Giesecke & Devrient Gmbh	Safety elements for antennas
US7991158B2	2006-12-13	2011-08-02	Tyfone, Inc.	Secure messaging
JP4888494B2 *	2007-02-06	2012-02-29	株式会社村田製作所	Packaging material with electromagnetic coupling module
FR2919409B1 *	2007-07-26	2009-09-04	Smart Packaging Solutions Sps	SECURE DOCUMENT WITH NON-CONTACT CHIP WITH DATA PROTECTION AGAINST UNAUTHORIZED READING.
US9741027B2	2007-12-14	2017-08-22	Tyfone, Inc.	Memory card based contactless devices
KR100949427B1 *	2007-12-14	2010-03-24	한국조폐공사	A security paper containing silk fiber and a method for discriminating the same
CN201222263Y *	2008-07-02	2009-04-15	黄石捷徽万达金卡有限公司	Crystal glue-dropping card
US7961101B2	2008-08-08	2011-06-14	Tyfone, Inc.	Small RFID card with integrated inductive element
US8451122B2	2008-08-08	2013-05-28	Tyfone, Inc.	Smartcard performance enhancement circuits and systems
EP2401708A4 *	2009-02-24	2012-08-15	Tyfone Inc	Contactless device with miniaturized antenna
US20100295286A1 *	2009-05-13	2010-11-25	Goldstein Keith E	Cover and method of manufacturing the same
WO2011030362A1 *	2009-09-14	2011-03-17	Paolo Stefanelli	Identification and tracking device that is flexible and resistant to chemical agents and high temperatures and pressures
FR2959842B1	2010-05-05	2012-05-04	Honnorat Rech S & Services	SECURE DOCUMENT, TESTER AND METHOD OF AUTHENTICATION.
FR2959843B1	2010-05-05	2013-01-25	Honnorat Rech S & Services	DISCRETE AUTHENTICATION DEVICE.
FR2962579A1 *	2010-07-12	2012-01-13	Ask Sa	RADIO FREQUENCY IDENTIFICATION DEVICE OF POLYCARBONATE AND METHOD OF MANUFACTURING THE SAME
US9061486B2 *	2010-12-06	2015-06-23	L-1 Secure Credentialing, Llc	ID documents having a multi-layered laminate structure
DE102011010127A1	2011-02-02	2012-08-02	Giesecke & Devrient Gmbh	Authenticity assurance of value documents by means of photochromic dyes
US8720776B2 *	2011-11-10	2014-05-13	Paul Llewellyn Greene	X-ray security system
JP6192897B2	2012-04-11	2017-09-06	サターン ライセンシング エルエルシーSaturn Licensing LLC	LIGHT EMITTING DEVICE, DISPLAY DEVICE, AND LIGHTING DEVICE
FR2995709A1	2012-09-18	2014-03-21	Arjowiggins Security	METHOD FOR MANUFACTURING ELECTRONIC CHIP STRUCTURE AND STRUCTURE THUS MANUFACTURED
GB2014055160D0	2014-03-27	2014-05-14	Rue De Int Ltd	Security booklet
GB2015013420D0 *	2015-01-27	2015-03-11	Univ Lancaster	Improvements relating to the authentication of physical entities
CN104933462B *	2015-05-05	2017-09-29	浙江立芯信息科技股份有限公司	The frangible label of car light

DE102015013621A1 *	2015-10-20	2017-04-20	Mühlbauer Gmbh & Co. Kg	Document book cover for a value and security document in the form of a book and method of making the same
US20170293830A1 *	2016-04-07	2017-10-12	Hazen Paper Company	Integrated electronic paper
US10111504782	2016-12-09	2018-10-30	Capital One Services, Llc	Transaction card with secured magnetic strip and method for making the same
JP6970927B2 *	2017-02-16	2021-11-24	大日本印刷株式会社	Information page
CZ30751686 *	2017-05-31	2018-11-07	Západočeská Univerzita V Plzni	A security card and a method of its authentication
DE102017007277A1 *	2017-08-01	2019-02-07	Giesecke+Devrient Mobile Security Gmbh	Data page made of hybrid material
US10204295B1	2017-09-12	2019-02-12	Graphene Security Limited	RFID security document

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
FR2868987A1	2005-10-21	STRUCTURE COMPRISING AN ELECTRONIC DEVICE, IN PARTICULAR FOR THE MANUFACTURE OF A SECURITY OR VALUE DOCUMENT
FR2877462B1	2007-01-26	STRUCTURE COMPRISING AN ELECTRONIC DEVICE FOR THE MANUFACTURE OF A SAFETY DOCUMENT.
WO2006026372A8	2007-03-29	Package having integral lens and wafer-scale fabrication method therefor
WO2007082966A3	2007-07-05	Integrated switch or integrated button
EP1511137A3	2005-07-27	Resonant cavity light emitting device
TW200707745A	2007-02-16	Insulation gate type semiconductor device and its manufacturing method
WO2005105472A3	2006-01-26	Improvements in substrates incorporating security devices
SG175571A1	2011-11-28	Lift installation for transporting lift users in a building area
TW200618361A	2006-06-01	Light-emitting-diode element with a light-emitting-diode chip
DE602004019855D1	2009-04-23	Security supervisor for an auxiliary computer attached to the telephone
FR2890378B1	2009-01-16	NACELLE HOOD FOR TURBOJET AND NACELLE COMPRISING AT LEAST ONE SUCH HOOD.
BR021270381	2012-08-21	bicomponent fiber.
FR2853165B1	2005-12-02	SENSOR ASSEMBLY, AND HOUSING FOR CARRYING OUT SUCH AN ASSEMBLY.
WO2005072290A3	2006-10-12	Methods of treating, reducing, or preventing autoimmune conditions
FR2868054B1	2006-06-02	DEVICE FOR PIVOTING A CONVEYOR, CONVEYOR EQUIPPED WITH SUCH A DEVICE, AND A VEHICLE OF THE CONCRETE TYPE EQUIPPED WITH SUCH A CONVEYOR
TR200302146T4	2004-02-23	Wheel for a crawler vehicle.
MA30562B1	2009-07-01	DEVICE FOR SECURING CONFIDENTIAL INFORMATION
FR2854730A1	2004-11-12	INTEGRATED CIRCUIT COMPRISING AT LEAST ONE METALIZATION LEVEL
FR2892843B1	2008-12-12	STRUCTURE COMPRISING AN ELECTRONIC DEVICE, IN PARTICULAR FOR THE MANUFACTURE OF A SAFETY OR VALUE DOCUMENT.
AR008218A1	1999-12-29	METHOD FOR PRODUCING A CUTTING BLADE FOR A THERMOPLASTIC RESIN PELLETIZER
ES1056145Y	2004-06-01	LEVER OF THE CAPE OF A CAR.
FR2872093B3	2006-05-26	PERFECTIONED ROOF COVER FOR A MOBILE RESIDENCE, A CARAVAN OR THE LIKE
FR2830039B1	2005-01-07	DORMANT FRAME, PROVIDED WITH THERMAL BRIDGE BREAKING MEANS, METAL JOINERY FOR WINDOW
EP1310993A3	2003-07-16	Method for enhancing the electric connection between a power electronic device and its package
AT254672T	2003-12-15	REFINING PRECIOUS METAL CONCENTRATES BY CHLORINE

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
FR0403908A	2004-04-14	2004-04-14	STRUCTURE COMPRISING AN ELECTRONIC DEVICE, IN PARTICULAR FOR THE MANUFACTURE OF A SECURITY OR VALUE DOCUMENT

Applications Claiming Priority (14)

Application	Filing date	Title
FR0403908A	2004-04-14	STRUCTURE COMPRISING AN ELECTRONIC DEVICE, IN PARTICULAR FOR THE MANUFACTURE OF A SECURITY OR VALUE DOCUMENT
US11/578,520	2005-04-14	Structure including an electronic device, in particular for fabricating a security document or a document of value
EP05747071.8A	2005-04-14	Structure comprising an electronic device particularly for the production of a security or value document
PL05747071T	2005-04-14	Structure comprising an electronic device particularly for the production of a security or value document
KR1020067023763A	2005-04-14	Structure comprising an electronic device particularly for the production of a security or value document
CA2562587A	2005-04-14	Structure comprising an electronic device particularly for the production of a security or value document
ARP050101463A	2005-04-14	STRUCTURE INCLUDING AN ELECTRONIC DEVICE, PARTICULARLY FOR THE MANUFACTURE OF A SECURITY OR VALUE DOCUMENT
EP20100176926	2005-04-14	Structure comprising an electronic device, in particular for manufacturing a security or value document
EP17189404.1A	2005-04-14	Structure comprising an electronic device, in particular for manufacturing a security or value document
BRPI0509985-6A	2005-04-14	structure for the manufacture of a security or value document, security or value document, process of manufacturing a structure for the manufacture of a security or value document, process for producing a security or value document, structure and security document
MXPA06011897A	2005-04-14	Structure comprising an electronic device particularly for the production of a security or value document.
PCT/FR2005/050240	2005-04-14	Structure comprising an electronic device particularly for the production of a security or value document
EP20100176939	2005-04-14	Structure comprising an electronic device, in particular for manufacturing a security or value document
US12/923,753	2010-10-06	Structure including an electronic device, in particular for fabricating a security document or a document of value

Legal Events

Date	Code	Title	Description
2009-10-23	TP	Transmission of property	
2016-04-21	PLFP	Fee payment	**Year of fee payment:** 13
2017-04-19	PLFP	Fee payment	**Year of fee payment:** 14
2018-04-20	PLFP	Fee payment	**Year of fee payment:** 15
2020-03-26	PLFP	Fee payment	**Year of fee payment:** 17
2021-03-25	PLFP	Fee payment	**Year of fee payment:** 18

Data provided by IFI CLAIMS Patent Services

Patents FI99071C

FI99071C -- Procedure for use of applications in a mobile telephone as well as a mobile telephone

Procedure for use of applications in a mobile telephone as well as a mobile telephone

Abstract

The invention relates to a mobile radio communication unit, comprising a controller (MCU) and at least one storage device (6). The at least one storage device stores at least one application program and identification information, wherein the identification information identifies a user of said mobile radio communication unit. And the mobile radio communication unit comprises an interface (7,23,8) coupled to the controller (MCU), the interface being for mechanically and electrically coupling to the at least one storage device. The at least one storage device is attachable to the interface (7), wherein while the interface is mechanically and electrically coupled to the at least one storage device, the controller is electrically coupled to the at least one storage device, and the application program is adapted to send messages to another application via the interface.

Classifications

G07G1/12 Cash registers electronically operated

View 35 more classifications

FI99071C

Finland

Download PDF Find Prior Art Similar

Other languages: Finnish, Swedish

Inventor: Mikko Terho, Petri Heinonen, Matti Marttila, Markku Rautiola

Worldwide applications

1995 FI 1996 US JP AU EP CN EP ES DE WO EP CN 1998 US US 2001 CN 2002 US 2004 US 2005 JP US 2006 JP

Application FI950685A events

1995-02-15 Application filed by Nokia Mobile Phones Ltd

1995-02-15 Priority to FI950685A

1995-02-15 Publication of FI950685A0

1996-08-16 Publication of FI950685A

1997-06-13 Application granted

1997-06-13 Publication of FI99071B

1997-09-25 Publication of FI99071C

2010-12-29 First worldwide family litigation filed

Show all events

Info: Patent citations (164), Cited by (531), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (14)

Hide Dependent

17 99071

A method for using an application (18) in a mobile station (1), 5 characterized in that the application has a first operating mode and a second operating mode, wherein the first operating mode is passive and in the second operating mode the application controls the central processing unit.

Method according to claim 1, characterized in that the application (18) is a debit card application.

Method according to claim 1, characterized in that the application (18) is a payment card application.

Method according to claim 1, characterized in that the application (18) is a credit card application.

Method according to Claim 1, characterized in that the mobile stations (1) communicate with one another by means of the first data transmission means IR.

Method according to Claim 1, characterized in that AT commands are used to control the central processing unit (MCU) of the mobile station. 25

Method according to Claim 1, characterized in that the central processing unit (MCU) of the mobile station (1) has two operating modes: - normal mode, and - application mode. 30

Method according to Claim 1, characterized in that the application (18) is of the power-up type, a menu type or an automatic type.

Mobile station (1) with means for operating the application (18), characterized in that the mobile station further comprises 99071 18 means (CPU, DATA-I / O, I / O, I / O ', I / O ", 14) for setting the application (18) to the first mode of operation, means (CPU, DATA-I / O, I / O, I / O ', I / O ", 14) for setting the application (18) to the second mode of operation, and 5 - means (CPU, DATA-I / O, I / O, I / O ', I / O ", 14) for controlling the MCU of the mobile station.

Mobile station (1) according to claim 9, characterized in that the mobile station (1) further comprises means (IR) for infrared data transmission.

Mobile station (1) according to claim 9, characterized in that the mobile station (1) further comprises means (19) for connecting the mobile station (1) to a computer. 15

Mobile station (1) according to Claim 9, characterized in that the mobile station (1) is a GSM mobile telephone.

Mobile station (1) according to claim 9, characterized in that said control units of the central processing unit are located in the application (18).

A system for making payments, characterized in that the system comprises 25. at least one mobile station (1) having - an application (18), - means for operating the application (18), and - first data transmission means (IR, 20, RF) for local data transmission for, 30. at least one cash register (21) or the like having second communication means (IR2), and; - the application (18) comprises means for transferring information between the first communication means (IR) and the second communication means (IR2). 19 99071

Description

99071

A method for using applications in a mobile station and a mobile station

The invention relates to a method for using applications in a mobile station, a mobile station and a system for making payments.

5

Mobile stations are now known in which the control card comprises a subscriber identification unit, such as a SIM module (Subscriber Identity Module), which comprises a control unit (CPU, Central Prossing Unit), program memory (ROM), read only memory (EEPROM, Electrically Erasable Programmable Read Only Memory) and Random Access Memory (RAM). To use a mobile station, you need to enter a personal identification number stored on the SIM module when using the mobile station, usually by switching on the mobile station. Other user-specific information, phone numbers, messages, etc. can also be stored in the data memory of the SIM module.

Nowadays, mobile stations have also been developed with a data connector for connecting an external data processing device, for example a laptop computer. In this case, the mobile station can be used as a data transmission medium between the laptop computer and some other data processing device via the mobile network. In this way, it is possible to contact, for example, the user's bank to monitor account information and make payments. However, such a system is quite cumbersome to use because a separate cable is required between the computer and the mobile station. In addition, the computer must be available when, for example, a bank connection is desired.

Today, your wireless is also known! functional smart cards, which are mainly used in payment applications such as bus travel payments and payphones. Such smart cards consist of e.g. central processing unit, program memory and data memory. The central unit controls the internal operation of the smart card in card usage situations according to the program code stored in the program memory. The data memory is used as a storage medium for information according to the purpose of the smart card, such as the monetary value of the smart card 35. To perform a payment transaction, the card also has data transmission equipment, such as a transmitter / receiver based on electromagnetic induction. The disadvantage of such smart cards is e.g. the fact that 99071 2 more different smart cards may be needed for different payment situations, so the number of smart cards to carry can be quite large. In addition, when the cash balance stored on the smart card expires, a new card must be purchased or an additional cash balance must be purchased for the used card at one of the sales-5 points that provide a replenishment service.

Japanese Patent Application JP 4,083,447 discloses a mobile station to which it is possible to add some features by means of a separate memory card. Such an application is preferably arranged for a specific use, such as to increase storage capacity or telephone number memory. Such applications are based on the central processing unit of the mobile station reading the data stored in the applications (memory cards) and acting as required by this data. The weakness of this method is e.g the fact that the mobile central processing unit must be pre-programmed with the functions necessary to perform the functions according to the different applications, in which case the development of new applications also requires changes in the mobile central processing unit software.

International patent application WO 91/12698 discloses a mobile station 20 to which features can be added by means of a separate additional card, such as a smart card. In this way, the use of the telephone can be restricted, for example, by barring international calls, long distance calls or calls to service numbers. Information on call restrictions is stored on an additional card that the user must install in the mobile station for 25 years of use of the mobile station. Thus, this method can only essentially limit the use of the features belonging to the mobile station.

In order to eliminate the above-mentioned drawbacks and to increase the state of the art in the art, it is an object of the present invention to provide a new method for using applications in a mobile station. The application is preferably arranged for a specific use, such as a credit card, debit card or electronic money. The application is preferably formed in an application module, which in terms of technical solutions may be similar to the above-mentioned SIM module. There can be several applications in the same application module. The application module is usually connected to a module card 99071 3 of a certain size made of plastic or similar material, so that an application module connector is arranged in connection with the application module for conducting the necessary buses from the mobile station to the application module. At the same time, the module card can have several application modules, in which case each application module has its own application module connector. The application module connectors of the mobile station are operatively connected to the application module connectors of the respective module cards.

Each module card is connected to a module card connector arranged in a mobile station, to which an application module connector is connected.

The invention is based on the idea that applications with a first operating mode and a second operating mode can be connected to a mobile station. The application in the first mode of operation does not actively do anything itself, but is as if in the background, passive. The application in the second operating mode is active and can control e.g. mat-15 coffee machine headunits. The application in the second mode of operation also has at its disposal those peripheral devices known to the mobile station, such as a display, a keyboard and status indicators, which the application has requested to use when switching to the second mode of operation.

There can preferably be three different types of applications used in the method according to the invention, depending on the situation in which the application can switch to another mode of operation: 1) the so-called power-up type, in which the application switches to another operating mode as soon as possible after switching on the mobile station and / or inserting the module card, 2) menu type, where the user can choose the application he wants to be active from the menu, and 3) an automatic type in which an application enters another mode of operation after a condition defined for the application is met. The automatic type can also be selected from the menu. The selection from the menu can also be considered in a situation where several power-up type applications are connected to the mobile station, one of which can switch to another operating mode. The method according to the invention is characterized in that the application has a first operating mode and a second operating mode, in which case in the first operating mode the application is passive and in the second operating mode the application controls the central unit of the mobile station. The mobile station according to the invention is characterized in that the mobile station further comprises 99071 4 means for setting the application to a first mode of operation in which the application is passive, means for setting the application to a second mode of operation in which the application is active, and 5 means for controlling the mobile station's central unit. toimintamoo-oxide.

The present invention provides significant advantages over prior art solutions. With the aid of the present invention, the possibilities of using a mobile station can be considerably increased. Mobile communications can also be used as a credit and / or debit card and instead of cash. Mobile communications can also be used to collect and present information such as schedules, stock quotes, exchange rates, etc. With the mobile station according to the invention, payments can be made in the store, e.g. directly from the account of the user of the mobile station, in which case no cash is required.

The invention will now be described in more detail with reference to the accompanying drawings, in which Figure 1 shows a block fault of a mobile station according to the invention, Figure 2 shows the electrical structure of an application module bus between an application module connector unit and a central unit Fig. 3a is a block diagram of the internal structure of a mobile control card, Fig. 3c shows a module card connected to two 35 application modules, Figs. 4a and 4b show a flow chart of the application from the first mode to the second mode, as a simplified diagram, Fig. 6 shows the use of the method according to the invention in connection with a payment card application, Fig. 7 shows two mobile stations according to the invention communication between the

In the application example of Figure 1, the card-controlled mobile station 1 consists of e.g. the central processing unit MCU, the user interface UI, the high frequency part RF, the low frequency part AUDIO, the power unit 2, the first communication means 15 IR and the application module connector unit 6. The functions of my mobile station are controlled by the central processing unit MCU with program code for storing various functions.

The user interface UI consists of e.g. even from current mobile stations, the display 7, the keypad 8 and the status indicators 23 are supported. The central unit generates various contextual messages, operating instructions, menus, etc. on the display 7. The keypad 8 allows the user to enter various information on the mobile station, such as PIN and phone number. The status indicators 23 can advantageously be used to detect the internal operating states of the mobile station 1.

The high frequency part RF is a transmitter and receiver unit belonging to a mobile station, known per se, which the mobile station uses to transmit and receive calls and messages on radio frequencies in a mobile communication network, such as a GSM network, via a mobile switching center MSC.

The low frequency part AUDIO preferably consists of a microphone 9, a headphone 10 and a buzzer 11 or the like.

35 6 99071

The operating energy required by the mobile station 1 is obtained from the battery 12 in the mobile station 1, which is charged if necessary. Power unit 2 monitors e.g. 12 battery charges and charging. The power unit 2 transmits the information to the central processing unit MCU when the state of charge of the battery 12 falls below a predetermined value, whereby the central processing unit MCU preferably notifies this by a buzzer 11 and / or a message 7 to be printed.

A module card 13 such as that shown in Figure 3a is connected to the module card connector (not shown). The module card 13 may have e.g. the control card SIM used for authentication 10. Application module connectors are arranged on the application modules 19 in the module card 13. Figure 3b shows the internal structure of the control card SIM in a reduced block diagram. The control unit CPU controls the operation of the control card SIM on the basis of the program code stored in the program memory ROM. The data-15 memory EEPROM can store various user-specific information, which is retained even if the control card SIM is removed from the application module connector unit 6. During the operation of the control card, the RAM can be used as a temporary data storage location. The bus adapter DATA-I / O adapts the control card to the SIM application module bus 14 and 20 to the control and data lines I / O.

It is also possible to connect other module cards 13 to the application module connector unit 6 of the application example of Fig. 1, in which case they are preferably attached to their own module card connectors. The application module 19 on the module card 13 may have a mechanical and electrical structure similar to the control card SIM shown in Figures 3a and 3b. From the application module connector unit 6 to the central unit MCU of the mobile station, there is an application module bus 14 by means of which the application modules 19 connected to the application module connector unit 6 communicate with the central unit MCU. In the transmission of data and commands, e.g. AT commands that are known e.g. most common modems. AT commands are described in more detail in Petri Heinonen's thesis Proposal for Standard AT Commands Used with GSM Mobile Equipment, Master of Science Thesis, 1994, Tampere University of Technology.

In addition to the application module bus 14, each application module connector 15, 16, 17 of the application module connector unit 6 has a separate control and data line I / O, I / O ', I / O "(Figure 2) to the central processing unit MCU. In this case, the control and data line 35 99071 7 I / O, I / O ', I / O "It is possible to use a structure based on the standard series ISO 7816. The standard series ISO 7816 presents e.g. voltage levels and timing diagrams according to which the application modules 19 are related to the control and data line I / O, I / O ', I / O ".

5

The application module connector unit 6 has a connector for each application module 19, through which the application module bus 14 is routed to the application module 19.

Several application modules 19 can also be connected to the same module card 13, as shown in Figure 3c. The second application module 19 'on the module card 13 can also be e.g. a SIM module.

The first data transmission means IR 15, such as an infrared transmitter / receiver, are also formed in the mobile station 1. The first data transmission means IR can be used for data transmission at close distances, e.g. in a store when making a payment.

The maximum communication means IR may also include a data connector 20, which 20 can be used to connect a computer to the mobile station 1.

Figures 4a and 4b show how application 18 is enabled, disabled, and how application 18 is changed from the first mode of operation to the second and vice versa. By the first operating mode-25a is meant a state in which the application does nothing on its own initiative, but receives its operating instructions through the application or the central processing unit MCU in the second operating mode. The second mode of operation in this description means a control mode, in which case an application in the second mode of operation has the possibility to control the operation of different units of the mobile station 1, including the central unit MCU, and send messages to other applications.

The central processing unit MCU can also have two different operating modes: 1) normal mode and 2) application mode. In the normal mode, the central processing unit MCU operates like a known mobile station 1. In the application mode, the central processing unit MCU may be controlled by an application 18 in another operating mode. Even in the application mode, the central processing unit MCU can read the keyboard 8 and transmit information about the key press 99071 8 to the application 18 in the second operating mode, if the application 18 in the second operating mode so wishes.

In the example of Figure 4, the operation starts by switching on the mobile station 1 5, after which the central processing unit MCU sets the control and data line I / O of the first application module connector 15 to a reset state (block 101). If an application module 19 is connected to the first application module connector 15 and sends an acceptable response to the central processing unit MCU (block 102), the central processing unit MCU sets the control and data line I / O enable state of the first application module connector 15 (block 103). In block 104, the CPU MCU determines whether all application module connectors 15, 16, 17 have been examined. If all the application module connectors 15, 16, 17 have not yet been examined, the operation proceeds again to step 101, where the next application module connector 16, 17 is now examined. If in block 15 the central processing unit MCU does not receive a response at all or the response is not acceptable, the operation proceeds to block 105, where the central processing unit MCU concludes that no application module 19 is connected to the examined application module connector 15, 16, 17.

After all the application module connectors 15, 16, 17 have been traversed, the operation continues in block 106, where user identification known per se is performed. If user authentication fails, the mobile station start-up is stopped (block 107). There are usually three ways for a user to enter their own personal identification number. Mi-25 If the access code is not entered correctly the third time, the user must enter a longer identification code, after which the user has three more opportunities to enter

his or her own personal access code correctly. If the user does not enter his passcode correctly in these three additional fields either, the user must enter a longer passcode again. If the 30 key figures are not entered correctly within the permitted attempts, the control card will destroy the information it contains, making the control card SI M unusable.

After successfully entering the personal identification number 35, the central processing unit MCU proceeds to block 108, where the central processing unit MCU queries for information about the applications 18 contained in the application module 19 connected to the first application module connector 15. If there are 18 applications in the application module 19, the central processing unit MCU reads

9 99071 applications 18 data (block 109) and store them in its memory (block 110).

If there are no applications 18 in the examined application module 19, the central processing unit MCU stores this information in its memory (block 111). In block 112, the central processing unit MCU determines whether all 5 application modules 19 have been examined. If there are still unexplored application modules 19, the operation returns to block 108, where information about the applications 18 contained in the next application module 19 is now queried.

After the central processing unit MCU has examined all the application modules 19, the operation 10 continues after block 112 in block 113, where the central processing unit MCU displays a menu on the mobile station 1 display 7 from which the user can select the application 18 he wants to switch to another operating mode. If the user selects an application 18, the CPU MCU asks for the parts of the user interface UI required by the selected application 18, such as the display 7, the keyboard 8 and / or the status indicators 26. If the CPU MCU does not receive an acceptable response from the selected application 18, the operation returns to block 113. In the event that the central processing unit MCU receives an accepted response from the selected application 18, the central processing unit MCU 20 enters the application mode, i.e., to control the selected application 18 (block 115).

If the user does not select the application 18 (block 113), the central processing unit MCU enters the normal mode (block 116), whereby no application 18 controls the central processing unit MCU 25, but all the applications 18 are in the first operating mode.

In the normal mode, in block 117, the central processing unit MCU may form a menu 7 of the 30 selectable applications 18 on the application modules 19 of the mobile station 1, from which the user can select the application 18 he wants to switch to another mode of operation (block 118). If the module card 13 is removed from the module card connector, all applications 18 on the removed module card 13 are removed from the menu of the mobile station 1 (block 128).

In block 118, the central processing unit MCU queries the applications 18 contained in the selected application module 19. If the central processing unit MCU receives an acceptable response from the application module 19, the central processing unit MCU ignores applications such as Wer up type 18 but stores information from other applications 18 (block 119). If the central processing unit MCU does not receive an acceptable response from application 18, no new applications 18 are added (block 120).

5 If the CPU MCU is in normal mode in block 116 and the user selects one of the selectable applications 18 from the menu, or an automatic type application 18 notifies the CPU MCU to switch to another mode, the CPU MCU asks the UI unit 1 required by the application 18 to switch to another mode (block 121). If the application 18 does not receive an acceptable response from the central processing unit MCU, the operation of the central processing unit MCU proceeds to block 117. If the application 18 receives an acceptable response from the central processing unit MCU, the central processing unit MCU enters application mode (block 115).

15

When the central processing unit MCU is in application mode (block 115) and the condition for transitioning to another mode of operation of an automatic type 18 application is met, the application 18 in second mode of operation is currently asked if the application of type auto type 20 can switch to another mode of operation (block 122). If handover is not allowed, operation returns to block 115. If handover is possible, the central processing unit MCU asks the application 18 of the automatic type which units of the user interface UI of the mobile station 1 it needs (block 123). If the answer is incorrect, the operation of the central processing unit MCU returns to block 115. If the response is acceptable, the application 18 of the automatic type switches to the second operation mode and at the same time the application 18 in the second operating mode switches to the first operation mode.

If the module card 13 in which the applications 18 of the application modules 19 in the first operating mode are in the module is removed from the module card connector, these applications 18 are deleted from the menu.

If a new module card 13 is added to the mobile station 1, the identifiers of the applications 18 of the application modules 19 on the module card 35 are queried in block 125. If the application module 19 sends the identifiers to the MCU, discards power up applications 18 and stores other applications 18 in the application module 19 in block 990 11 126. If no acceptable response is received from application module 19, no application module information is added (block 127).

If a module card 13 with a power up-type or automatic-type application 18 in the operating mode 5 is removed from the module card connector, the mobile station 1 is switched off.

Otherwise, the application 18 is switched to the first operating mode and the central processing unit MCU returns to the normal mode (block 116). The menu or automatic type application 18 in the second mode of operation may also return automatically or in a user-controlled manner to the first mode of operation (129).

The following describes in principle the operation of a bank or other payment card application in a mobile station 1 implemented by the method 15 according to the present invention (Figure 6).

Connected to the mobile station 1 is both a control card SIM and one application module 19, in which an application 18 is formed, which in this example is a bank card application. The application 18 has at least one account corresponding to the user's bank account, whereby the user can e.g. make payments from the account in app 18. The account information is preferably read from the bank account during the implementation phase of the application 18 and stored in the data memory EEPROM belonging to the application module 19 used by the application 18. In connection with the payment, the application 18 reduces the balance of the account in the application 18 accordingly. The updating of payment transactions, etc. in the application 18 to the user's bank account can advantageously take place automatically controlled by the application 18, e.g. at a certain time, and / or selected by the user from the menu of the mobile station 1, and / or in connection with the payment. In the bank account update phase, the application 18 30 controls the central processing unit MCU to establish a communication connection via the mobile network MSC and usually the fixed telephone network PSTN to the bank computer 22. The connection may be established by first asking the user for a telephone number or by using a number stored in the application's memory, the better.

99071 12

In the mobile station 1, the user can have several different accounts at the same time, such as a bank account, a credit account and / or a cash account, which can also be in different applications 18, even in different application modules 19. This has the advantage of e.g.

5 the fact that the user can transfer money between accounts, e.g., from a credit account to a bank account or a cash account.

The application 18 is activated e.g. after the mobile station 1 has been switched on, as shown in the flow chart of Figures 4a and 4b. The CPU-10 is printed by the MCU to display 7 messages for entering the passcode. The user enters his own code, which is read by the central processing unit MCU and transmitted to the control card SIM. The control unit CPU on the control card SIM examines the given code by comparing it with the previously stored code and informs the central unit MCU whether the code has been entered correctly. If the passcode was not correct, the MCU may possibly ask the user again to enter the passcode.

If the passcode is entered correctly, the central processing unit MCU operates according to the above steps. Since the other terminals 16, 17 do not have other application modules 19 in this application example, the central processing unit MCU displays a menu 7 from which the user can select the application 18 in the application module 19, which is a debit card application, after which the application 18 switches to another operating mode and the central processing unit MCU enters application mode.

25

The mobile station 1 can be used to make a call in the usual way. All other functions belonging to the mobile station 1 are also available. The essential difference here is that when a user enters, for example, a telephone number from the keypad 8, the central processing unit MCU forwards keystrokes to an application in the second operating mode, which controls the central processing unit MCU to establish a connection.

If the user wants to inquire about the balance of his bank account, he first selects the menu function using the keypad 8, in which case the central processing unit MCU transmits a keystroke to the application 18. The application 18 controls the central processing unit MCU to display a menu 7 from which 99071 13 can be selected. After the user selects the balance inquiry from the menu, the central processing unit MCU transmits a keystroke to the application 18, which examines it and sends a message to the central processing unit MCU to display 7 a text informing the user that the mobile station is performing a balance inquiry. Next, the application 18 retrieves the balance stored in the data memory EEPROM of the application module 19 and generates a message based thereon by which the central processing unit MCU prints the balance on the display 7.

10 The following is an example of implementing the above balance inquiry using AT commands:

Event code. + ckev: 91.1 AT command: AT + CDIS = "NOKSET", "View A", "menu v" "Quit" 15 AT command: at + cind = „„ 11,11 (update indicators)

Event code: + CKEV: 91.0

Event code: + ckev: 49.1 AT command: at + cind = „„ 11.1

Event code: + CKEV: 49.0 20 Event code: + ckev: 53.1 AT command: at + cind =„ „ 1,5

Event code: + CKEV: 53.0 AT command: AT + CDIS = "NOKSET", "Amount of", "balance", "", "OK", "Quit" AT command: at + cind =„„ , o, o 25 Event code: + CKEV: 91.1: AT command: AT + CDIS = "NOKSET", "Requesting. ", "Quit"

Event code: + CKEV: 91.0 AT command: AT + CMGS = "12345678" Request amount of balance messaged

Event code: + cmt text: "12345678", FIM 12,125,122,32.69 0.0.0„ 94102610100058,8, AT command: AT + CDIS = "NOKSET", 11 You have "," FIM 125232,69 " „ "Quit"

Payments from the account can also be easily made by entering 35 the appropriate information on the keypad of the mobile station 8.

99071 14

An example of an application of the method according to the invention will be described below, in which the application 18 is a cash application by means of which some payments can be made, such as in a shop or on a bus.

5 Application 18 is identified as shown in the previous example. Once the application 18 has switched to another mode of operation, the user can connect to the bank's computer 22 on the mobile station 1 and transfer money from his own account to the cash application. In practice, of course, money is not transferred concretely but electronically, which increases the balance of the payment card and the balance of 10 bank accounts. The user executes internal transfers from the bank account of the payment application to a cash account on the mobile station 1 or vice versa. Internal credit transfers require that the credit transfer information be updated on the bank's computer 22.

15 The payment is made by the user entering a certain code with which he informs the application 18 that he wants to pay for the purchases. The application then establishes a connection via the central processing unit MCU to the first communication means IR, such as an infrared transmitter / receiver or the like. Connected to the cash register 21 or the like 20 are other data transmission means IR2, such as an infrared transmitter / receiver, through which the application 18 and the cash register application of the cash register 21 can be in communication with each other.

Once the connection is established, the user enters the 25 PIN of his own payment card, which the payment card application still compares with the pre-stored one. If the code is entered correctly and there is a sufficient balance in the application 18, the payment transaction is registered both in the cash register 21 and in the application 18 of the mobile station, whereby the balance on the payment card is reduced accordingly. The update of the payment transaction to the bank's information machine 30 can take place either from the cash register application or from the application 18 of the mobile station 1.

For infrared data transmission, it is advantageous to use some known standard, such as the protocol stack (infrared Data Assosia-35 tion) defined by IrDA, which is based on the ISO OSI model (Open Systems Interconnection). The protocol stack uses the layers of the OSI model. 1) the physical layer, 2) the data link layer, 3) the network layer, and 7) the application layer.

99071 15

At the physical layer, data transmission can be based on infrared, but other known data transmission methods can also be used, such as ultrasound, electromagnetic induction or radio waves.

5 In the data link layer, e.g. verification of data transmission with, for example, error correction algorithms. In addition, the functions of the data link layer are performed e.g. identification of data transmission means in situations where there may be several data transmission means in operation at the same time, e.g. in shops with several cash register applications.

10

In the network layer, messages passing through the communication means can be distributed to the correct recipient, regardless of the number of communication means in operation. In addition, encryption of the information to be transmitted can be established in the network layer, which is especially important in payment applications.

The application 18 relates to data transmission via an application layer, where the application 18 transmits and receives the information and commands required for data transmission via the MCU of the mobile station, preferably to the first data transmission means IR, or to the mobile network.

Correspondingly, the second device participating in the data transmission, such as the cash register 21, has a cash register application which processes the messages received via the second data transmission means IR2 according to the above-mentioned layer structure 25.

Figure 5 shows a short diagram of the call flow between the application APPLICATION and the mobile switching center MSC belonging to the mobile communication network. In step 200, the application transmits the called telephone number to the mobile station central processing unit MCU, which transmits to the mobile switching center MSC the identification information and other necessary information for establishing a connection (steps 201, 202 and 203). The mobile switching center MSC transmits to the mobile station 1 information about the progress of the call (step 204) and the connection establishment (step 99071 16 205), after which the mobile station 1 sends an acknowledgment of the connection establishment to the mobile switching center MSC (step 206) and the application 18 (step 207). To end the connection, the application 18 sends a disconnect command to the mobile station central processing unit MCU 5 (step 208), which sends a disconnection request to the mobile switching center MSC (step 209). To the mobile switching center, the MSC sends an acknowledgment of the disconnection to the mobile switching center MCU (step 210). Finally, the mobile unit central processing unit MCU sends to the application 18 information that the connection has been disconnected (step 211).

10

The method according to the invention can be used for applications other than those related to payments. For example, schedule information and stock quotes can be retrieved to the mobile station 1.

Figure 7 shows an application in which two mobile stations 1 communicate with each other by means of the first data transmission means IR.

The method according to the invention enables a flexible way to increase the usability of the mobile station 1. The mat-20 coffee machine 1 according to the invention may have several providers of different functions which manufacture and sell applications 18. For credit card companies, such a method is one way to reduce abuses in credit card payments.

The invention is not limited only to the embodiments described above, but the invention can be modified within the scope of the appended claims.

Patent Citations (164)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
US3713148A	1970-05-21	1973-01-23	Communications Services Corp I	Transponder apparatus and system
US4189712A	1977-11-09	1980-02-19	Lemelson Jerome H	Switch and lock activating system and method
US4277837A *	1977-12-30	1981-07-07	International Business Machines Corporation	Personal portable terminal for financial transactions
US4305059A *	1980-01-03	1981-12-08	Benton William M	Modular funds transfer system
US4456414A *	1982-06-16	1984-06-12	Vericard Corporation	Funds transfer system using optically coupled, portable modules
GB8524020D0	1985-09-30	1985-11-06	British Telecomm	Electronic funds transfer
US5468947A	1986-08-08	1995-11-21	Norand Corporation	Pocket size data capture unit with processor and shell modules
JPS6427328A	1987-03-20	1989-01-30	Iwatsu Electric Co Ltd	Portable telephone system
US4880097A	1987-04-16	1989-11-14	Pom Incorporated	Park card system for electronic parking meter
US4823928A	1987-04-16	1989-04-25	Pom Incorporated	Electronic parking meter system
US5127040A *	1987-06-02	1992-06-30	Motorola, Inc.	Radiotelephone telephone number down loading
US4860336A *	1987-06-02	1989-08-22	Motorola, Inc.	Radiotelephone credit card data communications
DE3811277T1	1987-07-31	1989-08-24	Texas Instruments Deutschland Gmbh, 8050 Freising, De	TRANSPONDER ARRANGEMENT.
JP2753565B2	1988-01-26	1998-05-20	日立マクセル株式会社	IC card data transmission method
FR2636154B1	1988-09-08	1991-04-19	Regie Autonome Transports	NON-CONTACT INFRARED PEARING PROCESS BY MEMORY CARD, PARTICULARLY FOR MEANS OF TRANSPORT, AND PEARING DEVICE USING SUCH A METHOD
CA1317638C *	1988-09-09	1993-05-11	Stephen B. Meads	Mobile pay telephone system
US5134717A *	1988-11-26	1992-07-28	Motorola, Inc.	Radio telephone with repertory dialer
US4965821A *	1988-12-23	1990-10-23	Gte Mobilnet Incorporated	Cellular mobile radiotelephone-based system for rental of mobile equipment
FR2641635A1	1989-01-06	1990-07-13	Heckmann Antoine	Method of paying parking charges by infrared radiation and prepaid card and device for implementing it
JPH02305159A *	1989-05-19	1990-12-18	Toshiba Corp	Radio telephone set

US5068891A *	1989-05-31	1991-11-26	Marshall Marvin E	Credit control system for long distance telephone services
US5077832A	1989-08-07	1991-12-31	Ericsson Ge Mobile Communications Inc	Radio transceiver with optional display
US5023936A	1989-08-07	1991-06-11	General Electric Company	Method and apparatus for externally defining the operational mode of a digital radio transceiver
US5175759A *	1989-11-20	1992-12-29	Metroka Michael P	Communications device with movable element control interface
DE69112234T2	1990-01-30	1996-04-04	Visa Int Service Ass	International authorization system.
GB2241133A	1990-02-14	1991-08-21	Motorola Inc	Radiotelephone having removable memory means for storing radio user validation code
FI888420 *	1990-03-22	1993-07-12	Nokia Mobile Phones Ltd	Checking the card connection
JPH03273465A	1990-03-23	1991-12-04	Yokogawa Electric Corp	Wireless type charge paying device of charge prepayment system and portable medium
US5241410A *	1990-06-21	1993-08-31	Litephone Systems Ltd.	Enhanced infrared-connected telephone system
JPH0483447A	1990-07-26	1992-03-17	Tamura Electric Works Ltd	Mobile radio telephone system
JP2916185B2	1990-08-20	1999-06-28	横河電機株式会社	Wireless fee payment system
US5138650A *	1990-09-27	1992-08-11	Motorola, Inc.	Cordless telephone with internal debit and credit memory
JPH04150444A *	1990-10-11	1992-05-22	Matsushita Electric Ind Co Ltd	Terminal equipment for radio telephone system
US5353382A	1990-10-15	1994-10-04	California Institute Of Technology	Programmable synapse for neural network applications
GB2248999B	1990-10-17	1994-09-21	Racal Vodafone Ltd	Telecommunication networks
US5220593A	1990-10-24	1993-06-15	Gte Mobile Communications Service Corporation	Cellular radiotelephone credit card paystation method
US5144649A *	1990-10-24	1992-09-01	Gte Mobile Communications Service Corporation	Cellular radiotelephone credit card paystation method
US5222699A *	1990-11-05	1993-06-29	At&T Bell Laboratories	Recording and billing system
EP0490455B1	1990-12-10	1997-10-08	THOMSON multimedia	Method and apparatus for interfacing smart cards with terminals
US5221838A *	1990-12-24	1993-06-22	Motorola, Inc	Electronic wallet
SE9101105L	1991-04-12	1992-08-03	Comvik Gsm Ab	PHONE SYSTEM PROCEDURES
FI89999C *	1991-05-31	1993-12-10	Nokia Mobile Phones Ltd	Programming installation data in a mobile phone
FI89432C *	1991-06-26	1993-09-27	Nokia Mobile Phones Ltd	GENERING AV EN KLOCKFREKVENS I ETT SMART CARD GRAENSSNITT
FI96564C *	1991-07-08	1996-07-10	Nokia Mobile Phones Ltd	Private telephone number in cellular telephone system
US5659890A *	1991-07-25	1997-08-19	Casio Computer Co., Ltd.	Portable radio apparatus equipped with function to display received message information
US5850599A *	1992-09-25	1998-12-15	Ecs Enhanced Cellular Systems Manufacturing Inc.	Portable cellular telephone with credit card debit system
US5550897A *	1992-09-25	1996-08-27	Seiderman; Abe	Cellular telephone calling system using credit card validation
JPH0554205A	1991-08-21	1993-03-05	Sharp Corp	ic card system
US5933086A	1991-09-19	1999-08-03	Schlage Lock Company	Remotely-operated self-contained electronic lock security system assembly
GB2259797B	1991-09-19	1996-02-07	Kidi Technology Corp	Remotely-operated self-contained electronic lock security system assembly
US5625668A *	1991-09-27	1997-04-29	Telemac Cellular Corporation	Mobile phone with internal call accounting controls
US5294782A	1991-09-27	1994-03-15	Khyber Technologies Corporation	Integrated portable device for point of sale transactions
US5453601A *	1991-11-15	1995-09-26	Citibank, N.A.	Electronic-monetary system
US5382952A	1992-01-22	1995-01-17	Indala Corporation	Transponder for proximity identification system
FI98183C	1992-02-14	1997-04-25	Nokia Mobile Phones Ltd	Arrangement for connecting a data adapter to a GSM cellular telephone

FI1069028	1992-02-28	2001-04-30	Nokia Networks Oy	RADIOPHONE
GB2267794A	1992-04-24	1993-12-15	Alan Kilpatrick Conroy	A pre-payable mobile cellular phone
US5787174A	1992-06-17	1998-07-28	Micron Technology, Inc.	Remote identification of integrated circuit
US5754655A *	1992-05-26	1998-05-19	Hughes; Thomas S.	System for remote purchase payment and remote bill payment transactions
US5799068A *	1992-06-29	1998-08-25	Elonex I.P. Holdings Ltd.	Smart phone integration with computer systems
GB2269032B	1992-07-21	1996-03-20	Orbitel Mobile Communications	Reprogramming methods and apparatus
GB2269512B *	1992-08-03	1996-08-14	Nokia Mobile Phones Uk	Radio arrangement
FI109496B	1992-08-18	2002-08-15	Nokia Corp	Apparatus and method for providing digital infrared communication between a base unit of a radiotelephone device and another device
CA2101353A1	1992-09-04	1994-03-05	Jeffrey Charles Smolinske	System and method for transferring information between a radio transceiver and a portable memory element
US5453747A	1992-06-28	1995-09-26	Texas Instruments Deutschland Gmbh	Transponder systems for automatic identification purposes
SE470041B	1992-10-01	1993-10-25	Nordictel Ab	Digital mobile telephone system in which each subscription is assigned a subscriber number and multiple subscriber cards (SIM)
US5359182A *	1992-10-06	1994-10-25	Interdigital Technology Corporation	Wireless telephone debit card system and method
EP0669031B1 *	1992-11-11	1997-10-22	Telecom Finland Oy	Method for carrying out financial transactions by means of a mobile telephone system
US5465401A *	1992-12-15	1995-11-07	Texas Instruments Incorporated	Communication system and methods for enhanced information transfer
US5835276A *	1992-12-16	1994-08-02	Texas Instruments Incorporated	Communication system and methods for enhanced information transfer
US5351187A *	1992-12-30	1994-09-27	AVComm Incorporated	Automatic debiting parking meter system
US5864818A	1993-01-04	1999-01-26	Feldman; Ron	Automated hotel reservation processing method and system
US5506893A *	1993-02-19	1996-04-09	At&T Corp.	Telecommunication network arrangement for providing real time access to call records
DE4307122A1 *	1993-03-06	1994-09-08	Sel Alcatel Ag	Smart card
JPH06284067A	1993-03-30	1994-10-07	Toshiba Corp	Portable radio telephone set
US5604485A	1993-04-21	1997-02-18	Motorola Inc.	RF identification tag configurations and assemblies
US20010016825A1	1993-06-08	2001-08-23	Pugliese, Anthony V.	Electronic ticketing and reservation system and method
AT518388T *	1993-06-15	2011-08-15	Celltrace Llc	TELECOMMUNICATIONS SYSTEM
US5418837A	1993-07-30	1995-05-23	Ericsson-Ge Mobile Communications Inc.	Method and apparatus for upgrading cellular mobile telephones
US5574775A *	1993-08-04	1996-11-12	Lucent Technologies, Inc.	Universal wireless radiotelephone system
JPH0750890A	1993-08-05	1995-02-21	Mitsubishi Electric Corp	Speaker device
GB2282906B	1993-10-13	1996-11-06	Dataquill Ltd	Data enty systems
US5487175A *	1993-11-15	1996-01-23	Qualcomm Incorporated	Method of invoking and canceling voice or data service from a mobile unit
JPH07231367A *	1994-02-17	1995-08-29	Fujitsu Ltd	Personal communication charging service device by credit card
US5497411A *	1994-03-14	1996-03-05	Pellerin; Joseph C. E.	Telecommunications card-access system
US5724655A *	1994-04-12	1998-03-03	Motorola, Inc.	Method and apparatus for operating a communication unit consisting of multiple devices
US5488376A	1994-04-26	1996-01-30	Texas Instruments Incorporated	Transponder interface circuit
US5528222A	1994-09-09	1996-06-18	International Business Machines Corporation	Radio frequency circuit and memory in thin flexible package
DE9415302U1 *	1994-09-20	1995-01-26	Koehler Juergen	Mobile phone with reading and application unit for multifunction cards
US5608778A	1994-09-22	1997-03-04	Lucent Technologies Inc.	Cellular telephone as an authenticated transaction controller

US5604787A *	1994-10-07	1997-02-18	Motorola, Inc.	Method and apparatus for transferring information to a device in a communication system
SE515521C2	1994-10-11	2001-08-20	Combitech Traffic System Ab	Method and apparatus for radio communication between mutually moving objects
JP3571383B2	1994-10-19	2004-09-29	株式会社日立製作所	IC card, IC card read / write device and electronic wallet system
US5748737A	1994-11-14	1998-05-05	Daggar; Robert N.	Multimedia electronic wallet with generic card
US5854975A *	1994-12-23	1998-12-29	Freedom Wireless, Inc	Prepaid security cellular telecommunications system
US5577100A *	1995-01-30	1996-11-19	Telemac Cellular Corporation	Mobile phone with internal accounting
FI99071C	1995-02-15	1997-09-25	Nokia Mobile Phones Ltd	Procedure for use of applications in a mobile telephone as well as a mobile telephone
FI102018B1	1995-02-28	1998-09-30	Parkit Oy	Parking charge system, inspection device and means of identification
US5602919A *	1995-04-10	1997-02-11	Texas Instruments Incorporated	Speedup for monetary transactions using a transponder in conjunction with a smartcard
US5729697A	1995-04-24	1998-03-17	International Business Machines Corporation	Intelligent shopping cart
US5614892A	1995-04-24	1997-03-25	Pom, Inc.	Payment slot communicating apparatus for vending prices
NL1001376C2 *	1995-05-11	1996-11-12	Nederland Ptt	Method for executing an electronic payment transaction with a variable number of payment units, as well as payment means and system for applying the method.
US5805676A	1995-05-19	1998-09-08	Pcpi Phone, Inc.	Telephone/transaction entry device and system for entering transaction data into databases
US5727153A	1995-06-06	1998-03-10	Powell; Ken R.	Retail store having a system of receiving electronic coupon information from a portable card and sending the received coupon information to other portable cards
US5710886A	1995-06-16	1998-01-20	Sellectsoft, L.C.	Electric couponing method and apparatus
US5719918A *	1995-07-06	1998-02-17	Newnet, Inc.	Short message transaction handling system
KR100378112B1	1995-07-25	2003-05-23	삼성전자주식회사	Automatic locking/unlocking system using wireless communication and method for the same
US5600708A *	1995-08-04	1997-02-04	Nokia Mobile Phones Limited	Over the air locking of user identity modules for mobile telephones
US5640002A	1995-08-15	1997-06-17	Ruppert; Jonathan Paul	Portable RF ID tag and barcode reader
US5578391A	1995-09-25	1996-11-26	Motorola, Inc.	Battery pack having a disconnect switch circuit
US5848152A	1995-09-26	1998-12-08	Motorola, Inc.	Communication device having interchangeable faceplates and active keypad cover
US6094138A	1998-02-27	2000-07-25	Motorola, Inc.	Integrated circuit assembly and method of assembly
US5737710A	1995-11-07	1998-04-07	Amtech Corporation	Automated vehicle parking system for a plurality of remote parking facilities
US5692032A *	1995-11-27	1997-11-25	Nokia Mobile Phones Ltd.	Mobile terminal having one key user message acknowledgment function
US5943423A *	1995-12-15	1999-08-24	Entegrity Solutions Corporation	Smart token system for secure electronic transactions and identification
SE515611C2	1995-12-18	2001-09-10	Combitech Traffic Syst Ab	Device for data transmission by radio communication
US5809243A *	1995-12-29	1998-09-15	Lsi Logi Corporation	Personal interface system for wireless and wired communications
US6347218B1	1996-02-28	2002-02-12	Nokia Mobile Phones Limited	Electronic device with housing supplement
US5835862A *	1996-03-06	1998-11-10	Nokia Mobile Phones Ltd.	Data adapter unit for infrared communications
TW373374B	1996-04-25	1999-11-01	Daishin Frame Inc	Method and apparatus for managing subscription of commercial articles
US5911121A	1996-05-23	1999-06-08	Ericsson Inc.	Method and apparatus for automatically configuring a control program for a mobile radio communication device
US5845259A	1996-06-27	1998-12-01	Electronic Consumer Concepts, L.L.C.	Electronic coupon dispensing system
US5943624A *	1996-07-15	1999-08-24	Motorola, Inc.	Contactless smartcard for use in cellular telephone

US5819234A	1996-07-29	1998-10-06	The Chase Manhattan Bank	Toll collection system
US5991749A	1996-09-11	1999-11-23	Morrill, Jr.; Paul H.	Wireless telephony for collecting tolls, conducting financial transactions, and authorizing other activities
JP3528473B2	1996-11-07	2004-05-17	ブラザー工業株式会社	Cooling device in image forming apparatus
SE516507C2	1996-12-23	2002-01-22	Ericsson Telefon Ab L M	Rechargeable battery with built-in safety circuit for a portable electrical appliance
JP3278465B2	1996-12-27	2002-04-08	キヤノン株式会社	Sheet processing apparatus and image forming apparatus having the same
US5768370A	1997-01-08	1998-06-16	Nokia Mobile Phones, Ltd.	User changeable cosmetic phone interface
US6125281A	1997-01-31	2000-09-26	Nokia Mobile Phones Limited	Real-time SMS application messaging using an SMSC-linked server
US6091956A	1997-06-12	2000-07-18	Hollenberg; Dennis D.	Situation information system
NL1006770C2	1997-08-13	1999-02-16	Steve Hjalmar Barends	Parking payment system.
US5909176A	1997-09-23	1999-06-01	Intermec Ip Corporation	Anti-theft and identification devices for concealing in articles
US6073840A	1997-09-26	2000-06-13	Gilbarco Inc.	Fuel dispensing and retail system providing for transponder prepayment
PT990356E	1997-11-19	2002-07-31	Swisscom Mobile Ag	MOVEL APPARATUS INTELLIGENT CARD AND COMMUNICATIONS PROCESS
US6249227B1	1998-01-05	2001-06-19	Intermec Ip Corp.	RFID integrated in electronic assets
US5969691A	1998-02-10	1999-10-19	Gilbarco Inc.	Fuel dispenser transponder antenna arrangement
AUPP220998A0	1998-03-05	1998-04-02	Keycorp Limited	Mobile electronic payment terminal
US6075971A	1998-03-27	2000-06-13	Intel Corporation	Method and apparatus for providing and monitoring coupons via a network
US5949335A	1998-04-14	1999-09-07	Sensormatic Electronics Corporation	RFID tagging system for network assets
CA2264341A1 *	1998-04-14	1999-10-14	Mikohn Gaming Corporation	Pachinko stand-alone and bonusing game
US6107920A	1998-06-09	2000-08-22	Motorola, Inc.	Radio frequency identification tag having an article integrated antenna
EP1339032B1	1998-08-14	2007-10-17	3M Innovative Properties Company	Applications for radio frequency identification systems
US6100804A	1998-10-29	2000-08-08	Intecmec Ip Corp	Radio frequency identification system
AU1602500A	1998-11-02	2000-05-22	Smartdisk Corporation	Home point of sale (pos) terminal and electronic commerce method
MY119951A	1998-12-09	2005-08-30	Shell Int Research	Transponder communications system
US6577861B2	1998-12-14	2003-06-10	Fujitsu Limited	Electronic shopping system utilizing a program downloadable wireless telephone
JP2000184085A	1998-12-18	2000-06-30	Fujitsu Ltd	Portable equipment, attachment for portable terminal and system using portable equipment
KR19990024210A	1998-12-22	1999-03-25	김재한	Apparatus and method for storing and playing digital audio data in portable radiotelephones
SE516100C2	1999-05-26	2001-11-19	Henry Duhs	Arrangement with mobile communication unit and RFID circuit to provide a service
EP1208504A4	1999-07-02	2002-08-21	Zebrapass Inc	System and method for provisioning ticket purchases over global or local networks
WO2001017298A1	1999-09-02	2001-03-08	Automated Business Companies	Communication and proximity authorization systems
US6526335B1	2000-01-24	2003-02-25	G. Victor Treyz	Automobile personal computer systems
US20020095391A1	2000-06-14	2002-07-18	Garret Swart	Methods and apparatus for providing variable price structures for time-based services available through a transaction system
US6823188B1	2000-07-26	2004-11-23	International Business Machines Corporation	Automated proximity notification
US6771981B1 *	2000-08-02	2004-08-03	Nokia Mobile Phones Ltd.	Electronic device cover with embedded radio frequency (RF) transponder and methods of using same
JP4083447B2	2002-03-07	2008-04-30	トヨタ自動車株式会社	Nickel hydroxide for producing lithium nickelate, method for producing the

				same, lithium nickelate and secondary battery
SI1488075T1	2002-03-18	2006-06-30	Koninkl Philips Electronics Nv	Portable device comprising a communication station configuration and a data carrier configuration
JP4100191B2	2003-02-21	2008-06-11	松下電器産業株式会社	Electrophotographic equipment
US6915541B2	2003-03-19	2005-07-12	Faip North America, inc.	Water-operated wash brush
DE102008035889A1	2007-08-30	2009-03-19	Merck Patent Gmbh	liquid-crystal display
EP2266164B1	2008-03-04	2014-05-28	Cardiac Pacemakers, Inc	Implantable multi-length rf antenna
JP5284246B2	2009-03-03	2013-09-11	株式会社神戸製鋼所	Solid wire for welding
CN104025257B	2011-10-24	2017-09-19	株式会社尼康	Lamp optical system, exposure device and assembly manufacture method

* Cited by examiner, † Cited by third party

Cited By (531)

Publication number	Priority date	Publication date	Assignee	Title
Family To Family Citations				
FI990710C *	1995-02-15	1997-09-25	Nokia Mobile Phones Ltd	Procedure for use of applications in a mobile telephone as well as a mobile telephone
US5835061A	1995-06-06	1998-11-10	Wayport, Inc.	Method and apparatus for geographic-based communications service
US8606851B2	1995-06-06	2013-12-10	Wayport, Inc.	Method and apparatus for geographic-based communications service
IT1277879B1 *	1995-07-27	1997-11-12	Telecom Italia Mobile Spa	RADIO TERMINAL WITH ADDITIONAL CHIP CARD READER.
FI961154A *	1996-03-13	1997-09-14	Nokia Mobile Phones Ltd	Method and arrangement for restricting cell phone use
US6823317B1 *	1996-04-02	2004-11-23	Axxian Technologies Inc	Urban parking system
DE59702957D1	1996-09-13	2001-03-01	Siemens Ag	CASHLESS PAYMENT WITH A MOBILE RADIO
JPH1091866A	1996-09-18	1998-04-10	Hitachi Ltd	Electronic money transaction system
JP3660101B2 *	1996-11-14	2005-06-15	松下電器産業株式会社	Personal electronic payment system
US7054271B2 *	1996-12-06	2006-05-30	Ipco, Llc	Wireless network system and method for providing same
US8982856B2	1996-12-06	2015-03-17	Ipco, Llc	Systems and methods for facilitating wireless network communication, satellite-based wireless network systems, and aircraft-based wireless network systems, and related methods
FI104937B *	1997-01-27	2000-04-28	Sonera Oyj	A subscriber identity module, a mobile station and a method for performing a smart card operation
TW355899B *	1997-01-30	1999-04-11	Qualcomm Inc	Method and apparatus for performing financial transactions using a mobile communication unit
US6233327B1 *	1997-02-14	2001-05-15	Statsignal Systems, Inc.	Multi-function general purpose transceiver
FI109505B *	1997-03-24	2002-08-15	Fd Finanssidata Oy	Use of banking services in a digital cellular radio system
US6868364B1 *	1997-03-26	2002-03-26	Pierre H. Nel	Interactive system for and method of performing financial transactions from a user base
US6868391B1	1997-04-15	2005-03-15	Telefonaktiebolaget Lm Ericsson (Publ)	Tele/datacommunications payment method and apparatus
FI105135B *	1997-04-30	2000-06-15	Nokia Mobile Phones Ltd	A system and method for transmitting a call and a mobile station
US6167271A *	1997-05-05	2000-12-26	Northern Telecom Limited	Interface between cellular and wired networks with enhanced subscriber mobility
SE512748C2 *	1997-05-15	2000-05-08	Access Security Sweden Ab	Procedure, active card, system and use of active card to carry out an electronic transaction
US5933785A *	1997-05-20	1999-08-03	Motorola, Inc.	Telephone and method for concurrent registration of two identification numbers using multi-number sim card

DE19724901A1 *	1997-06-12	1998-12-17	Siemens Nixdorf Inf Syst	Mobile radio telephone and those with a coupled computer for Internet or network applications and method for operating such a combination of devices
DK099202ST3 *	1997-06-27	2002-10-28	Swisscom Mobile Ag	Transaction method with a portable identification element
SE512838C2 *	1997-06-30	2000-05-22	Satsafe Mls Ab	Payment operation execution system
US6157966A *	1997-06-30	2000-12-05	Schlumberger Malco, Inc.	System and method for an ISO7816 complaint smart card to become master over a terminal
FI106378	1997-07-02	2000-09-15	Sonera Oyj	A method for managing applications stored on a subscriber identity module
US7239706B1 *	1997-08-06	2007-07-03	Deutsche Telekom Ag	Transcoder for decoding encoded TV programs
CN1246941A *	1997-08-13	2000-03-08	松下电器产业株式会社	Mobile electronic commerce system
FR2767437B1 *	1997-08-14	1999-09-17	Alsthom Cge Alcatel	IMPROVED METHOD FOR LOADING A PREDETERMINED LIST OF ITEMS BY A MOBILE TERMINAL DRIVEN BY A SUBSCRIBER IDENTIFICATION MODULE, ORDER, CORRESPONDING SUBSCRIBER IDENTIFICATION MODULE AND MOBILE TERMINAL
US6914893B2	1998-06-22	2005-07-05	Statsignal Ipc, Llc	System and method for monitoring and controlling remote devices
US8410931B2	1998-06-22	2013-04-02	Sipco, Llc	Mobile inventory unit monitoring systems and methods
US6891838B1 *	1998-06-22	2005-05-10	Statsignal Ipc, Llc	System and method for monitoring and controlling residential devices
US6437692B1	1998-06-22	2002-08-20	Statsignal Systems, Inc.	System and method for monitoring and controlling remote devices
PT990356E *	1997-11-19	2002-07-31	Swisscom Mobile Ag	MOVEL APPARATUS INTELLIGENT CARD AND COMMUNICATIONS PROCESS
FR2771205B1 *	1997-11-20	2000-01-21	Gemplus Card Int	METHOD, CHIP CARD AND TERMINALS FOR PERFORMING TRANSACTIONS THROUGH A TELECOMMUNICATION NETWORK
CA2315000A1 *	1997-12-17	1999-06-24	Philippe Jacot	Method for carrying out financial transactions, system therefor and electronic purse
US6138002A *	1997-12-18	2000-10-24	Ericsson Inc.	System and method for providing services based on broadcasted system information
US6311167B1	1997-12-22	2001-10-30	Motorola, Inc.	Portable 2-way wireless financial messaging unit
US6038549A *	1997-12-22	2000-03-14	Motorola Inc	Portable 1-way wireless financial messaging unit
US6314519B1	1997-12-22	2001-11-06	Motorola, Inc.	Secure messaging system overlay for a selective call signaling system
US6041314A *	1997-12-22	2000-03-21	Davis, Walter Lee	Multiple account portable wireless financial messaging unit
KR100382181B1	1997-12-22	2003-05-09	모토로라 인코포레이티드	Single account portable wireless financial messaging unit
US6105006A *	1997-12-22	2000-08-15	Motorola Inc	Transaction authentication for 1-way wireless financial messaging units
US7167711B1	1997-12-23	2007-01-23	Openwave Systems Inc.	System and method for controlling financial transactions over a wireless network
IT1305659B1 *	1998-02-16	2001-05-15	Giorgio Liverotti	GSM MOBILE TERMINAL PERFECTED
US7162532B2	1998-02-23	2007-01-09	Koehler Steven M	System and method for listening to teams in a race event
FI980427A 1	1998-02-25	1999-08-26	Ericsson Telefon Ab L M	Procedure, arrangement and device for verification
FR2776448B1 *	1998-03-20	2000-04-28	Gemplus Card Int	TELECOMMUNICATION TERMINAL CHIP CARD READER
US20040098584A1 *	1998-03-25	2004-05-20	Sherman Edward G.	Method and system for embedded, automated, component-level control of computer systems and other complex systems
JPH11345264A *	1998-06-03	1999-12-14	Nippon Medeipakku Kk	Payment system and paying method
FR2779896B1 *	1998-06-15	2000-10-13	Sfr Sa	METHOD FOR REMOTE PAYING, BY MEANS OF A MOBILE RADIOTELEPHONE, THE ACQUISITION OF A GOOD AND / OR A SERVICE AND CORRESPONDING MOBILE RADIOTELEPHONE SYSTEM AND
FR2779895B1 *	1998-06-15	2000-08-11	Sfr Sa	METHOD AND SYSTEM FOR REMOTE PAYING USING A MOBILE RADIOTELEPHONE FOR THE ACQUISITION OF GOODS AND / OR SERVICES
FR2779850A1 *	1998-06-16	1999-12-17	Roland Moreno	METHOD AND SYSTEM FOR USING A MICROCIRCUIT CARD IN A PLURALITY OF APPLICATIONS
US6424845B1 *	1998-06-19	2002-07-23	Ncr Corporation	Portable communication device
US7650425B2	1999-03-18	2010-01-19	Sipco, Llc	System and method for controlling communication between a host computer and

				communication devices associated with remote devices in an automated monitoring system
FR2780800B1 *	1998-07-03	2000-09-08	Sagem	ELECTRONIC PAYMENT PROCESS
US6480699B1 *	1998-08-28	2002-11-12	Woodtoga Holdings Company	Stand-alone device for transmitting a wireless signal containing data from a memory or a sensor
FI981902A *	1998-09-04	2000-03-05	Sonera Oyj	Security module, security system and mobile station
AT442746T	1998-09-10	2009-09-15	Swisscom Ag	PROCEDURE FOR BUYING GOODS OR SERVICES WITH A MOBILE PHONE
EP0987660A1 *	1998-09-14	2000-03-22	Ncr International Inc.	Portable electronic apparatus
FR2785135B1 *	1998-10-22	2000-12-29	Sfr Sa	METHOD FOR LAUNCHING AN APPLICATION BY A TERMINAL, UNDER THE CONTROL OF A SUBSCRIBER IDENTIFICATION MODULE, CORRESPONDING SUBSCRIBER IDENTIFICATION MODULE AND TERMINAL
FR2785134B1 *	1998-10-22	2001-01-26	Sfr Sa	METHOD FOR ACCESSING A SERVICE SERVER FROM A MOBILE STATION, CORRESPONDING SUBSCRIBER IDENTIFICATION MODULE AND TERMINAL
AU1222499A *	1998-12-02	2000-06-19	Swisscom Ag	Method and system for charging or recharging an account with a value corresponding to a sum of money
FR2787273B1 *	1998-12-14	2001-02-16	Sagem	SECURE PAYMENT PROCESS
JP2000184085A	1998-12-18	2000-06-30	Fujitsu Ltd	Portable equipment, attachment for portable terminal and system using portable equipment
US6216015B1 *	1999-02-04	2001-04-10	Motorola, Inc.	Wireless subscriber unit and method for managing smart card data
FI107860B *	1999-02-09	2001-10-15	Sonera Smarttrust Oy	Procedure and systems for a telecommunications system and a subscriber identity module
FR2790162B1 *	1999-02-19	2001-04-13	France Telecom	TELEPAYMENT PROCEDURE AND SYSTEM FOR IMPLEMENTING THIS PROCESS
GB2347255A *	1999-02-22	2000-08-30	Ericsson Telefon Ab L M	Method of loading a cash card using a mobile phone
JP3415616B1 *	1999-02-25	2003-06-09	順子 杉中	Terminal
SE513773C2 *	1999-03-19	2000-11-06	Ericsson Telefon Ab L M	Method and system for electronic commerce
FI990695A *	1999-03-29	2000-09-30	Nokia Mobile Phones Ltd	Electronic money transfer
FR2791846B1	1999-04-01	2001-06-01	Sfr Sa	TELEPHONE TERMINAL, REMOVABLE DATA MEDIUM PROVIDED WITH MEANS FOR DELETING COMMON FEATURES AND CORRESPONDING FUNCTION MENUS MANAGEMENT METHOD
DE59906976D1 *	1999-04-07	2003-10-16	Swisscom Mobile Ag	METHOD AND SYSTEM FOR ORDERING, LOADING AND USING ACCESS TICKETS
US6542721B2 *	1999-10-11	2003-04-01	Peter V. Boesen	Cellular telephone, personal digital assistant and pager unit
US7508411B2 *	1999-10-11	2009-03-24	S.P. Technologies Llp	Personal communications device
FR2793576B1 *	1999-05-11	2001-11-16	Gemplus Card Int	RADIOTELEPHONE TERMINAL WITH A CHIP CARD WITH A BROWSER
FI114434B *	1999-05-11	2004-10-15	Nokia Corp	communication equipment
FI991105A *	1999-05-14	2000-11-15	Nokia Networks Oy	Method and digital mobile communication system
DE19925254A1 *	1999-06-01	2000-12-07	Nokia Mobile Phones Ltd	Method for operating a communication arrangement
FR2794547B1 *	1999-06-03	2001-08-24	Gemplus Card Int	PREPARATION AND EXECUTION OF A PROGRAM IN AN ADDITIONAL CHIP CARD OF A TERMINAL
EP1808831A1 *	1999-06-03	2007-07-18	Gemplus	Preparing and executing a programme in a terminal supplementary chip card
FR2794595B1 *	1999-06-03	2002-03-15	Gemplus Card Int	PRE-CHECKING A PROGRAM IN AN ADDITIONAL CHIP CARD OF A TERMINAL
US20040160917A1 *	1999-06-22	2004-08-19	Elizndi Ihab H.	Multibeam antenna for a wireless network
JP2001014277A *	1999-06-28	2001-01-19	Olympus Optical Co Ltd	Information processing system and camera system
FR2795905B1 *	1999-06-30	2001-08-24	Sagem	MOBILE PHONE WITH MULTIPLE CHIP SUPPORT ARCHITECTURE
SE517861C2 *	1999-07-15	2002-07-23	Soeren Andersson	Procedure for carrying out financial transactions and systems for carrying out the procedure
DE10035929A1 *	1999-07-22	2001-03-29	Bernd Schneider	Portable communications device comprising chip card and radio interface has transponder and antenna on chip card

US7729986B1	1999-07-30	2010-06-01	Visa International Service Association	Smart card transactions using wireless telecommunications network
US8095463B1 *	1999-08-02	2012-01-10	Openwave Systems Inc.	System and method for prepaid account replenishment
US7376583B1	1999-08-10	2008-05-20	Gofigure, L.L.C.	Device for making a transaction via a communications link
US9064281B2	2002-10-01	2015-06-23	Mastercard Mobile Transactions Solutions, Inc.	Multi-panel user interface
US7308426B1 *	1999-08-11	2007-12-11	C-Sam, Inc.	System and methods for servicing electronic transactions
US7088692B1	1999-08-18	2006-08-08	Nokia Corporation	Apparatus, and associated method, for rewarding performance of a computer game at a mobile terminal
SE515327C2	1999-08-27	2001-07-16	Ericsson Telefon Ab L M	Device for carrying out secure transactions in a communication device
WO2001016897A1 *	1999-08-27	2001-03-08	Siemens Aktiengesellschaft	Telecommunications terminal
WO2001017298A1	1999-09-02	2001-03-08	Automated Business Companies	Communication and proximity authorization systems
US7837116B2	1999-09-07	2010-11-23	American Express Travel Related Services Company, Inc	Transaction card
US7827106B2	2001-07-10	2010-11-02	American Express Travel Related Services Company, Inc.	System and method for manufacturing a punch-out RFID transaction device
WO2001018903A2 *	1999-09-08	2001-03-15	Siemens Aktiengesellschaft	Mobile radio telephone antenna comprising an integrated functional unit
US6647270B1	1999-09-10	2003-11-11	Richard B. Himmelstein	Vehicletalk
AU5759699A	1999-09-22	2001-04-24	Keiichi Nakajima	Electronic settlement system, settlement device, and terminal
DE19946537A1 *	1999-09-28	2001-04-05	Deutsche Telekom Mobil	Procedure for billing internet services via mobile radio
SE516779C2 *	1999-10-01	2002-02-26	Ericsson Telefon Ab L M	Portable communication device with a user interface and a working method for the same
SE517445C2	1999-10-01	2002-06-04	Anoto Ab	Position determination on a surface provided with a position coding pattern
WO2001026400A1 *	1999-10-01	2001-04-12	Swisscom Mobile Ag	Method for authenticating electronic certificates, issued by a certification authority in a mobile device and a corresponding identification module
US7239346B1	1999-10-18	2007-07-03	Priddy Dennis G	System and architecture that supports a multi-function semiconductor device between networks and portable wireless communications products
EP1145200B1 *	1999-10-25	2003-02-05	Swisscom Mobile AG	Method and system for transacting payments
FR2800228B1 *	1999-10-26	2002-02-08	Wavecom Sa	SYSTEM AND METHOD FOR CONTROLLING THIRD PARTY EQUIPMENT THROUGH A SIM CARD THROUGH A RADIO COMMUNICATION MODULE, CORRESPONDING RADIO COMMUNICATION MODULE AND THIRD PARTY EQUIPMENT
IL149356D0	1999-11-03	2002-11-10	Wayport Inc	Distributed network communication system which enables multiple network providers to use a common distributed network infrastructure
WO2001039464A1 *	1999-11-19	2001-05-31	Swisscom Mobile Ag	Adaptable chip card
WO2001039131A1 *	1999-11-25	2001-05-31	Fujitsu Limited	Portable terminal
ES2201808T3 *	1999-12-23	2004-03-16	Swisscom Mobile Ag	PROCEDURE AND PAYMENT TRANSACTION SYSTEM.
ES2201809T3 *	1999-12-23	2004-03-16	Swisscom Mobile Ag	PROCEDURE AND PAYMENT TRANSACTION SYSTEM.
GB2357618A *	1999-12-23	2001-06-27	Nokia Mobile Phones Ltd	Transaction system
JP3840021B2 *	1999-12-27	2006-11-01	株式会社東芝	Mobile radio terminal
JP2001186556A *	1999-12-27	2001-07-06	Toshiba Corp	Mobile wireless terminal
US6816724B1 *	1999-12-28	2004-11-09	Nokia Corporation	Apparatus, and associated method, for remotely effectuating a transaction service
EP1304007A1 *	2000-05-26	2003-04-23	Cegetel Groupe	Method for interactive exchange between a subscriber identification module co-operating with a terminal in a radiotelephone, and a local device