

[Home](#) > [Smart Card Technology](#)

Smart Card Technology

[R&D Trend](#)
[Module Technology](#)
[Product Technology](#)
[Biometrics Technology](#)
[Smart Card Technology](#)
[Security Industrial](#)

What is Smart Card

A smart card, chip card, or integrated circuit card (ICC) is any pocket-sized card with embedded integrated circuits. Smart cards are made of plastic, generally polyvinyl chloride, but sometimes polyethylene terephthalate based polyesters, acrylonitrile butadiene styrene or polycarbonate. Since April 2009, a Japanese company has manufactured reusable financial smart cards made from paper.[1]

Smart cards can provide identification, authentication, data storage and application processing.[2] Smart cards may provide strong security authentication for single sign-on (SSO) within large organizations.

What is its History &Design

Invention

In 1968 and 1969 German electrical engineers Helmut Gröttrup and Jürgen Dethloff jointly filed patents for the automated chip card (for details see page of Helmut Gröttrup). French inventor Roland Moreno[3] patented the memory card concept[4] in 1974. An important patent for smart cards with a microprocessor and memory as used today was filed by Jürgen Dethloff in 1976 and granted as USP 4105156 in 1978.[5] In 1977, Michel Ugon from Honeywell Bull invented the first microprocessor smart card. In 1978, Bull patented the SPOM (self-programmable one-chip microcomputer) that defines the necessary architecture to program the chip. Three years later, Motorola used this patent in its "CP8". At that time, Bull had 1,200 patents related to smart cards. In 2001, Bull sold its CP8 division together with its patents to Schlumberger, who subsequently combined its own internal smart card department and CP8 to create Axalto. In 2006, Axalto and Gemplus, at the time the world's top two smart card manufacturers, merged and became Gemalto. In 2008 Dexa Systems spun off from Schlumberger and acquired Enterprise Security Services business, which included the smart card solutions division responsible for deploying the first large scale public key infrastructure (PKI) based smart card management systems.

The first mass use of the cards was as a telephone card for payment in French pay phones, starting in 1983.[citation needed]

Carte Bleue

After the Télécarte, microchips were integrated into all French Carte Bleue debit cards in 1992. Customers inserted the card into the merchant's POS terminal, then typed the PIN, before the transaction was accepted. Only very limited transactions (such as paying small highway tolls) are processed without a PIN.

Smart-card-based "electronic purse" systems store funds on the card so that readers do not need network connectivity. They entered European service in the mid-1990s. They have been common in Germany (Geldkarte),

Smart Card Technology



- [Biometrics Technology](#)
- [Smart Card Technology](#)
- [Security Industrial](#)

[More >>](#)

Products



- [GPS310F Guard Patrol with GPRS](#)
- [GPS310 Guard Patrol with GPRS W](#)
- [GPS800 Guard Patrol with TFT sc](#)
- [GPS320 Guard Patrol/Tour Stick](#)
- [GPS500 Guard Patrol Stick with](#)
- [GPS500 Guard Patrol Stick with](#)

[More >>](#)

Contact Us



- Service: 0755-83418779
- Email: support@epordo.com

[Find out more >>](#)

Austria (Quick Wertkarte), Belgium (Proton), France (Moneo[6]), the Netherlands (Chipknip Chipper (decommissioned in 2001)), Switzerland ("Cash"), Norway ("Mondex"), Sweden ("Cash", decommissioned in 2004), Finland ("Avant"), UK ("Mondex"), Denmark ("Danmønt") and Portugal ("Porta-moedas Multibanco").

Since the 1990s, smart-cards have been the SIMs used in European GSM mobile phone equipment. Mobile phones are widely used in Europe, so smart cards have become very common.

EMV

For more details on this topic, see EMV.

EMV-compliant cards and equipment are widespread except in a few countries such as the United States. Typically, a country's national payment association, in coordination with MasterCard International, Visa International, American Express and JCB, jointly plan and implement EMV systems.

Historically, in 1993 several international payment companies agreed to develop smart-card specifications for debit and credit cards. The original brands were MasterCard, Visa, and Europay. The first version of the EMV system was released in 1994. In 1998 the specifications became stable.

EMVCo maintains these specifications. EMVCo's purpose is to assure the various financial institutions and retailers that the specifications retain backward compatibility with the 1998 version. EMVCo upgraded the specifications in 2000 and 2004.[7]

Development of contactless systems[edit]

Contactless smart cards do not require physical contact between a card and reader. They are becoming more popular for payment and ticketing. Typical uses include mass transit and motorway tolls. Visa and MasterCard implemented a version deployed in 2004–2006 in the U.S. Most contactless fare collection systems are incompatible, though the MIFARE Standard card from NXP Semiconductors has a considerable market share in the US and Europe.

Smart cards are also being introduced for identification and entitlement by regional, national, and international organizations. These uses include citizen cards, drivers' licenses, and patient cards. In Malaysia, the compulsory national ID MyKad enables eight applications and has 18 million users. Contactless smart cards are part of ICAO biometric passports to enhance security for international travel.

Design

A smart card may have the following generic characteristics:

Dimensions similar to those of a credit card. ID-1 of the ISO/IEC 7810 standard defines cards as nominally 85.60 by 53.98 millimetres (3.370 in × 2.125 in). Another popular size is ID-000 which is nominally 25 by 15 millimetres (0.984 in × 0.591 in) (commonly used in SIM cards). Both are 0.76 millimetres (0.030 in) thick.

Contains a tamper-resistant security system (for example a secure cryptoprocessor and a secure file system) and provides security services (e.g., protects in-memory information).

Managed by an administration system which securely interchanges information and configuration settings with the card, controlling card blacklisting and application-data updates.

Communicates with external services via card-reading devices, such as ticket readers, ATMs, DIP reader, etc.

Contact smart cards

Illustration of smart card structure and packaging

Smart card reader on a laptop

A smart card pinout. VCC: Power supply. RST: Reset signal, used to reset the card's communications. CLK: Provides the card with a clock signal, from which data communications timing is derived. GND: Ground (reference voltage).

VPP: ISO/IEC 7816-3:1997 designated this as a programming voltage: an input for a higher voltage to program persistent memory (e.g., EEPROM). ISO/IEC 7816-3:2006 designates it SPU, for either standard or proprietary use, as input and/or output. I/O: Serial input and output (half-duplex). C4, C8: The two remaining contacts are AUX1 and AUX2 respectively, and used for USB interfaces and other uses.[8] However, the usage defined in ISO/IEC 7816-2:1999/Amd 1:2004 may have been superseded by ISO/IEC 7816-2:2007.[citation needed]

Contact smart cards have a contact area of approximately 1 square centimetre (0.16 sq in), comprising several gold-plated contact pads. These pads provide electrical connectivity when inserted into a reader,[9] which is used as a communications medium between the smart card and a host (e.g., a computer, a point of sale terminal) or a mobile telephone. Cards do not contain batteries; power is supplied by the card reader.

The ISO/IEC 7810 and ISO/IEC 7816 series of standards define:

physical shape and characteristics

electrical connector positions and shapes

electrical characteristics

communications protocols, including commands sent to and responses from the card

basic functionality

Because the chips in financial cards are the same as those used in subscriber identity modules (SIMs) in mobile phones, programmed differently and embedded in a different piece of PVC, chip manufacturers are building to the more demanding GSM/3G standards. So, for example, although the EMV standard allows a chip card to draw 50 mA from its terminal, cards are normally well below the telephone industry's 6 mA limit. This allows smaller and cheaper financial card terminals.

Communication protocols for contact smart cards include T=0 (character-level transmission protocol, defined in ISO/IEC 7816-3) and T=1 (block-level transmission protocol, defined in ISO/IEC 7816-3).

Contactless smart cards

Main article: Contactless smart card

A second card type is the contactless smart card, in which the card communicates with and is powered by the reader through RF induction technology (at data rates of 106–848 kbit/s). These cards require only proximity to an antenna to communicate. Like smart cards with contacts, contactless cards do not have an internal power source. Instead, they use an inductor to capture some of the incident radio-frequency interrogation signal, rectify it, and use it to power the card's electronics.

APDU transmission via a contactless interface is defined in ISO/IEC 14443-4.

Hybrids

A hybrid smart card which clearly shows the antenna connected to the main chip

Dual-interface cards implement contactless and contact interfaces on a single card with some shared storage and processing. An example is Porto's multi-application transport card, called Andante, which uses a chip with both contact and contactless (ISO/IEC 14443 Type B) interfaces.

Applications

Financial

Smart cards serve as credit or ATM cards, fuel cards, mobile phone SIMs, authorization cards for pay television, household utility pre-payment cards, high-security identification and access-control cards, and public transport and public phone payment cards.

Smart cards may also be used as electronic wallets. The smart card chip can be "loaded" with funds to pay parking meters, vending machines or merchants. Cryptographic protocols protect the exchange of money between the smart card and the machine. No connection to a bank is needed. The holder of the card may use it even if not the owner. Examples are Proton, Geldkarte, Chipknip and Moneo. The German Geldkarte is also used to validate customer age at vending machines for cigarettes.

Main articles: Contactless smart card and Credit card

These are the best known payment cards (classic plastic card):

Visa: Visa Contactless, Quick VSDC, "qVSDC", Visa Wave, MSD, payWave

MasterCard: PayPass Magstripe, PayPass MChip

American Express: ExpressPay

Discover: Zip

Roll-outs started in 2005 in the U.S. Asia and Europe followed in 2006. Contactless (non-PIN) transactions cover a payment range of ~\$5–50. There is an ISO/IEC 14443 PayPass implementation. Some, but not all PayPass implementations conform to EMV.

Non-EMV cards work like magnetic stripe cards. This is common in the U.S. (PayPass Magstripe and VISA MSD). The cards do not hold or maintain the account balance. All payment passes without a PIN, usually in off-line mode. The security of such a transaction is no greater than with a magnetic stripe card transaction.

EMV cards can have either contact or contactless interfaces. They work as if they were a normal EMV card with a contact interface. Via the contactless interface they work somewhat differently, in that the card commands enabled improved features such as lower power and shorter transaction times.

SIM

The subscriber identity modules used in mobile-phone systems are reduced-size smart cards, using otherwise identical technologies.

Identification

Smart-cards can authenticate identity. Usually, they employ a public key infrastructure (PKI). The card stores an encrypted digital certificate issued from the PKI provider along with other relevant information. Examples include the U.S. Department of Defense (DoD) Common Access Card (CAC), and other cards used by other governments for their citizens. If they include biometric identification data, cards can provide superior two- or three-factor authentication.

Smart cards are not always privacy-enhancing, because the subject may carry incriminating information on the card. Contactless smart cards that can be read from within a wallet or even a garment simplify authentication; however, criminals may access data from these cards.

Cryptographic smart cards are often used for single sign-on. Most advanced smart cards include specialized cryptographic hardware that uses algorithms such as RSA and DSA. Today's cryptographic smart cards generate key pairs on board, to avoid the risk from having more than one copy of the key (since by design there usually isn't a way to extract private keys from a smart card). Such smart cards are mainly used for digital signatures and secure identification.

The most common way to access cryptographic smart card functions on a computer is to use a vendor-provided PKCS#11 library.[citation needed] On Microsoft Windows the CSP API is also supported.

The most widely used cryptographic algorithms in smart cards (excluding the GSM so-called "crypto algorithm") are Triple DES and RSA. The key set is usually loaded (DES) or generated (RSA) on the card at the personalization stage.

Some of these smart cards are also made to support the NIST standard for Personal Identity Verification, FIPS 201.

Turkey implemented the first smart card driver's license system in 1987. Turkey had a high level of road accidents and decided to develop and use digital tachograph devices on heavy vehicles, instead of the existing mechanical ones, to reduce speed violations. Since 1987, the professional driver's licenses in Turkey have been issued as smart cards. A professional driver is required to insert his driver's license into a digital tachograph before starting to drive. The tachograph unit records speed violations for each driver and gives a printed report. The driving hours for each driver are also being monitored and reported. In 1990 the European Union conducted a feasibility study through BEVAC Consulting Engineers, titled "Feasibility study with respect to a European electronic drivers license (based on a smart-card) on behalf of Directorate General VII". In this study, chapter seven describes Turkey's experience.

Argentina's Mendoza province began using smart card driver's licenses in 1995. Mendoza also had a high level of road accidents, driving offenses, and a poor record of recovering fines.[citation needed] Smart licenses hold up-to-date records of driving offenses and unpaid fines. They also store personal information, license type and number, and a photograph. Emergency medical information such as blood type, allergies, and biometrics (fingerprints) can be stored on the chip if the card holder wishes. The Argentina government anticipates that this system will help to collect more than \$10 million per year in fines.

In 1999 Gujarat was the first Indian state to introduce a smart card license system.[10] As of 2005, it has issued 5 million smart card driving licenses to its people.[11]

In 2002, the Estonian government started to issue smart cards named ID Kaart as primary identification for citizens to replace the usual passport in domestic and EU use. As of 2010 about 1 million smart cards have been issued (total population is about 1.3 million) and they are widely used in internet banking, buying public transport tickets, authorization on various websites etc.

By the start of 2009 the entire population of Spain and Belgium will have an eID card that is used for identification. These cards contain two certificates: one for authentication and one for signature. This signature is legally enforceable. More and more services in these countries use eID for authorization.[12][13]

After August 14, 2012, the ID card of Pakistan will be replaced. The Smart Card is a third generation chip-based identity document that is produced according to international standards and requirements. The card has over 36 physical security features and has the latest encryption codes. This smart card will also replace the NICOP (the ID card for overseas Pakistani).

Smart cards may identify emergency responders and their skills. Cards like these allow first responders to bypass organizational paperwork and focus more time on the emergency resolution. In 2004, The Smart Card Alliance expressed the needs: "to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification".[14] emergency response personnel can carry these cards to be positively identified in emergency situations. WidePoint Corporation, a smart card provider to FEMA, produces cards that contain additional personal information, such as medical records and skill sets.

In 2007, the Open Mobile Alliance (OMA) proposed a new standard defining V1.0 of the Smart Card Web Server (SCWS), an HTTP server embedded in a SIM card intended for a smartphone user.[15] The non-profit trade association SIMalliance has been promoting the development and adoption of SCWS. SIMalliance states that SCWS offers end-users a familiar, OS-independent, browser-based interface to secure, personal SIM data. As of mid-2010,

SIMalliance had not reported widespread industry acceptance of SCWS.[16] The OMA has been maintaining the standard, approving V1.1 of the standard in May 2009, and V1.2 is expected to be approved in October 2012.[17]

Public transit

Main article: List of smart cards

Smart cards and integrated ticketing are used by many public transit operators. Card users may also make small purchases using the cards. Some operators offer points for usage, exchanged at retailers or for other benefits.[18] Examples include Singapore's CEPAS, Hong Kong's Octopus Card, London's Oyster Card, Dublin's Leap card, Brussels' MoBIB, Québec's OPUS card, San Francisco's Clipper card and Sydney's Opal card. However, these present a privacy risk because they allow the mass transit operator (and the government) to track an individual's movement. In Finland, for example, the Data Protection Ombudsman prohibited the transport operator Helsinki Metropolitan Area Council (YTV) from collecting such information, despite YTV's argument that the card owner has the right to a list of trips paid with the card. Earlier, such information was used in the investigation of the Myyrmanni bombing.[citation needed]

The UK's Department for Transport mandated smart cards to administer travel entitlements for elderly and disabled residents. These schemes let residents use the cards for more than just bus passes. They can also be used for taxi and other concessionary transport. One example is the "Smartcare go" scheme provided by Ecebs.[19] The UK systems use the ITSO_Ltd specification.

Computer security

Smart cards can be used as a security token.

The Mozilla Firefox web browser can use smart cards to store certificates for use in secure web browsing.[20]

Some disk encryption systems, such as FreeOTFE, TrueCrypt and Microsoft Windows 7 BitLocker, can use smart cards to securely hold encryption keys, and also to add another layer of encryption to critical parts of the secured disk.
[21]

GnuPG, the well known encryption suite, also supports storing keys in a smartcard.[22]

Smart cards are also used for single sign-on to log on to computers.

Schools

Smart cards are being provided to students at schools and colleges.[23][24][25] Uses include:

Tracking student attendance

As an electronic purse, to pay for items at canteens, vending machines, laundry facilities, etc...

Tracking and monitoring food choices at the canteen, to help the student maintain a healthy diet

Tracking loans from the school library

Access control for admittance to restricted buildings, dormitories, and other facilities. This requirement may be enforced at all times (such as for a laboratory containing valuable equipment), or just during after-hours periods (such as for an academic building that is open during class times, but restricted to authorized personnel at night), depending on security needs.

Access to transportation services

Healthcare

Smart health cards can improve the security and privacy of patient information, provide a secure carrier for portable medical records, reduce health care fraud, support new processes for portable medical records, provide secure access to emergency medical information, enable compliance with government initiatives (e.g., organ donation) and mandates, and provide the platform to implement other applications as needed by the health care organization.[26]

Other uses

Smart cards are widely used to protect digital television streams. VideoGuard is a specific example of how smart card security worked.

Multiple-use systems

The Malaysian government promotes MyKad as a single system for all smart-card applications. MyKad started as identity cards carried by all citizens and resident non-citizens. Available applications now include identity, travel documents, drivers license, health information, an electronic wallet, ATM bank-card, public toll-road and transit payments, and public key encryption infrastructure. The personal information inside the MYKAD card can be read using special APDU commands.[27]

Security

It has been suggested that Smart_card_security be merged into this article. (Discuss) Proposed since January 2014.

Main article: Smart card security

Smart cards have been advertised as suitable for personal identification tasks, because they are engineered to be tamper resistant. The chip usually implements some cryptographic algorithm. There are, however, several methods for recovering some of the algorithm's internal state.

Differential power analysis involves measuring the precise time and electrical current required for certain encryption or decryption operations. This can deduce the on-chip private key used by public key algorithms such as RSA. Some implementations of symmetric ciphers can be vulnerable to timing or power attacks as well.

Smart cards can be physically disassembled by using acid, abrasives, or some other technique to obtain unrestricted access to the on-board microprocessor. Although such techniques obviously involve a fairly high risk of permanent damage to the chip, they permit much more detailed information (e.g. photomicrographs of encryption hardware) to be extracted

Benefits

The benefits of smart cards are directly related to the volume of information and applications that are programmed for use on a card. A single contact/contactless smart card can be programmed with multiple banking credentials, medical entitlement, driver's license/public transport entitlement, loyalty programs and club memberships to name just a few. Multi-factor and proximity authentication can and has been embedded into smart cards to increase the security of all services on the card. For example, a smart card can be programmed to only allow a contactless transaction if it is also within range of another device like a uniquely paired mobile phone. This can significantly increase the security of the smart card.

Governments and regional authorities save money because of improved security, better data and reduced processing costs. These savings help reduce public budgets or enhance public services. There are many examples in the UK, many using a common open LASSeO specification.[28]

Individuals have better security and more convenience with using smart cards that perform multiple services. For example, they only need to replace one card if their wallet is lost or stolen. The data storage on a card can reduce duplication, and even provide emergency medical information.

Problems

The plastic card in which the chip is embedded is fairly flexible. The larger the chip, the higher the probability that normal use could damage it. Cards are often carried in wallets or pockets, a harsh environment for a chip. However, for large banking systems, failure-management costs can be more than offset by fraud reduction.[citation needed]

If the account holder's computer hosts malware, the smart card security model may be broken. Malware can override the communication (both input via keyboard and output via application screen) between the user and the application. Man-in-the-browser malware (e.g. the trojan Silentbanker) could modify a transaction, unnoticed by the user. Banks like Fortis and Belfius in Belgium and Rabobank ("random reader") in the Netherlands combine a smart card with an unconnected card reader to avoid this problem. The customer enters a challenge received from the bank's website, a PIN and the transaction amount into the reader, The reader returns an 8-digit signature. This signature is manually entered into the personal computer and verified by the bank, preventing malware from changing the transaction amount.

Smart cards have also been the targets of security attacks. These attacks range from physical invasion of the card's electronics, to non-invasive attacks that exploit weaknesses in the card's software or hardware. The usual goal is to expose private encryption keys and then read and manipulate secure data such as funds. Once an attacker develops a non-invasive attack for a particular smart card model, he is typically able to perform the attack on other cards of that model in seconds, often using equipment that can be disguised as a normal smart card reader.[29] While manufacturers may develop new card models with additional security, it may be costly or inconvenient for users to upgrade vulnerable systems. Tamper-evident and audit features in a smart card system help manage the risks of compromised cards.

Another problem is the lack of standards for functionality and security. To address this problem, The Berlin Group launched the ERIDANE Project to propose "a new functional and security framework for smart-card based Point of Interaction (POI) equipment".[30]..



