receiving from the authorizing server an authorization message authorizing the cash payment;

in response to receiving the authorization message, receiving a user selection of a payment accepting machine distinct from the mobile device;

transmitting from the mobile device to the payment accepting machine an electronic command including one or more time-dependent and payment accepting machine- dependent conditions, wherein a first of the one or more time-dependent and payment accepting machine-dependent conditions comprises a predefined time or time period by which a button or control at the payment accepting machine must be engaged;

displaying the one or more time-dependent and payment accepting machine- dependent conditions on a display of the mobile device;

at the payment accepting machine: receiving the electronic command and the one or more time-dependent and payment accepting machine-dependent conditions from the mobile device;

determining that the one or more time-dependent and payment accepting machine-dependent conditions are met, including determining that the button or control at the payment accepting machine has been engaged within the predefined time or time period; and

in response to the determination that the one or more time-dependent and payment accepting machine-dependent conditions are met, issuing the cash payment.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to EL MEHDI OUSSIR whose telephone number is (571)270-0191. The examiner can normally be reached on M-F 9AM - 5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Neha W. Patel can be reached on 571-270-1492. The fax phone number for the organization where this application or proceeding is assigned is 571-270-1191.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Sincerely,

/EL MEHDI OUSSIR/
Primary Examiner, Art Unit 3685
04/03/2023

Notice of References Cited	Application/Control No. 15/893,514	Applicant(s)/Patent Under Reexamination Patel et al.	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20140012414-A1	01-2014	Perez; Ivaro Osnaya	G07F9/001	700/241
*	B	US-11042852-B1	06-2021	Wadhwa; Gaurav	G06Q20/40145	1/1
*	C	US-20160350744-A1	12-2016	Tang; Tai Kwan Jimmy	G06Q20/326	1/1
*	D	US-20170193479-A1	07-2017	Kamat; Shreyas	G06Q20/3276	1/1
*	E	US-20150154579-A1	06-2015	Teicher; Mordechai	G06Q20/40145	705/21
*	F	US-20150235202-A1	08-2015	Zabala; Jose Rafael	G06Q20/326	700/232
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N	JP-H1125320-A	07-1997	JP	SHIODA TAKUJI et al.	
	O	JP-2004310740-A	11-2004	JP	TSUJI N	
	P	JP-4586607-B2	11-2010	JP	KIHARA H	
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Heimerl et al. Communitysourcing: Engaging local crowds to perform expert work via physical kiosks, https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=253ca0e33ed5fbd6e77bbcd3a5ec430b2d67e0a4 (Year: 2012)
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Petitioner Exhibit 1002-2696

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

24341 7590 06/28/2023
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER
HOLLY, JOHN H

ART UNIT	PAPER NUMBER
3696	

DATE MAILED: 06/28/2023

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/983,311	11/08/2022	PARESH K. PATEL	104402-5058-US	1703

TITLE OF INVENTION: SYSTEMS AND METHODS FOR DETERMINING ELECTRIC PULSES TO PROVIDE TO AN UNATTENDED MACHINE BASED ON REMOTELY-CONFIGURED OPTIONS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	09/28/2023

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 40% the amount of undiscounted fees, and micro entity fees are 20% the amount of undiscounted fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

Petitioner Exhibit 1002-2697

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

24341 7590 06/28/2023
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/983,311	11/08/2022	PARESH K. PATEL	104402-5058-US	1703

TITLE OF INVENTION: SYSTEMS AND METHODS FOR DETERMINING ELECTRIC PULSES TO PROVIDE TO AN UNATTENDED MACHINE BASED ON REMOTELY-CONFIGURED OPTIONS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	09/28/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS
HOLLY, JOHN H	3696	705-020000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑ Issue Fee ❑ Publication Fee (if required)

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via Patent Center or EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

❑ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

❑ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

Petitioner Exhibit 1002-2698

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/983,311	11/08/2022	PARESH K. PATEL	104402-5058-US	1703

24341 7590 06/28/2023

Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER	
HOLLY, JOHN H	

ART UNIT	PAPER NUMBER
3696	

DATE MAILED: 06/28/2023

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Petitioner Exhibit 1002-2699

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Petitioner Exhibit 1002-2700

Notice of Allowability	Application No. 17/983,311	Applicant(s) PATEL, PARESH K.	
	Examiner JOHN H HOLLY	Art Unit 3696	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to Communication filed May 15, 2023.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are 2-31 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some* c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☑ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☐ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/John H. Holly/
Primary Examiner, Art Unit 3696

Petitioner Exhibit 1002-2701

Notice of Pre-AIA or AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

DETAILED ACTION

This communication is in response to a Communications filed May 15, 2023.

Allowable Subject Matter

Claims 2 – 31 are allowed over prior art of record.

Reasons for Allowance

The following is an examiner's statement of reasons for allowance:
The prior art of record neither anticipates nor renders obvious the claimed subject matter of the instant application as a whole either taken alone or in combination, in particular, prior art of record does not teach “in response to receiving the first set of remotely-configured options, displaying, in the application, user interface objects that allow for selection of respective options in the first set of remotely-configured options; detecting a selection of a first user interface object that corresponds to a first option in the first set of remotely-configured options; after detecting the selection of the first user interface object, receiving, from the server, pulse information specifying a count, amplitude, shape, or interval of electric pulses to be provided to the control unit of the unattended machine by the pulse-providing device in accordance with the first option; and sending the pulse information to the pulse-providing device; and at the pulse-providing device: receiving the pulse information; determining based on the received pulse information a signal sequence of electrical pulses to output to the control unit of

the unattended machine in order to initiate a cashless operation of the unattended machine, wherein the signal sequence of electrical pulses emulates an analog signal generated by a coin receiving switch of the unattended machine, and wherein the signal sequence is characterized by the count, amplitude, shape, or interval of electric pulses specified by the pulse information; and causing the unattended machine to initiate the cashless operation by issuing the signal sequence of electrical pulses to the control unit.".

The following prior art references have been deemed most relevant to the allowed claim(s):

The closest prior art Mordechai Teicher (Pub. # US 2010/0312692 A1) teaches a compact payment terminal for operating upon a purchase made by a customer at a retail device is provided. The customer carries a mobile communication device that includes a payment module and a communication module. The compact payment terminal includes a first interface for interfacing with the retail device, a second interface for interfacing with the mobile communication device of the customer and a processing unit connected to the first and second interface. The compact payment terminal is configured to receive, via the first interface, a payment request from the retail device, cooperate, via the second interface, with the payment module of the mobile communication device for initiating a payment transaction respective to the payment request, and selectably conduct, via the second interface and the communication module of the mobile communication device, a communication session between the processing unit and at least one server.

The closest prior art Jonathan L. Lei et al. (Pub. # US 2003/0158891 A1) teaches a wireless network system includes a server system connected to a network. An electronic device is provided having a wireless transceiver adapted to communicate via at least one of light transmission and radio frequency (RF) transmission. A portable wireless device is provided having a wireless connection to the network. The portable wireless device is adapted to communicate wirelessly with the electronic device. The

electronic device communicates with the server system over the network through the portable wireless device. The electronic device may conduct real-time and/or non-real-time transactions with the server system by utilizing the portable wireless device as a communication proxy.

The claims allow an unattended machine, which is not connected to any network, to accept remotely- configured options (e.g., multi-credit pricing options) that are configured at a server and sent to a pulse-providing device that is coupled with the unattended machine via an exchange of data. For unattended machines that rely on legacy communication protocols, the exchange of data includes instructions that allow a pulse-providing device of the unattended machine to provide electric pulses that are determined in accordance with remotely-configured options that are selected by a user of a mobile device. By providing these electric pulses, the pulse-providing device causes the unattended machine to operate as if it had been paid with coins, even if no coins were physically inserted. The claims recites features of the .mobile device, which, in addition to acting as the communication bridge, also facilitates user selection of a product or service offered by the attended machine, allowing the server to determine how many electric pulses the machine must be provided in accordance with the user's selections. The claimed solution is necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks and recite significantly more than an abstract idea.

Conclusion

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John H. Holly whose telephone number is 571.270.3461. The examiner can normally be reached on MON. - FRI 10 AM - 8 PM p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Namrata Boveja can be reached on (571)-272-8105. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

/John H. Holly/
Primary Examiner, Art Unit 3696

Notice of References Cited	Application/Control No. 17/983,311	Applicant(s)/Patent Under Reexamination PATEL, PARESH K.	
	Examiner JOHN H HOLLY	Art Unit 3696	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20100312692-A1	12-2010	TEICHER; MORDECHAI	G06Q20/3278	455/414.1
*	B	US-20030158891-A1	08-2003	Lei, Jonathan L.	G06Q20/327	709/203
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
*	U	ProQuestDialogNPL STIC Search History
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Petitioner Exhibit 1002-2706

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/893,514	02/09/2018	Paresh K. Patel	104402-5026-US	4668

24341 7590 09/30/2022

Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
09/30/2022	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

padocketingdepartment@morganlewis.com
vskliba@morganlewis.com

Petitioner Exhibit 1002-2707

Office Action Summary	Application No. 15/893,514	Applicant(s) Patel et al.	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 05/23/2022.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 11,16,18-19 and 21-28 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 24 and 28 is/are rejected.

8) ☑ Claim(s) 11,16,18-19,21-23 and 25-27 is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☑ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 05/23/2022 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

Petitioner Exhibit 1002-2708

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

2. This communication is a Non-Final Action in response to Applicant's request for continued examination filed on 05/23/2022.

3. Claims 11, 16, 18-19, and 21-28 have been examined in this application. All other claims have been cancelled. Claims 26-28 are newly presented.

4. The information disclosure statements (IDS) submitted on July, 20, 2021 and August 15, 2022 have been considered.

Response to Arguments

5. Applicant's arguments, filed May 23, 2022, page 8, regarding drawings objections have been considered and are persuasive. The objection is withdrawn.

6. Applicant's arguments, page 9, regarding claim rejections under 35 U.S.C. 112(b) have been fully considered and are persuasive; the rejections are withdrawn.

Specification

7. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Claim 18 recites "wherein the mobile device is a dedicated electronic device distinct from the payment accepting machine." The Specification recites "dedicated

refund center devices" in Paragraph 0090. The Specification can be amended to capture the proper antecedent basis for the "dedicated electronic device" as claimed in claim 18.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112(a):

> (a) IN GENERAL.—The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

The following is a quotation of the first paragraph of pre-AIA 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

8. Per claim 24, the claim recites "wherein the cash payment is a withdrawal from a user account that is linked with the authorizing server."

Because the cash payment is defined as a payment resulting from a refund request, it is not known how a refund can be provided to the user if "the cash payment is a withdrawal from a user account…" Such a withdrawal would constitute a charge not a refund for the user. Furthermore, no support was found in the Specification detailing how the refund is issued by initiating a withdrawal from the user's account.

As a result, the claim is rejected.

9. Claim 28 is rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one

skilled in the relevant art that the inventor or a joint inventor, or for applications subject to pre-AIA 35 U.S.C. 112, the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim 28 recites "wherein determining that the button or control at the payment accepting machine has been engaged within the predefined time or time period includes determining that a valid code has been entered at the payment accepting machine within the predefined time or time period." Emphasis added.

The Specification, see Paragraphs 0275-0277, clearly recite that both a code and a phone number must be entered in order to redeem that code prior to the user proceeding with the refund request.

Second, the condition associated with the user pressing the button/controller is not recited as being linked to the entering of the code and phone number. The Specification was reviewed and no recitation of the user entering the code without the phone number was found. Also, no support was found linking the entering of the code and the phone number with the time condition required to receive the refund.

As a result, the claim is rejected.

Prior Art

U.S. Patent 9,547,859 to Patel el al. is directed to a device with one or more processors, memory, and two or more communication capabilities obtains, from a payment module, an authorization request via a first communication capability (e.g., Bluetooth). The device sends, to a server, the authorization request via a second communication capability distinct from the first communication capability (e.g., cellular or WiFi technology). In response to sending the

authorization request, the device obtains, from the server, authorization information via the second communication capability. After obtaining the authorization information, the device detects a trigger condition to perform a transaction with a payment accepting unit associated with the payment module. In response to detecting the trigger condition, the device sends, to the payment module, at least a portion of the authorization information via the first communication capability.

U.S. Patent Application Publication 2016/0086145 to Tsutsui teaches a voucher ticket system and method of use employing a bill validator installed into any suitable automated machine, including an Automated Teller Machine (ATM), a gaming machine, etc. The bill validator is integrated with a bill reader, a voucher ticket reader, a reader for acquisition of electronic voucher ticket information from a portable computing device, a printer, and other supporting peripheral devices. The voucher ticket system includes a secured communication link with a host account manager serving a plurality of electronic money accounts. The method includes steps of receiving a value of electronic money or identification information associated with the electronic voucher ticket with account information associated with the electronic money account and sending the received value of the electronic money or the identification information of the voucher ticket to an upper control section of the one of the gaming machine and the ATM for completion of a financial transaction.

Further searches including non-patent literature and foreign references have been carried out. However, the references found and those cited fail to disclose the claim limitations of claim 11 as a whole. The combination of references to teach the claimed limitations would not have been obvious to one of ordinary skill in the art before the effective filing date of the Application.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure is listed on for PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to EL MEHDI OUSSIR whose telephone number is (571)270-0191. The examiner can normally be reached on M-F 9AM - 5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Neha W. Patel can be reached on 571-270-1492. The fax phone number for the organization where this application or proceeding is assigned is 571-270-1191.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Sincerely,

/EL MEHDI OUSSIR/
Primary Examiner, Art Unit 3685

Notice of References Cited	Application/Control No. 15/893,514	Applicant(s)/Patent Under Reexamination Patel et al.	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20030009385-A1	01-2003	Tucciarone, Joel D.	H04L9/40	705/26.1
*	B	US-20160012465-A1	01-2016	Sharp; Jeffrey A.	G06Q20/321	705/14.17
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N	WO-2006020692-A2	02-2006	WO	ALDERUCCI D P	G06Q30/06
	O	JP-2010528716-A	05-2008	JP	No matching document found	
	P	KR-20130138637-A	09-2012	KR	No matching document found	
	Q	WO-2016158748-A1	10-2016	WO	MATSUI T	G06K9/00228
	R	CN-106803175-A	06-2017	CN	CARLSON M	G06F8/65
	S	CN-108352094-A	07-2018	CN	PISHCHIK K E	G06Q10/0836
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	When the Future Feels Worse Than the Past: A Temporal Inconsistency in Moral Judgment. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.675.3584&rep=rep1&type=pdf (Year: 2010)
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Petitioner Exhibit 1002-2714

Communitysourcing: Engaging Local Crowds to Perform Expert Work Via Physical Kiosks

Kurtis Heimerl[1], Brian Gawalt[1], Kuang Chen[1], Tapan S. Parikh[2], Björn Hartmann[1]
University of California, Berkeley – Computer Science Division[1], School of Information[2]
{kheimerl,gawalt,kuangc,bjoern}@cs.berkeley.edu, parikh@ischool.berkeley.edu

ABSTRACT
Online labor markets, such as Amazon's Mechanical Turk, have been used to crowdsource simple, short tasks like image labeling and transcription. However, expert knowledge is often lacking in such markets, making it impossible to complete certain classes of tasks. In this work we introduce an alternative mechanism for crowdsourcing tasks that require specialized knowledge or skill: *communitysourcing* — the use of physical kiosks to elicit work from specific populations. We investigate the potential of communitysourcing by designing, implementing and evaluating *Umati: the communitysourcing vending machine*. Umati allows users to earn credits by performing tasks using a touchscreen attached to the machine. Physical rewards (in this case, snacks) are dispensed through traditional vending mechanics. We evaluated whether communitysourcing can accomplish expert work by using Umati to grade Computer Science exams. We placed Umati in a university Computer Science building, targeting students with grading tasks for snacks. Over one week, 328 unique users (302 of whom were students) completed 7771 tasks (7240 by students). 80% of users had never participated in a crowdsourcing market before. We found that Umati was able to grade exams with 2% higher accuracy (at the same price) or at 33% lower cost (at equivalent accuracy) than traditional single-expert grading. Mechanical Turk workers had no success grading the same exams. These results indicate that communitysourcing can successfully elicit high-quality expert work from specific communities.

Author Keywords
Crowdsourcing, Kiosks, Ubiquitous Computing, CSCW

ACM Classification Keywords
H.5.2 Information Interfaces and Presentation: User Interfaces - Graphical User Interfaces

General Terms
Design, Human Factors, Experimentation

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
CHI'12, May 5-10, 2012, Austin, Texas, USA.
Copyright 2012 ACM 978-1-4503-1015-4/12/05...$10.00.

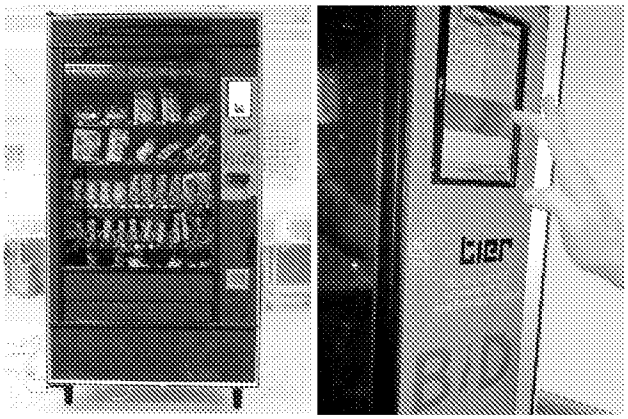


Figure 1. With Umati, the communitysourcing vending machine, users complete tasks on a touchscreen and receive non-monetary rewards.

INTRODUCTION
Crowdsourcing, the division and assignment of tasks to large, distributed groups of online users, has the potential to create new jobs, improve the efficiency of labor markets, and enable a wide variety of new applications. Researchers have demonstrated compelling new systems enabled by crowdsourcing, including applications that assist the blind with visual tasks [8] and that help writers to copy-edit prose [7]. Many crowdsourcing efforts leverage *microtask* markets, which provide platforms for posting and finding short tasks – frequently seconds to minutes long. One of the best-known markets, Amazon Mechanical Turk (MTurk), attracts thousands of employers [15] and has had hundreds of thousands of worker accounts [30].

One limitation of microtask markets is the difficulty of accessing groups with domain-specific skills or knowledge. The short work durations and small rewards attract specific user demographics [30], limiting the variety of knowledge and expertise available. In contrast, vertical online communities (such as graphic design site 99Designs [1] and Q&A site Stack Overflow [25]) successfully gather experts, but they must either focus on building and maintaining a community of volunteers [25], or on enticing experts with high rewards for complex tasks. These hurdles limit the potential for crowdsourcing of expert work.

To enable crowdsourcing of expert work for short duration tasks, we introduce the concept of *communitysourcing*. Communitysourcing deploys tasks on physical kiosks in specific locations that attract the right "crowds" (while repelling the wrong ones), and in contexts where people have

Petitioner Exhibit 1002-2715

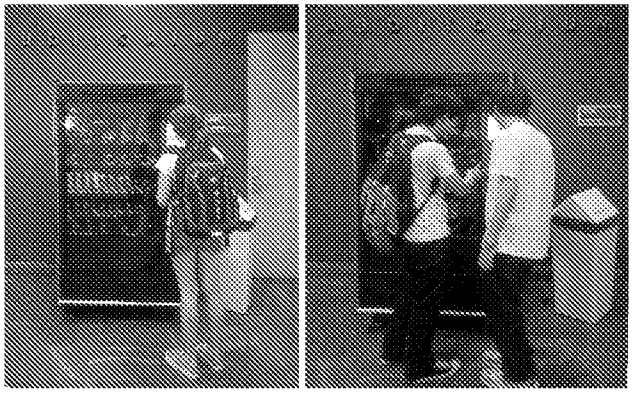


Figure 2. In our study, Umati was deployed in a public hallway. Students and other building occupants graded CS exam questions on Umati.

idle time ("cognitive surplus" [31]). Communitysourcing leverages the specific knowledge and skills of the targeted community; in return, it provides context- and community-specific rewards that users value more than money.

To explore the potential of communitysourcing, we asked the following research questions:

- Can communitysourcing successfully enlist new user groups in crowd work?
- Can communitysourcing outperform existing crowdsourcing methods for expert, domain-specific tasks?
- How does communitysourcing compare to traditional forms of labor, in terms of quality and cost?

We explored these questions by designing, implementing and evaluating a specific communitysourcing instance: *Umati: the communitysourcing vending machine* (see Figure 1). We built Umati by modifying a commercial vending machine. On Umati, instead of inserting money, users select and perform tasks on a high-resolution touch screen. Earned credits can be used to choose and buy items — an internal computer controls the motors that operate each of the vending arms.

We tested Umati with a Computer Science exam grading task. Grading exams is a time consuming, high-volume job that requires significant domain expertise for consistent, correct scoring of open-ended questions. Grading can also be partitioned into many small tasks. We placed Umati in the primary hallway in our Science building and filled it with snacks (see Figure 2). Exams covered introductory Computer Science topics in programming languages, algorithms, and data structures. Umati successfully targeted a specific population (81% of users were trained in Computer Science or Electrical Engineering) and achieved significant throughput: 328 participants graded 7771 exam answers in one week, for approximately $200 of snacks. Umati attracted new workers: 80% of participants had never participated in crowdsourcing before. We compared communitysourced grades against grades from a set of ten experts. Umati was able to exceed the accuracy of traditional single-expert grading (80.3% to 78.3% at the same price) or, alternatively, lower cost by 33% (at the same accuracy). For comparison, we also recruited graders on Mechanical Turk; these workers could not grade

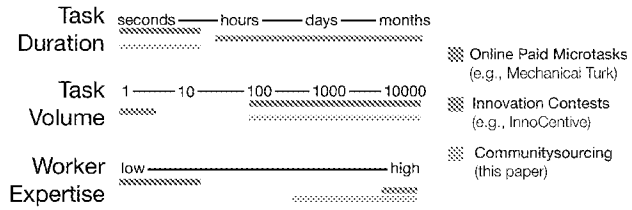


Figure 3. Communitysourcing occupies a unique position in the design space of crowdsourced work: it enables short, high-volume tasks that require high levels of expertise.

accurately ($< 25\%$ agreement with our experts). Our results suggest that communitysourcing can exceed traditional expert performance in domains where online crowdsourcing fails.

In this paper, we begin with a discussion of related work and describe the design space of communitysourcing. We motivate the choice of an exam grading task, then describe the implementation of Umati. We follow with a detailed evaluation of the system and conclude with a summary of our results and pointers to future work.

RELATED WORK

Communitysourcing touches on prior work in crowdsourcing, location-based computing, and kiosk systems. Our experimental task also relates to prior efforts in peer grading. We discuss each area in turn.

Crowdsourcing

Crowdsourcing and human computation are active areas of research inquiry; recent surveys describe a range of approaches [21, 28]. Projects have investigated incentives and game mechanics to motivate workers [35], new applications enabled by crowdsourcing [7, 8, 36], tools to develop crowdsourcing applications [22], and algorithms to coordinate crowd work [5, 6, 20]. Researchers have also contributed methodologies for conducting experiments using online labor [13, 19]. Much recent work focuses on increasing the complexity of work products created by a pool of unskilled workers through redundant microtasks. While communitysourcing also targets tasks of short duration, it recruits domain experts through appropriate choice of location and incentive (see Figure 3).

The dominant strategy to elicit expert responses or expert work online has been to build narrow, domain-specific communities. Topical communities of unpaid volunteers can provide high-quality answers to technical questions. However, creating successful online communities is an uncertain, labor-intensive proposition that requires leadership and constant monitoring [25]. Some online platforms succeed in eliciting paid expert work through competitions, e.g., InnoCentive for pharmaceutical research [2]; 99Designs for graphic design [1]; or TopCoder for programming [4]. Competitions are not appropriate for high-volume work because they strive to find the single best solution among the submissions. Communitysourcing can provide higher throughput by engaging many experts in short tasks.

Petitioner Exhibit 1002-2716

Location-based Computing and Kiosks

Researchers have investigated the role of physical location in crowdsourcing. In participatory sensing [12], people collect and report data about their environment. For example, Creek Watch [18] uses GPS coordinates to crowdsource local watershed measurements. Multiple mobile start-up companies are delivering questions and tasks to members in a given location [11, 23]. In these systems, users first have to sign up for the service and agree to have their location tracked. Communitysourcing attracts people who already frequent a particular locale through a kiosk interface.

Computer-based kiosks have long been used for self-service ticketing, banking, and location-specific information, e.g., in museums [17]. Kiosks have also been deployed in rural areas and developing countries for Internet access, for unsupervised education [27, 32], and to aid communities in reconciliation after civil unrest [33]. Research has focused on security of such public systems [9] and on facilitating information transfer between kiosks and other computing devices [14, 16]. To our knowledge, Umati is the first kiosk that elicits work and rewards workers with physical items.

Education and Grading

Grading open-ended exams is an intrinsically subjective process. One common mechanism for consistently and efficiently grading open-ended questions is peer assessment. Students grading other students can lead to positive impacts on learning and attitude [24, 34]. Peer assessment is usually restricted to students within a particular course, and is prescribed by course staff. In Computer Science, prior work has investigated web-based peer review of assignments [10]. Averages of redundant peer scores are strongly correlated with teachers' scores [29]. Umati generalizes peer assessment beyond course boundaries: it enlists volunteers and provides physical rewards to incentivize participation.

DESIGN CONSIDERATIONS FOR COMMUNITYSOURCING

Successful communitysourcing depends on careful selection of tasks, locations, and incentives. This section discusses important design considerations for each category.

Task Selection

Communitysourcing is best suited for short-duration, high-volume tasks that require specialized knowledge or skills which are specific to a community, but widely available within that community. Simple tasks without expertise requirements (e.g., address verification or text transcription) are a better fit for generic crowdsourcing platforms like Mechanical Turk. Low-volume, long-duration expert jobs (like graphic design or programming) are better served by vertical online markets.

Some representative tasks well-suited for a community-sourcing approach include grading exams in academia, bug and tech support triage in technology companies, fact checking for journalism, and community-specific market research in bars or specialty shops. Short task durations enable users to work on a kiosk without ergonomic issues, and enable many user to participate. Public kiosks can potentially attract a large number of users, supporting, as well as requiring, a high task volume.

Location Selection

A communitysourcing system must target those locations where the required skills are prevalent. The locations must also repel those *without* the required knowledge. For instance, placing a kiosk in a bar could potentially target young men with market research tasks – but the kiosk would also be accessible by young women. A better location to exclusively target men would be their restroom at the bar.

The targeted community must also have some "cognitive surplus" [31] available for doing work. Practically, this means placing the kiosk in an area where people have spare time, e.g., in lounges, government office waiting rooms, or airports.

Reward Selection

Rewards must be interesting and valuable to the targeted community in the given location. For instance, airport travelers may value Wifi Internet access. In contrast, Wifi access has lower utility on a college campus, where free Internet is readily available. While cash is an obvious reward (consider an ATM-like kiosk), it has been shown that individuals can value items more than money in specific contexts and locations [26].

COMMUNITYSOURCING IN ACTION

For our deployment, we chose exam grading as an experimental task, a university department as the location, and snacks as rewards. This section briefly justifies these design choices in light of the earlier design guidelines for communitysourcing.

Task: Grading exams is a painful, high-volume task for teaching staff. An individual student answer can be graded quickly, but large courses with hundreds of students generate thousands of answers. While people outside an academic discipline are unlikely to possess the requisite knowledge to grade open-ended problems, redundant peer grades are strongly correlated with expert scores [29], suggesting that students can grade each others' assignments and exams.

Location: College campuses commonly assign buildings to disciplines (departments). These buildings rarely attract visitors outside the discipline. Our Computer Science (CS) building supports mainly CS classes, along with a few unrelated events. We placed our kiosk in front of the major lecture hall in the CS building, an area where students often wait for class to begin, maximizing the cognitive surplus.

Reward: Food is the most common reward given to entice students to participate in campus events. Companies commonly provide pizza to bring students to recruitment events; teachers bring candy to class sections to entice participation. We decided to use snacks as our reward. This choice also impacted the physical design of our kiosk. The most common system for distributing snacks is the ubiquitous vending machine; it is familiar and clearly communicates the nature of the rewards being distributed.

Petitioner Exhibit 1002-2717

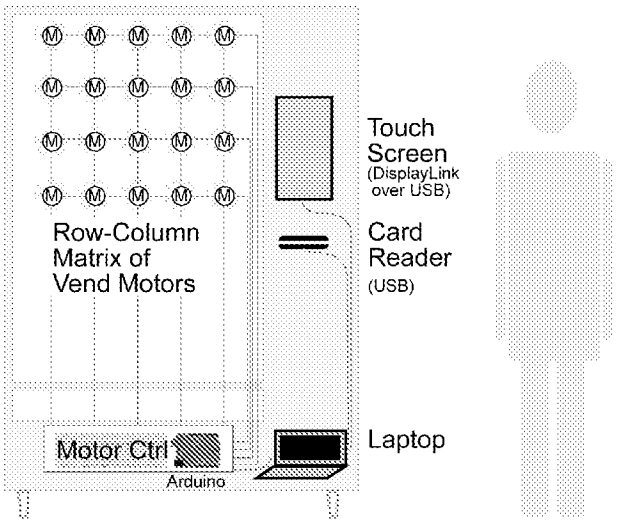


Figure 4. Umati uses an internal laptop to control a touchscreen, USB card reader, and the vending motors. Users complete tasks on the touchscreen for rewards from the machine.

These design decisions guided our implementation of *Umati: the communitysourcing vending machine*, as described in the next section.

UMATI: SYSTEM IMPLEMENTATION

The Umati system comprises custom vending hardware; a generic software platform for work tasks; and specific task user interfaces. We describe each in turn.

Hardware: Hacking a Vending Machine

Umati is a modified commercial vending machine (specifically, a 1986 Snackshop 4600, Figure 1). We removed all legacy vending equipment (the bill exchanger, coin reader, keypad interface, analog motor-control circuit boards), leaving just the vending shelves and dispensing mechanism. We installed a touchscreen and keycard reader on the front of the machine, which provide the primary user interface (see Figure 4). Users must first swipe their magnetic strip ID card (given to all students, faculty, and staff on campus); card IDs enable Umati to distinguish users, though our prototype does not link card IDs to users' names. Users complete tasks on the touch screen interface which is connected to an internally mounted laptop.

Rewards are dispensed through programmatic control of the vending mechanisms. The shelves use metal spirals driven by DC motors. The motor leads form a row-column matrix: when a particular row lead is powered and a column lead grounded, the motor at the intersection of row and column spins, dispensing an item. We attached the row-column end points to relays controlled by an Arduino microcontroller, and programmed the microcontroller to respond to vend requests from the laptop over a serial link. Motors spin uniformly enough to vend items with open-loop control, powering motors for a fixed amount of time.

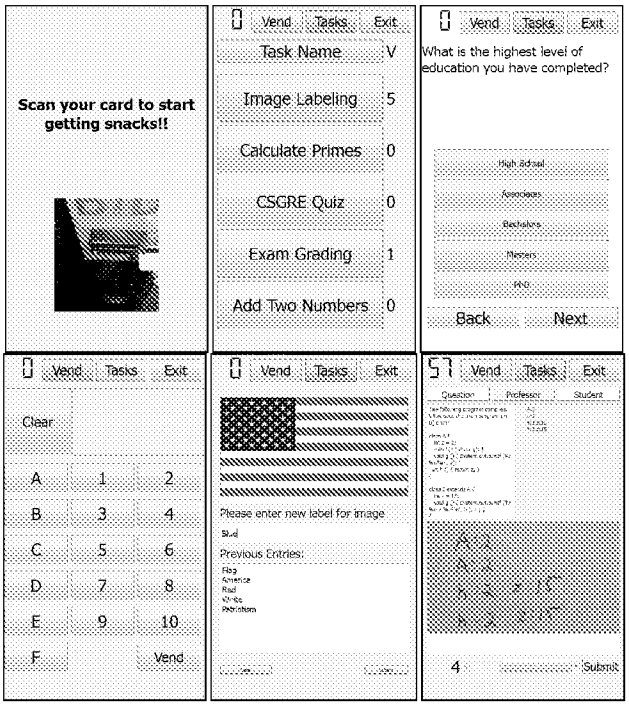


Figure 5. Umati's UI, clockwise from top left: introductory attract screen, task selection, survey task, grading task, image labeling task, and vending interface.

Software: Maximizing a Small Touch Screen

We developed the Umati software using Python and the PyQt4 UI toolkit. Umati's architecture was designed as a generic task platform: each task and its user interface are written as plug-ins to a work management system. As a result, Umati supports many task types besides exam grading.

When the machine is idle, it displays an *attract screen*: a looping video demonstrating how to log in by swiping an ID card (see Figure 5). After swiping, users are presented with the *Task Selection* screen, allowing them to choose their task. If there is just one available task, the selection screen is bypassed and users are immediately presented with that task. The user's earned credits are shown in the top left, and stored across work sessions. When a user wishes to cash in their credits, they switch to the *Vending* interface which provides a software keypad to select the tray of the desired item.

Tasks

We have implemented a variety of tasks for Umati: math tests, CS GRE questions, surveys, exam grading, and image labeling. Some of these task interfaces are shown in Figure 5. For our evaluation, we tested just two: surveys and grading.

Surveys: The survey task constructs an interface from an external XML file that defines questions and multiple choice answer sets. For our deployment, Umati had a basic demographic survey which collected age, department, educational status, and prior exposure to crowdsourcing. Every user was required to complete this survey before starting another task on Umati.

Petitioner Exhibit 1002-2718

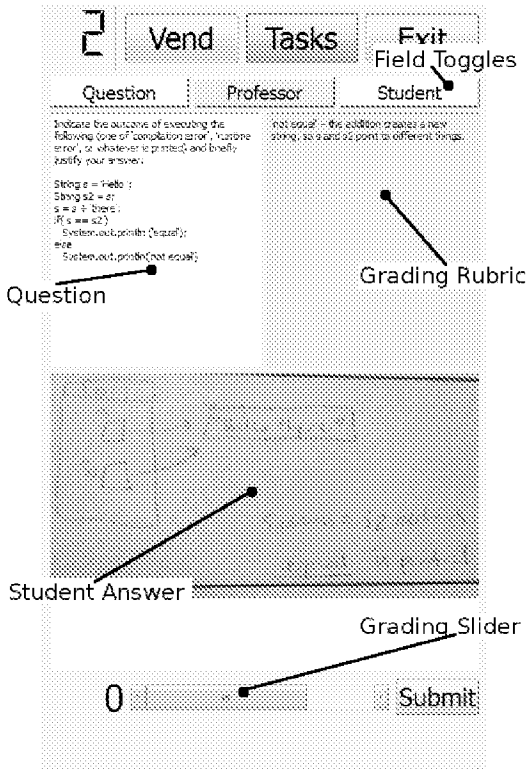


Figure 6. The Umati grading interface shows a question, an answer key, and an image of a student response. Workers assign points with a slider.

Grading: The grading interface presents three panels of information simultaneously to the participant: the question, the instructor's answer key, and a student answer (see Figure 6). Each panel can be opened and closed using toggle buttons on the top row, to maximize the limited screen space. Each panel also allows panning by dragging and zooming by double-tapping. Grades are gathered on a numeric scale: the user enters the grade using a slider widget. Upon submission, Umati presents another student answer *to the same question*, if one is available. This allows a user to memorize the question and answer key, accelerating their grading of student answers. It also supports grading privacy, as graders cannot easily grade all of a specific student's answers. Users cannot grade the same exam answer twice.

Spam Detection: Incorrect or low-quality responses ("spam") are common for crowdsourcing; workers often complete tasks quickly and with little thought in order to maximize their earnings. To account for this tendency, Umati implements a simple spam detection system. Each task definition includes "gold standard" tasks, comprised of a task with a known correct response. If a user fails two of these tasks, that user is logged out and their ID is blacklisted from future use. Inserting such checks is a well-established technique for improving the quality of crowdsourced work [19].

EVALUATION

Our evaluation sought to answer three primary research questions about communitysourcing: Can it enlist new user groups in crowd work? Can it outperform existing crowdsourcing methods? And can it match more traditional approaches, in terms of cost and accuracy?

Study Design

We created a set of Computer Science exams with answers. Three groups of participants graded the exams: users of our vending machine (Umatiers), Mechanical Turk workers (Turkers), and a group of former or potential Computer Science teaching assistants (Experts).

Exam Corpus

We created a custom exam from prior mid-term questions of our Computer Science department's second-semester undergraduate course, *CS2*. The exam was comprised of 13 questions covering basic complexity theory, object-oriented programming, search algorithms, and bit operations. Eight undergraduate students were recruited as test-takers. These students had recently completed CS2 or were enrolled at the time of the study. Students completed the exam on paper. For our *gold standard* tasks, we added an exam completed using the instructor's grading rubric, giving us question/answer pairs that are always correct. These answers were used for our spam detection algorithm. 105 sample exam answers were generated in total. Test-takers received either a 5 USD gift card, or could make an equivalent charitable donation.

Common Grading Instructions

Graders in all conditions were asked to assign 0 to 4 points for each question. The Instructor's answer key was used as the grading rubric. The rubric provided no instructions for assigning partial credit. While all questions required computer science knowledge to produce a correct answer, they varied in the amount of knowledge required to assess that answer. Some were *simple*, requiring only basic pattern matching for identifying correct answers. Others were *open-ended*, requiring a deeper understanding of the underlying material. Assigning partial credit for incomplete answers always required domain-specific knowledge.

For the exam we tested, five questions were simple, while eight were open-ended. An example open-ended question and grading rubric follows:

> *Q: Briefly explain the difference between a (Java) instance variable and a (Java) class variable.*
>
> *A: Each object has its own distinct copy of an instance variable. But all the objects in a class share just one 'copy' of a class variable.*

Paper exams had a defined answer box for each question. We used Shreddr [3] to extract scanned answers from the exams. These images of answers were shown in the grading interface (Figure 6). Three sets of participants then graded the exams: 1) Umati users, 2) Mechanical Turk users, and 3) experts recruited from a pool of qualified students. These conditions are described in more detail below.

Grading on Umati

We deployed Umati outside the main Computer Science lecture hall for one week. This lecture hall is primarily

Petitioner Exhibit 1002-2719

used for undergraduate courses, although graduate students, staff, faculty and visitors also frequent this centrally located ground-floor area. Users received no other introduction to the system or tasks besides the looping video instructing them to swipe their card.

The machine was loaded with $200 worth of candy. Users earned one credit per graded answer, and five for completing the survey. Most items were priced at 20 credits (with some priced at 10 and 30). In a small pilot study, we found that users completed roughly 20 tasks in five minutes. We estimated that five minutes was the maximum amount of time users would be willing to spend in front of a vending machine at any one time. Candy was purchased from a local bulk wholesale store at an average of 45 cents per item. At this price, Umatiers were paid 2.25 cents per answer, in candy.

Grading on Mechanical Turk

Workers on Amazon's Mechanical Turk (Turkers) graded the same exam questions and answers, on a web interface that was similar to the Umati touch screen interface; workers saw the question, the answer key, and the student's answer. Each Human Intelligence Task (HIT) consisted of grading all 9 answers to the same question (8 students and the experimenter's gold standard), paying 23 cents (2.6 cents / answer). We posted 130 HITs on Turk, obtaining 10 sets of grades for each student answer.

Turkers answered the same gold standard questions as Umati users, and we applied a similar spam detection algorithm. We present two sets of results: 1) all Turkers (regardless of gold standard performance); and 2) the subset of Turkers that passed the spam filter (failing at most one gold standard question). As with Umati, any answers provided before a second failed question are used in our analysis.

After a first set of workers completed our grading HITs, we also attempted to recruit more knowledgeable Turkers through a qualification test. Workers had to pass the test before they could grade exam answers. The test comprised five multiple choice questions on computational complexity and Java. For example:

What is the Big-O run-time of the following algorithm?

```
function(arg1, arg2):
   return arg1+arg2
```

A: $O(1)$ *B:* $O(logn)$ *C:* $O(n)$ *D:* $O(nlogn)$ *E:* $O(n^2)$

For these qualified Turkers we offered 25 cents per set of 9 grades (2.8 cents /answer).

Grading By Experts

Ten former or potential CS teaching assistants graded the exam corpus on paper. These graders included: one graduate instructor for *CS 2*, one high-scoring undergraduate (received an A in *CS 2*), and eight CS PhD students. All had prior teaching experience. Each participant was paid 25 USD in Amazon credit to grade all 105 answers.

At our university, only graduate students are allowed to grade exams. Graduate students earn over 38 dollars per hour, when including basic tuition and fee remission. On average, experts graded 115 answers per hour, for an effective rate of 34 cents per answer. All of the expert graders passed the gold-standard spam detection algorithm, as should be expected.

Measures

Grading is inherently subjective — even experts can disagree. To enable meaningful comparisons between our different conditions, we define dependent measures that compare *grade distributions* and *agreement with median expert scores.*

Comparing Grade Distributions

For both crowdsourced grading methods, Umati and Mechanical Turk, we compute a Chi Squared test statistic across the 105 exam answers to determine if the distribution of crowdsourced grades in either condition differs significantly from the expert distribution.

Grade Agreement

To measure the grading accuracy of our approach, we use the median of all expert graders (*median expert grade*) as the "correct" grade for a student's answer. We then compute *grade agreement* as the percentage of exam answers for which the median Umati and Turk grades match the median expert grade.

The status quo is to use a single expert grader, not the median of multiple graders. To investigate the relationship between grading accuracy and the cost of recruiting additional graders, we randomly sample (with replacement) subsets from each distribution of graders (expert, Umati, and Turk). For instance, we sample a single expert grader from the expert distribution, and compare that to the median expert grade for all exam answers. Similarly, we also sample subpopulations (for instance, seven Turkers), take the median of their grade distribution, and compare that to the ("correct") median expert grade for all exam answers. This is repeated 1000 times to compute the *subgroup grade agreement* (e.g., between seven Turkers and all ten experts).

Results

We report descriptive usage results, comparisons of the experimental conditions, and qualitative observations.

Umati Users

328 participants graded 7771 exam answers on Umati in one week. Figure 7 shows self-reported demographic data from the survey. The users were primarily undergraduate computer scientists. 80% of Umati users had never previously participated in any online crowdsourcing activity (showing that Umati engaged new users in crowdsourcing). Users who successfully completed at least one task had a median usage time of 4 minutes, completing an average of 16 tasks. The most active user (or group, see below) worked continuously for more than an hour, completing 85 tasks in a row. Several users completed all 105 of the grading tasks. 61 users (19%) were blacklisted by the system for failing gold standard tasks. The high failure rate may be a consequence of the machine's

Petitioner Exhibit 1002-2720

Filters	Participants	%	Tasks Completed	Task %
Total	328	100%	7771	100%
Undergraduates	263	80%	6297	81%
Graduates	39	12%	943	12%
Other (Professors, Visitors, Staff)	26	8%	531	7%
Computer Science	234	71%	5977	77%
Electrical Engineering	34	10%	485	6%
Other/Not Affiliated	60	18%	1309	17%
Had Not Crowdsourced	262	80%	5933	76%
Had Crowdsourced	66	20%	1838	24%
Knows about Crowdsourcing	216	66%	4469	58%
Does Not Know About Crowdsourcing	112	34%	3302	42%

Figure 7. Descriptive statistics for one week of Umati use.

novelty: users may have explored the interface without understanding the consequences of incorrect answers.

81% (268) of Umati users majored in Computer Science or Electrical Engineering; both groups are required to take *CS 2*. Our system was able to effectively engage our target population and complete a large number of tasks. This demonstration of Umati's ability to target crowdsourcing work to hundreds of unique, expert users over the span of just one week is a primary result of our work. We also note that these numbers were achieved despite limited resources: twice, our vending machine was emptied of snacks in less than two days; we refilled once. Effectively, the machine ran for four of the seven days.

Mechanical Turk Users

We gathered 1050 grades in three days using Mechanical Turk. 46 unique Turkers graded exams, with 16 (35%) failing the spam detection (incorrectly grading two or more *gold standard* questions). While we offered higher wages to workers who passed the CS qualification, no workers successfully qualified during our experiment. We conclude that a qualification exam is not an efficient mechanism for attracting workers with computer science knowledge on Mechanical Turk.

Comparing Grade Distributions

We computed the distribution of grades for each exam answer from experts, Turkers and Umatiers. These distributions were summed across all responses, and across all answer items, to produce the statistic used to test the potential differences between response distributions.

Chi Squared tests find a significant difference between the expert and either Turker score distribution ($P_{TURK} < .001$ and $P_{TURK_{NoSpam}} < .001$). We see no such significant difference between the experts and Umati users ($0.263 < P_{UMATI} < .997$) [1]. This suggests that the Umatiers, on aggregate, grade similarly to experts; Turkers do not.

[1]The 105 survey items allowed for 5 score options, zero to four. Each individual answer's distribution then has 4 degrees of freedom (knowing the probability mass in bins 0 through 3 fixes the amount of mass in bin 4). From this, we know the number of degrees of freedom for the overall Chi Squared test is at least $4 \times 105 = 420$ and at most $5 \times 105 - 1 = 524$, depending on the amount of dependence between the student answers. This provides us with bounds on the p-values of each experiment.

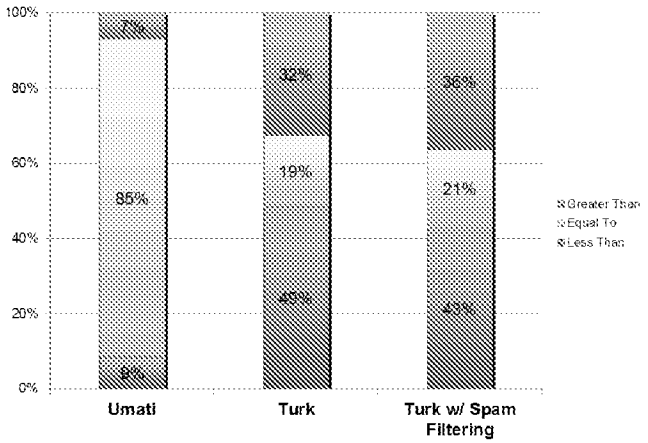


Figure 8. Agreement between conditions and the median of the 10 expert graders. Umati users' response distributions were much closer to the experts than distributions of Mechanical Turk users.

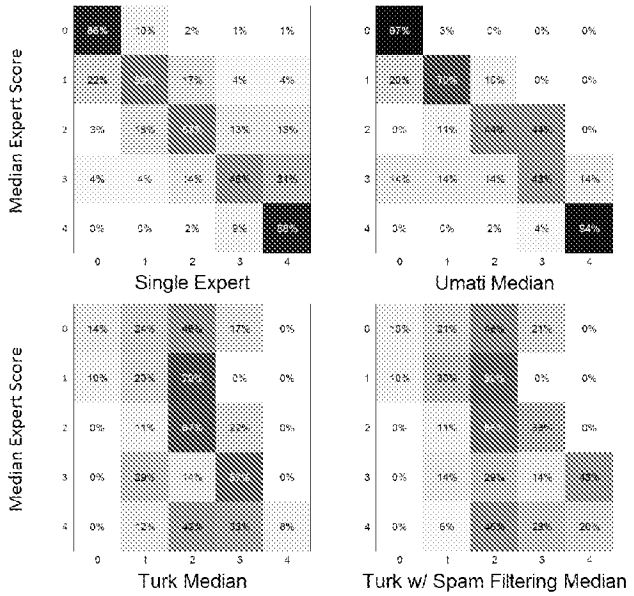


Figure 9. Comparing grade agreement between the the experts and our test conditions. Umatiers and single experts often agreed with the pool of experts. Turkers were consistently random.

Comparing Grades

Umati users agreed with the experts' median grade 85% of the time (Figure 8). In comparison, Turkers only agreed with experts 19% of the time; this figure increases only slightly to 21% with spam filtering. [2]

Figure 9 shows how different graders diverged from the grades of *all* expert graders. Boxes along the diagonal show agreement with experts. Individual experts and Umatiers agree strongly with all experts on assigning full credit or no credit. Single experts appear to have less variance than

[2]Random guesses have an expected agreement of 20% on a five-point scale.

Petitioner Exhibit 1002-2721

Umatiers when assigning partial credit. We reserve a careful study of systematic biases to future work. MTurk workers' responses have no discernible pattern, leading to a generally centered (2/4) median score.

Price-Accuracy Trade-off

We explore the effects of assigning varying numbers of graders on accuracy by sampling subgroups from the distribution of experts, Turkers, and Umatiers and calculating median agreements for these groups to all experts.

Figure 10 plots agreement as greater numbers of respondents are considered. Individual expert graders agreed with the median of all experts 78.3% of the time. Ten Umatiers agreed 79% of the time, but cost 33% less ($10 \times 2.3 = 23$ cents/grade vs 34 cents/grade). Mechanical Turk users never approximate the experts, regardless of their number. In fact, Turkers are *less* likely to agree with the median expert grade as the number of respondents increases.

If we keep cost constant, Umati is more accurate than a single expert grader (see Figure 11). Thirty-four cents can buy one expert answer, with an accuracy of 78.3%; or fifteen Umatiers, who have an accuracy of 80.3%. Because result quality is achieved through multiple graders at lower individual pay, it is easy to increase or decrease the accuracy by adjusting the number of redundant assignments. Additional workers can also be dynamically assigned to more difficult or controversial cases where initial ratings diverge, while the number of assignments can be held low for answers that are clearly correct or incorrect.

Qualitative Observations

Throughout the week-long deployment, we observed users to obtain feedback on usability and user experience. At times, student interest was higher than our single machine could handle: queues formed in front of the machine. We noticed that groups of students often used the system together (see Figure 2). Some groups were formed ad-hoc, by students waiting in line. Other groups approached the machine together. Using Umati seemed to be a social event; groups would argue about the specific merits of different answers. Such additional discussion is an unexpected secondary benefit: academic departments will likely welcome increased discussion of class material by their students. Groups would also share the rewards, for instance splitting a bag of candy amongst the participants.

However, groups could also negatively impact grading: student groups seemed more inclined to attempt to defraud the system. One group attempted to pry open the door. Queues of waiting students potentially limit the throughput of the machine, but are hard to avoid — physical interfaces do not scale easily. A number of users complained that they were unjustly blacklisted. Often this was because they had forgotten to log out. A few users reported being removed because they were exploring and were not aware of the repercussions. Better instructions about safeguarding mechanisms could address these problems.

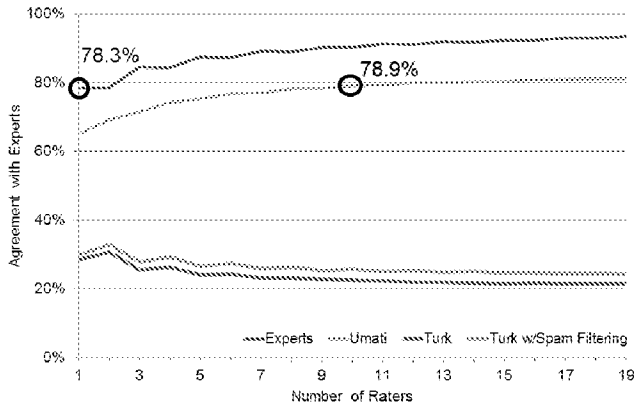


Figure 10. The accuracy of Umati users becomes comparable to a small number of experts as more participants are involved. Here, we show the point where Umati accuracy surpasses that of a single expert.

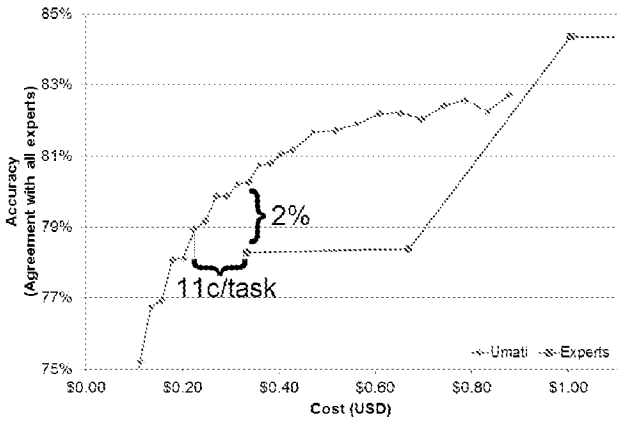


Figure 11. Accuracy (compared with all experts), for experts and Umati. One expert grader costs the university approximately 34 cents/task.

DISCUSSION

In this section we discuss some important limitations of Umati and of our particular study design. We also discuss possible alternative strategies for communitysourcing.

Privacy and Confidentiality for Grading

Publicly displaying student answers raises obvious privacy and confidentiality concerns. For example, handwriting might reveal the identity of a test taker. Students may not want peers grading their exams (though peer grading already exists in different forms at many schools). For the experiment described in this paper, paid participants generated exam answers; students' course grades were not determined by Umati workers. In the future, Umati can be used in situations where students have consented to this form of grading at the outset of a course. Alternatively, Umati can be used for many forms of assessment with lower stakes, e.g., homework grading or practice exams.

With the current design, students may also attempt to game the system by providing high grades to their own (or their

Petitioner Exhibit 1002-2722

friend's) answers. We limited this concern by forcing graders to view all submissions to one question before moving on to the next questions. Attackers thus must grade *every* answer to *every* question in order to comprehensively cheat for just one student. Umati also gathers the student's ID, allowing us to programmatically block them from grading exams for classes they are enrolled in, or have not yet taken. To reduce the risk of cheating and of inadvertent identification by peers, test-takers and test-graders could also be geographically and socially separated – for example, students on the East Coast could grade assignments from students on the West Coast, and vice versa.

Study Limitations

Our current study has several important limitations that should be addressed in future work.

No Comparison to Expert Work Platforms

We compared the effectiveness of grading tasks on Umati to Mechanical Turk. However, other crowdsourcing technologies could potentially be useful for grading. For instance, the computing experts on Stack Overflow [25] should have the expertise required to assess introductory exams. Similarly, we could hire a contractor on oDesk.

We are skeptical that these other engines are well suited for short-duration, expert tasks like grading. An individual expert (as on oDesk) is unlikely to be better or cheaper than the student graders we compared against. Stack Overflow workers provide the *best* answer to a question, disallowing the high-volume of tasks needed for grading. However, we have not yet tested whether these intuitions hold.

Short Deployment

A major limitation of our study is the short one-week duration of the deployment. High initial usage led to task starvation: we did not have enough sample tasks for graders. After one week, each exam response had already gathered an average of 68 grades.

While we know that the initial interest was high, we cannot yet comment on sustained, steady-state usage of Umati. We observed that more tasks were completed in the latter half of our deployment, suggesting that user momentum was still building. We are actively seeking new high-volume tasks for future deployments.

Similarly, we cannot say how much of this initial interest in Umati was due to the specific properties of our targeted crowd. It may be that Computer Science students are more excited about crowdsourcing than other groups. We hope to resolve this by targeting different communities (with different tasks) in the future.

Interface Affordances Limit Work Duration

We chose grading as an example communitysourcing task for Umati in part because it could be achieved with minimal user input. Umati's design might preclude many other types of work. This is primarily due to its limited input and output affordances: a 7-inch vertical touch-screen is inefficient and error-prone for many data-entry heavy tasks. Kiosks must appear *approachable* to attract users and be *robust* to public abuse. Overly complex interfaces can create challenges for achieving these goals.

An alternative would be to divide work and reward interfaces: experts could perform work on their own computers or smart phones, e.g., through a web interface, and then come to a nearby kiosk or vending machine to redeem their rewards. In such a design, the kiosk would primarily enforce locality and community membership. However, this design would reduce the social visibility of the machine: in our deployment, students were frequently attracted by watching other students use Umati. In addition, communitysourcing requires available cognitive surplus. There are few other distractions in a public hallway; spare time may be more difficult to find when competing with a myriad of ways to spend time on the Internet. We reserve further study of these questions for future work.

Applications of Communitysourcing to Other Problems

Our study demonstrated the value of communitysourcing for one particular task domain and reward type. Grading is just one example of a high-volume task that requires an expert population; we could instead provide specialized surveys. Snacks are just one of many possible rewards; students may prefer video game currency to snacks. In the future, we plan to develop alternative embodiments of communitysourcing, and to develop a theory of how the combination of task, location and reward affect work quality and quantity. For example, future deployments could include: a bug triage espresso machine in the lounge of a big technology company; a jukebox with market research tasks at a bar; or a slot machine in the airport with travel review tasks.

CONCLUSION

In this work we introduced the idea of communitysourcing — the use of physical kiosks to crowdsource work from targeted populations. Communitysourcing is achieved by: 1) situating tasks in specific physical spaces that attract the right "crowd" and where people have idle time and 2) providing physical, context- and community-specific rewards that users value more than money. These two key points invite new expert workers to participate in short duration crowd work.

To explore the potential of communitysourcing, we designed, implementing and evaluated a specific communitysourcing interface for a particular expert task. *Umati, the communitysourced vending machine* enabled users to earn credit for purchasing snack items by performing grading tasks on a touchscreen. We investigated whether Umati can recruit new users: over one week, Umati successfully targeted a student community, with 302 students (of 328 total) grading 7240 (of 7771 total) exam answers. 80% of all the users had never participated in crowdsourcing before. We also investigated how task quality compared to both online crowdsourcing and traditional, offline work.

We found that Umati was able to grade exams more accurately (80.3% vs 78.3% at the same cost), or at lower

Petitioner Exhibit 1002-2723

cost (23c/answer vs 34c/answer at equivalent accuracy), than traditional single-expert grading. Workers on Mechanical Turk were unable to successfully grade the exams.

In the future, we would like to test Umati over a longer period of time, to observe patterns of use and investigate the long-term prospects of expert work on kiosks. We would also like to consider alternate communitysourcing scenarios with varying configuration of task, location and reward; for example, one where users could complete tasks online using their own computers, obtaining one-time keys that can be redeemed for credit.

ACKNOWLEDGMENTS

We thank Bryan Trinh for his help constructing Umati and Kehontas Rowe for task design and video production. We thank Kelly Buchanan, Isabelle Stanton, and Alice Chen for putting up with us. Lastly, we thank Eric Brewer and Laurent El Ghaoui for letting us take on this project.

REFERENCES

1. 99Designs. http://www.99designs.com/. Retrieved 9/2011.
2. Innocentive. http://www.innocentive.com/. Retrieved 9/2011.
3. Shreddr. http://www.shreddr.org/. Retrieved 9/2011.
4. Topcoder. http://www.topcoder.com/. Retrieved 9/2011.
5. Ahmad, S., Battle, A., Malkani, Z., and Kamvar, S. The jabberwocky programming environment for structured social computing. In *Proceedings of UIST'11*, ACM (2011), 53–64.
6. Bernstein, M. S., Brandt, J., Miller, R. C., and Karger, D. R. Crowds in two seconds: Enabling realtime crowd-powered interfaces. In *Proceedings of UIST'11*, ACM (2011), 33–42.
7. Bernstein, M. S., Little, G., Miller, R. C., Hartmann, B., Ackerman, M. S., Karger, D. R., Crowell, D., and Panovich, K. Soylent: a word processor with a crowd inside. In *Proceedings of UIST'10*, ACM (2010), 313–322.
8. Bigham, J. P., Jayant, C., Ji, H., Little, G., Miller, A., Miller, R. C., Miller, R., Tatarowicz, A., White, B., White, S., and Yeh, T. Vizwiz: nearly real-time answers to visual questions. In *Proceedings of UIST'10*, ACM (2010), 333–342.
9. Garriss, S., Cáceres, R., Berger, S., Sailer, R., van Doorn, L., and Zhang, X. Trustworthy and personalized computing on public kiosks. In *Proceeding of MobiSys '08*, ACM (New York, NY, USA, 2008), 199–210.
10. Gehringer, E. F. Electronic peer review and peer grading in computer-science courses. In *Proceedings of SIGCSE'01*, ACM (2001), 139–143.
11. Gigwalk. http://www.gigwalk.com. Retrieved 9/2011.
12. Goldman, J., Shilton, K., Burke, J., Estrin, D., Hansen, M., Ramanathan, N., Reddy, S., Samanta, V., Srivastava, M., and West, R. Participatory Sensing: A citizen-powered approach to illuminating the patterns that shape our world. *Foresight & Governance Project, White Paper* (2009).
13. Heer, J., and Bostock, M. Crowdsourcing graphical perception: using mechanical turk to assess visualization design. In *Proceedings of CHI'10*, ACM (New York, NY, USA, 2010), 203–212.
14. Huang, A., Pulli, K., and Rudolph, L. Kimono: kiosk-mobile phone knowledge sharing system. In *Proceedings of MUM'05*, ACM (New York, NY, USA, 2005), 142–149.
15. Ipeirotis, P. G. Analyzing the Amazon Mechanical Turk marketplace. *ACM XRDS 17* (December 2010), 16–21.
16. Izadi, S., Brignull, H., Rodden, T., Rogers, Y., and Underwood, M. Dynamo: a public interactive surface supporting the cooperative sharing and exchange of media. In *Proceedings of UIST'03*, ACM (New York, NY, USA, 2003), 159–168.
17. Kearsley, G. *Public Access Systems: Bringing Computer Power to the People*. Ablex Publishing Corporation, 1994.
18. Kim, S., Robson, C., Zimmerman, T., Pierce, J., and Haber, E. Creek watch: Pairing usefulness and usability for successful citizen science. In *Proceedings of CHI '11*, ACM (2011), 2125–2134.
19. Kittur, A., Chi, E. H., and Suh, B. Crowdsourcing user studies with mechanical turk. In *Proceeding of CHI'08*, ACM (New York, NY, USA, 2008), 453–456.
20. Kittur, A., Smus, B., Khamkar, S., and Kraut, R. Crowdforge: Crowdsourcing complex work. In *Proceedings of UIST'11*, ACM (2011), 1801–1806.
21. Law, E., and von Ahn, L. *Human Computation: An Integrated Approach to Learning from the Crowd*. Morgan & Claypool, 2011.
22. Little, G., Chilton, L. B., Goldman, M., and Miller, R. C. Turkit: human computation algorithms on mechanical turk. In *Proceedings of UIST '10*, ACM (New York, NY, USA, 2010), 57–66.
23. Localmind. http://www.localmind.com. Retrieved 9/2011.
24. Mafi, M. Grading: Involving students in a time-saving solution to the homework problem. *Engineering Education 79*, 3 (April 1989), 444–446.
25. Mamykina, L., Manoim, B., Mittal, M., Hripcsak, G., and Hartmann, B. Design Lessons from the Fastest Q&A Site in the West. In *Proceeding of the CHI'11*, ACM (2011), 2857–2866.
26. Menger, C. *Grundsätze der Volkswirtschaftslehre*. Braumüller, 1871.
27. Mitra, S. Self organising systems for mass computer literacy: Findings from the 'hole in the wall' experiments. *International Journal of Development Issues 4*, 1 (2005), 71–81.
28. Quinn, A., and Bederson, B. Human computation: A survey and taxonomy of a growing field. In *CHI '2011: Proceeding of the twenty-ninth annual SIGCHI conference on Human factors in computing systems* (2011), 1403–1412.
29. Reily, K., Finnerty, P. L., and Terveen, L. Two peers are better than one: aggregating peer reviews for computing assignments is surprisingly accurate. In *Proceedings of GROUP '09*, ACM (2009), 115–124.
30. Ross, J., Irani, L., Silberman, M. S., Zaldivar, A., and Tomlinson, B. Who are the crowdworkers?: shifting demographics in mechanical turk. In *Extended Abstracts of CHI'10*, ACM (2010), 2863–2872.
31. Shirky, C. *Cognitive Surplus: Creativity and Generosity in a Connected Age*. Penguin Press, 2010.
32. Slay, H., Wentworth, P., and Locke, J. Bingbee, an information kiosk for social enablement in marginalized communities. In *Proceedings of SAICSIT '06* (2006), 107–116.
33. Smyth, T. N., Etherton, J., and Best, M. L. Moses: exploring new ground in media and post-conflict reconciliation. In *Proceedings of CHI '10*, ACM (2010), 1059–1068.
34. Topping, K. Peer assessment between students in colleges and universities. *Review of Educational Research 68*, 3 (1998), 249–276.
35. von Ahn, L., and Dabbish, L. Designing games with a purpose. *Communications of the ACM 51* (August 2008), 58–67.
36. Yan, T., Kumar, V., and Ganesan, D. Crowdsearch: exploiting crowds for accurate real-time image search on mobile phones. In *Proceedings of MobiSys '10*, ACM (New York, NY, USA, 2010), 77–90.

Petitioner Exhibit 1002-2724

NATIONAL AUTOMATIC MERCHANDISING ASSOCIATION

Serving the Vending / Foodservice management industry

Multi-Drop Bus / Internal Communication Protocol

MDB / ICP

Supported by the Technical Members of:

NAMA	**N**ational **A**utomatic **M**erchandising **A**ssociation
EVA	**E**uropean **V**ending **A**ssociation
EVMMA	**E**uropean **V**ending **M**achine **M**anufacturers **A**ssociation

Version 3.0

March 26, 2003

National Automatic Merchandising Association
20 N. Wacker Drive, Suite 3500
Chicago, Illinois 60606-3120 USA
312-346-0370 FAX 312-704-4140
E-Mail: Tech@vending.org

Petitioner Exhibit 1002-2725
CSC ServiceWorks – Ex. 1008

(this page intentionally left blank)

Multi-Drop Bus / Internal Communication Protocol

Table of Contents

Revisions

Introduction

Section 1
General Information

1. Introduction
2. Operational and Application Notes
3. Levels and Options

Section 2
Communication Format

1. Byte Format
2. Block Format
3. Peripheral Addresses
4. Software Operational Rules
5. Typical Session Examples
6. File Transport Layer

Section 3
Bus Timing

1. Timing Definitions
2. Timing Specifications
3. Timing Diagram

Section 4
Hardware Specification

1. Bus Power Supply Definition
2. Bus Transmitter/Receiver Specification
3. Connector Specification
4. Example Schematic

Section 5
Coin Acceptor/Changer
VMC/Peripheral Communication Specifications

1. Introductions
2. VMC Commands
3. VMC Command Format
4. Changer Non-Response Time
5. Changer Power Requirements

Petitioner Exhibit 1002-2727
CSC ServiceWorks – Ex. 1008
Page 3 of 270

Section 6
Bill Validator
VMC/Peripheral Communication Specifications

1. Introductions
2. VMC Commands
3. VMC Command Format
4. Bill Validator Non-Response Tome
5. Bill Validator Power Requirements

Section 7
Cashless Device(s)
VMC/Peripheral Communication Specifications

1. Introduction
2. State Definitions
3. Command Protocol
4. Cashless Device Command Response Formats
5. Cashless Device Non-Response Time
6. Cashless Device Power Requirements

Section 8
Communications Gateway
VMC/Peripheral Communication Specifications

1. Introduction
2. VMC Commands
3. Communications Gateway Command Format
4. Communications Gateway Non-Response Time
5. Communications Gateway Power Requirements
6. Communications Gateway Examples

Section 9
Universal Satellite Device
VMC/Peripheral Communication Specifications

1. Introduction
2. USD Summary
3. Command Protocol
4. USD Power Requirements
5. Examples - Mode 1 / 2 / 3 Sessions
6. Examples - Data Block Transfers

Section 10
Coin Hopper or Tube – Dispenser
VMC/Peripheral Communication Specifications

1. Introduction
2. VMC Commands
3. VMC Command Format
4. Dispenser Non-Response Time
5. Dispenser Power Requirements

Petitioner Exhibit 1002-2728
CSC ServiceWorks – Ex. 1008
Page 4 of 270

Appendix 1
Currency Codes

Appendix 2
Battery Operated Card Reader

Petitioner Exhibit 1002-2720
CSC ServiceWorks – Ex. 1008
Page 5 of 270

Revisions

Version 3.0

Version 3.0 of this specification is the third release of the international **Multi-Drop Bus / Internal Communication Protocol** (**MDB / ICP**). This specification is the continued effort put forth by technical members of NAMA and the EVA. The basis for this specification is the Version 2.0 international **Multi-Drop Bus / Internal Communication Protocol** (**MDB / ICP**) released on October 4, 2002.

Of special note are the four major changes that were made to the specification:

- Added a second Cashless Device peripheral address in Section 7
- Replaced the Audit Unit with the Communications Gateway in Section 8
- Added the Coin Hopper or Tube – Dispenser in Section 10 (new)
- Assigned 2 addresses to be used for experimental peripherals

The following lists the primary revisions to the Version 3.0 of the **MDB / ICP.**

Section 1 – General Information

Section 1.3

- Changed the Level and Options chart for the Communications Gateway and the Coin Hopper or Tube – Dispenser

Section 2 – Communication Format

Section 2.2

- Added headers for the Response Codes
- Clarified non response processing for Master-to-Peripheral and Peripheral-to-Master communication.

Section 2.3

- Updated the Peripheral Address table for the Communications Gateway, Coin Hopper, Cashless Payment 1, and Experimental addresses
- Defined the use of the experimental addresses

Section 2.5

- Added new RESET examples F & G.

Petitioner Exhibit 1002-2730
CSC ServiceWorks – Ex. 1008
Page 6 of 270

Section 5 – Coin Acceptor / Changer

Section 5.2

- Renamed the STATUS command to SETUP command
- Added a new Possible Credited Coin Removal status code (0Dh)

Section 6 – Bill Validator

Section 6.2

- Renamed the STATUS command to SETUP command
- Added a new Possible Credited Bill Removal status code (0Ch)

Section 7 – Cashless Device(s) **(New Cashless Device #2)**

Changed name from Cashless Payment to Cashless Device

Section 7.1

- Added information regarding the dual addresses for two Cashless Device peripherals (10h and 60h)

Section 7.3

- Updated Command & Response table for dual addresses

Section 7.4

- Updated Command/Response Formats for dual addresses

Section 8 – Communications Gateway **(New Peripheral)**

Sections 8.1 through 8.6

- Replaced former Audit Unit sections with new Communications Gateway Sections

Section 9 –Universal Satellite Device (USDC)

Section 9.3

- Updated POLL table with proper number of bytes (FTL portion)
- Changed "numeric row and column" to "Item Number"

Section 10 – Coin Hopper or Tube – Dispenser **(New Peripheral)**

Sections 10.1 through 10.5

- Added complete new sections

Petitioner Exhibit 1002-2731
CSC ServiceWorks – Ex. 1008
Page 7 of 270

Version 2.0

Version 2.0 of this specification is the second release of the international **Multi-Drop Bus / Internal Communication Protocol** (**MDB / ICP**). This specification is the culmination of effort put forth by technical members of NAMA, the EVMMA, and the EVA. The basis for this specification is the Version 1.0 international **Multi-Drop Bus / Internal Communication Protocol** (**MDB / ICP**) released on October 14, 1998.

The following lists the primary revisions to the Version 2.0 of the **MDB / ICP**

Introduction

Foreword

- Clarified that the Standard is a communication interface

Section 1 - General Information

Section 1.1

- Added 3rd paragraph noting interface specification vs. system specification

Section 1.3

- Added entire Levels and Options section

Section 2 - Communication Format

Section 2.1

- Changed Mode Bit Master-to-Peripheral text

Section 2.2

- Removed "command" from Master-to-Peripheral 4th paragraph
- Changed RET description

Section 2.3

- Defined address 0000xxxB (00H) for VMC
- Provided address information to show hexadecimal format

Section 2.4

- Changed format to 2.4.X sub-sections and added 2.4.4 on Levels

Section 2.5

- Changed RET description

Section 2.6

- Added complete File Transport Layer Section

Section 3 - Bus Timing

Section 3.1

- Added 2nd sentence to t_{setup}

Section 4 - Hardware Specification

Section 4.3

- Modified complete section and added AMP as alternate source to Molex

Section 4.4

- Added pin numbers to schematic

Petitioner Exhibit 1002-2732
CSC ServiceWorks – Ex. 1008
Page 8 of 270

Section 5 - Coin Acceptor / Changer

Section 5.1

- Provided additional address information

Section 5.3

- Added recommended RESET command sequence
- Modified STATUS response to indicate Country / Currency Codes
- Modified County / Currency Code to include ISO 4217 (Appendix A1)
- Added Note 2 to DISPENSE (ODH) command
- Added FTL POLLed responses
- Added FTL "b3" option bit
- Added FTL expansion commands
- Cosmetic changes to all EXPANSION commands
- Split ALTERNATIVE PAYOUT (0FH-02H) and PAYOUT STATUS (0FH-03H) command into two separate commands (cosmetic change only)
- Added text to ALTERNATIVE PAYOUT (0FH-02H) Y1 description
- Added Note 3 to ALTERNATIVE PAYOUT STATUS (0FH-03H)

Section 5.5

- Added "**See Note 2 …**" text
- Added "If both peripherals supported" to Note

Section 6 - Bill Validator

Section 6.1

- Provided additional address information

Section 6.3

- Added recommended RESET command sequence
- Modified STATUS response to indicate Country / Currency Codes
- Modified County / Currency Code to include ISO 4217 (Appendix A1)
- Added Level 2 information
- Added Level 2 option bytes w/ new EXPANSION COMMANDs:
  - 37H 01H Level 2 Option Bit Enable
  - 37H 02H Level 2 Identification
- Added FTL POLLed responses
- Added FTL "b0" option bit
- Added FTL expansion commands
- Modified last sentence in SECURITY command to link to Z9-Z10 STATUS response
- Cosmetic changes to all EXPANSION commands

Section 6.5

- Added "If both peripherals supported" to Note

Petitioner Exhibit 1002-2738
CSC ServiceWorks – Ex. 1008
Page 9 of 270

Section 7 - Cashless Payment

Section 7.2 & 7.2.7

- Added Level 03 Negative Vend Request

Section 7.2.2

- Changed 1st sentence to link Setup to 7.4.1 information

Section 7.2.4

- Added Negative Vend and Revalue

Section 7.2.7

- Added Level 03 Negative Vend Request

Section 7.3

- Added bold text regarding defining currency at the beginning of a session
- Broke uninterruptable table into VMC Command and Reader Response
- Added Level 03 NEGATIVE VEND REQUEST to VMC Command table
- Added Level 03 DATA ENTRY REQUEST to Reader Response table
- Highlighted command out of sequence hard resets from VMC
- Moved Vend Failure Sequence to 7.4.8

Section 7.3 – Table 1

- Changed name to COMMANDS & RESPONSES
- Changed Comment column to VMC / Reader Level Support
- Linked all commands and responses to Levels
- Added DATA ENTRY REQUEST POLLed responses
- Added FTL POLLed responses
- Added FTL commands
- Added NEGATIVE VEND REQUEST responses
- Defined 14H-1AH and 20H-FEH as “For Future Use”

Section 7.4.1

- Cosmetically modified RESET command sequence
- Added 32 bit SETUP MAX/MIN PRICE
- Changed text following **Reader response**

Section 7.4.2

- Clarified Level 01 information (reader has no revalue capability)
- Added Level 03 information
- Modified SETUP response to indicate Country / Currency Codes
- Modified County / Currency Code to include ISO 4217 (Appendix A1)
- Added bold Note in Z3-Z4 County / Currency Code
- Added definition for Miscellaneous Options “b4 – b7”

Section 7.4.3

- Added Level 03 SETUP if Expanded Currency Mode

Section 7.4.4

- Added Level 03 BEGIN SESSION response if Expanded Currency Mode
- Added Level 03 VEND APPROVED response if Expanded Currency Mode
- Added Level 03 PERIPHERAL ID response if Expanded Currency Mode
- Clarified COMMAND OUT OF SEQUENCE definition

Petitioner Exhibit 1002-2734
CSC ServiceWorks – Ex. 1008
Page 10 of 270

- Added Level 03 REVALUE LIMIT AMOUNT response if Expanded Currency Mode
- Added Level 03 DATA ENTRY REQUEST response if Data Entry Mode
- Added Level 03 DATA ENTRY CANCEL response if Data Entry Mode
- Added Level 03 FTL REQ TO RCV response if FTL Mode
- Added Level 03 FTL RETRY / DENY response if FTL Mode
- Added Level 03 FTL SEND BLOCK response if FTL Mode
- Added Level 03 FTL OK TO SEND response if FTL Mode
- Added Level 03 FTL REQ TO SEND response if FTL Mode

Section 7.4.5

- Added Level 03 VEND command if Expanded Currency Mode
- Added Level 03 VEND APPROVED response if Expanded Currency Mode

Section 7.4.8

- Added Vend Failure (from 7.3)

Section 7.4.10

- Added Level 03 VEND command if Expanded Currency Mode

Section 7.4.11 (new)

- Added complete Level 03 NEGATIVE VEND Request section

Section 7.4.15 (new)

- Added complete Level 03 DATA ENTRY Request section

Section 7.4.16

- Added Level 03 REVALUE Request command if Expanded Currency Mode

Section 7.4.17

- Added Level 03 REVALUE Limit Request command if Expanded Currency Mode

Section 7.4.18

- Added Level 03 EXPANSION REQUEST ID response if Expanded Currency Mode

Section 7.4.22

- Added Level 03 EXPANSION ENABLE OPTIONS command

Section 7.4.23

- Added Level 03 FTL REQ TO RCV command & responses if FTL Mode

Section 7.4.24

- Added Level 03 FTL RETRY / DENY command if FTL Mode

Section 7.4.25

- Added Level 03 FTL SEND BLOCK command & response if FTL Mode

Section 7.4.26

- Added Level 03 FTL OK TO SEND command if FTL Mode

Section 7.4.27

- Added Level 03 FTL REQ TO SEND command & responses if FTL Mode

Section 7.7

- Added Example Vend Session #10 (Single Negative Vend)

Petitioner Exhibit 1002-2735
CSC ServiceWorks – Ex. 1008
Page 11 of 270

Section 8 - Audit Device

Section 8.1

- Provided additional address information

Section 8.3

- Added FTL POLLed responses
- Added FTL "b3" option bit
- Added FTL expansion commands

Section 9 - Universal Satellite Device

Section 9.1

- Provided additional address information

Section 9.3

- Added FTL POLLed responses
- Added FTL "b2" option bit
- Added FTL expansion commands

Document Revision History

- Deleted

Appendix 1 - Currency Codes

- Added entire section (based on **ISO 4217**)

Appendix 2 - Battery Operated Card Reader

- Added entire section

Version 1.0

Version 1.0 of this specification is the first release of the international **Multi-Drop Bus / Internal Communication Protocol** (**MDB / ICP**). This specification is the culmination of effort put forth by technical members of NAMA, the EVMMA, and the EVA. The basis for this specification is the **International Multi-Drop Bus Interface Standard** published by NAMA and the **Internal Communication Protocol** published by the EVMMA. The NAMA document was originally introduced on October 19, 1993 and later revised on August 19, 1994, June 20, 1997, and October 15, 1997. The EVMMA document was adopted in 1994 and later revised in 1995.

The following lists the primary revisions to the original two documents which were "combined" to create Version 1.0 of the **MDB / ICP**. In actuality, the NAMA **MDB** was the basis of the **MDB / ICP** with the exception of Section 7 which came from the EVMMA **ICP**. Besides typographical corrections and actual feature changes (below), the entire document was edited to provide a more uniform appearance.

The following lists the primary revisions to the Version 1.0 of the **MDB / ICP.**

Petitioner Exhibit 1002-2736
CSC ServiceWorks – Ex. 1008
Page 12 of 270

Hardware Specification - Section 4.3

- Added drawings of the MDB male and female connectors.

Coin Acceptor / Changer - Section 5.3

- Added Expansion commands:
  - 0F-05 Send Current Diagnostic Status
  - 0F-06 Send Controlled Manual Fill Report
  - 0F-07 Send Controlled Manual Payout Report

Coin Acceptor / Changer - Section 5.5

- Added coin acceptance and coin payout power requirements for coin changers using motorized payout mechanisms.
- Added note about simultaneously supplying bill validator transport power.

Bill Validator - Section 6.5

- Added note about simultaneously supplying coin mechanism coin acceptance power.

Cashless Payment - Section 7.2.6

- Added Level 02 Revalue capability.

Cashless Payment - Section 7.3

- Added Level 02 REVALUE REQUEST.
- Removed NAK (NCK) response from uninterruptable state and unexecutable command descriptions.
- Eliminated the BUSY response to vend failure sequences.
- Modified Table 1 per above.

Cashless Payment - Section 7.4.1

- Further defined the initializing sequence following a RESET command.

Cashless Payment - Section 7.4.2

- Further defined the Z7 Application Maximum Response Time.
- Added Z8 – b3 for supporting the VEND/CASH SALE subcommand.

Cashless Payment - Section 7.4.4

- Begin Session (03h) - Added Level 02 Reader Z4-Z10 data.
- Malfunction/Error (0Ah) - Added error code 1100 (refund error).
- Command Out of Sequence (0Bh) - Added Z2 data.
- Eliminated Busy (0Ch) response.
- Added Level 02 Reader Revalue Approved (0Dh) response.
- Added Level 02 Reader Revalue Denied (0Eh) response.
- Added Level 02 Reader Revalue Limit Amount (0Fh) response.
- Added Level 02 Reader User File Data (10h) response.

Petitioner Exhibit 1002-2737
CSC ServiceWorks – Ex. 1008
Page 13 of 270

- Added Level 02 Reader Time/Date Request (11h) response.

Cashless Payment - Section 7.4.10

- Added Level 01 Reader CASH SALE (13h/05h) VMC command.

Cashless Payment - Section 7.4.14

- Added Level 02 Reader Revalue - Request (15h/00h) VMC command.

Cashless Payment - Section 7.4.15

- Added Level 02 Reader Revalue – Limit Request (15h/01h) VMC command.

Cashless Payment - Section 7.4.17

- Obsoleted EXPANSION – Read User File (17h/01h) VMC command.

Cashless Payment - Section 7.4.18

- Obsoleted EXPANSION – Write User File (17h/02h) VMC command.

Cashless Payment - Section 7.4.19

- Added Level 02 Reader Write Time/Date File (17h/03h) VMC command.

Cashless Payment - Section 7.5

- Further defined the non-response time with the "Application Maximum Response Time" Z7.

Cashless Payment - Section 7.6 (original ICP Spec)

- Moved this section (ICP Payment Media Return Button) to Section 7.3.2.

Cashless Payment - Section 7.6 (MDB/ICP Spec)

- Previously was the ICP 7.7 with no modifications.

Petitioner Exhibit 1002-2738
CSC ServiceWorks – Ex. 1008
Page 14 of 270

(*this page intentionally left blank)*

Petitioner Exhibit 1002-2739
CSC ServiceWorks – Ex. 1008
Page 15 of 270

Introduction

Foreword

This voluntary Standard contains basic requirements for a vending machine communication interface within the limitations given below and in the General Information section of this Standard. These requirements are based on sound engineering principles, research, field experience, and an appreciation of the problems of manufacture, installation, and use derived from consultation with and information obtained from manufacturers, users, and others having specialized experience. These requirements are subject to revision as further experience and investigation may show it necessary or desired.

NAMA, in performing its functions in accordance with its objectives, does not assume or undertake to discharge any responsibility of the manufacturer or any other party. The opinions and findings of NAMA represent its professional judgment given with due consideration to the necessary limitations of practical operation and state of the art at the time the NAMA Standard is processed. NAMA shall not be responsible to anyone for use or reliance upon Standard by anyone. NAMA shall not incur any obligation or liability for damages, including consequential damages, arising out of or in connection with the use, interpretation of, reliance upon this Standard.

Standard Review

A complete review of this standard shall be conducted at least every five years to keep requirements consistent with technology. These reviews shall be conducted by representatives from industry and user groups on the NAMA Vending Technology Standards Committee at that time.

Petitioner Exhibit 1002-2740
CSC ServiceWorks – Ex. 1008
Page 16 of 270

(this page intentionally left blank)

Petitioner Exhibit 1002-2741
CSC ServiceWorks – Ex. 1008
Page 17 of 270

Section 1

General Information

1.1 Introduction

This document defines a serial bus interface for electronically controlled vending machines. The interface is a 9600 baud Master-Slave arrangement where all peripherals are Slaves to a Master controller.

The intent of this document is to standardize vending machines that employ electronic control (traditionally known as vending mechanism controller - VMC) so that all vending and peripheral equipment communicates identically.

It should be noted that this document is a vending machine interface / protocol specification and **not** a vending machine system specification. Each machine manufacturer should provide a specification on the overall operation of the machine.

1.2 Operational and Application Notes

The serial bus, or Multi-Drop Bus (MDB) is configured for Master-Slave operation. There is one Master with capability of communicating with up to thirty-two peripherals. The Master is defined as the Vending Machine Controller (VMC).

Each peripheral is assigned a unique address and command set. The master will "poll" the Bus for peripheral activity. That is, each peripheral is asked for activity, and responds with either an acknowledge, negative acknowledgment, or specific data dependent on its current activity. If a peripheral does not respond within a predefined time, (t-non-response as defined in the peripheral sections) it is assumed that it is not present on the Bus.

Bus interference, or "crashes" are prevented because each peripheral only responds upon being polled. Since there is only one master, and all communication is initiated by the Master, Bus "crashes" are easily precluded.

All peripherals will recognize a disable command, or commands, sent by the Master. This allows for disabling of individual peripherals for various reasons, for example, power management techniques.

Error checking and correction is accomplished by using checksums (CHK) and a retransmit command.

Petitioner Exhibit 1002-2742
CSC ServiceWorks – Ex. 1008
Page 18 of 270

1.3 Levels and Options

Since the introduction of the earliest Multi-Drop Bus specification, functional levels and operational options have been established for most of the peripherals on the MDB/ICP interface. These have provided the capability for new features to be implemented as new requirements and features were needed for the international vending industry.

1.3.1 Levels

Levels of peripheral functionality were established when a major change occurred in the peripheral that added extended commands and responses. Due to potential conflicts between a VMC level and a peripheral level, neither the VMC nor the peripheral should issue a command or reply with a response that is not supported by the other device.

The VMC must initially determine (via the appropriate STATUS or SETUP command) the level of a peripheral before determining which commands it can issue to that device. **A VMC must only send commands that are supported by the peripheral.** For example, a Level 3 command may only be issued to a Level 3 or higher peripheral and must not be issued to a Level 1 or 2 peripheral.

The Cashless Payment and the Universal Satellite Device can also learn the respective level of the VMC for that device. This information is sent via the SETUP command. **It is the responsibility of the peripheral to only send responses that are supported by the VMC.** For example, a Level 3 response may only be sent to a Level 3 or higher VMC and must not be sent to a Level 1 or 2 VMC. Effectively, the VMC and peripheral should support the highest common level.

For total compatibility, VMCs and peripherals should support all lower levels. **For new designs after July 2000, it is strongly recommended that VMCs and peripherals must support all lower levels.** Commercial or regional issues may cause machine or peripheral manufacturers to implement only specific levels; however, this is a decision (and risk) made by the machine or peripheral manufacturer.

1.3.2 Options

Options were established in the peripherals to provide various additional operational features that may be required for specific vending applications. As the name implies, these features are “above and beyond” the standard core of required functionality.

At power on and after a Bus Reset or a RESET command, all options are disabled. During the initialization command sequences, the VMC determines the optional features supported by the peripherals. The VMC will then enable the features it is going to use. Until the feature is enabled, it is the responsibility of the peripheral to ignore feature specific commands and not respond with feature specific responses.

Petitioner Exhibit 1002-2748
CSC ServiceWorks – Ex. 1008
Page 19 of 270

1.3.3 Currently Established Levels and Options

The following table provides a brief description of each of the currently established levels and options of the various MDB/ICP peripherals. Please refer to the specific sections for each device for more detailed information.

Peripherals	Levels	Options	Description
Coin Changer	1	n/a	Never released
	2	none	Supports standard commands
	3	below	Supports Expansion ID command and optionally supports commands for features below
		b0	Alternative Payout Method
		b1	Extended Diagnostics
		b2	Controlled Manual Fill and Payout
		b3	File Transport Layer (FTL)
Bill Validator	1	none	Supports standard commands and Expansion ID command without options
	2	below	Supports expansion ID command with options and optionally supports commands for features below
		b0	File Transport Layer (FTL)
Cashless Device #1 & #2	1	below	Supports standard commands and Expansion ID command. Readers do not have revaluation capability
		b0*	Reader is capable of restoring funds to card
		b1*	Reader is multivend capable
		b2*	Reader has a display available
		b3*	Reader supports VEND-CASH SALE command
			*bits in the SETUP-Config command
	2	above	Supports Revalue, Time/Date, Read User File (obsolete), and Write User File (obsolete) commands

Petitioner Exhibit 1002-2744
CSC ServiceWorks – Ex. 1008
Page 20 of 270

Peripherals	Levels	Options	Description
Cashless Device #1 & #2 (continued)	3	above & below	Supports expansion ID command with options and optionally supports commands for features below (bits in the Level 3 Expansion ID command)
		b0**	File Transport Layer (FTL)
		b1**	16 or 32 Bit Monetary Format
		b2**	Multi Currency / Multi Lingual
		b3**	Negative Vend
		b4**	Data Entry
			**bits in the Level 3 Expansion ID command
Communications Gateway	1	none	Obsolete (former Audit Unit)
	2	none	Obsolete (former Audit Unit)
	3	below	Supports Expansion ID command and optionally supports commands for features below
		b0	File Transport Layer (FTL)
		b1	Verbose Mode
Universal Satellite Device (USD)	1	below	Supports all basic commands and optionally supports commands for features below
		b0	USD is capable of storing and controlling pricing
		b1	USD is capable of selecting items to vend
		b2	File Transport Layer (FTL)
Coin Hopper or Tube - Dispenser	1	below	Supports Expansion ID command and optionally supports commands for features below
		b0	File Transport Layer (FTL)

Petitioner Exhibit 1002-2745
CSC ServiceWorks – Ex. 1008
Page 21 of 270

Section 2

Communication Format

2.1 Byte Format

Baud Rate: 9600 NRZ

Serial Bit Format:
1 Start Bit
8 Data Bits
1 Mode Bit
1 Stop Bit

11 Bits Total

LSB										MSB
Start	0	1	2	3	4	5	6	7	Mode	Stop

Mode Bit: Master-to-Peripheral

The mode bit differentiates between ADDRESS bytes and DATA bytes. ADDRESS bytes must be read by all peripherals, DATA bytes are only read by the peripheral that has been addressed.

The mode bit is set (logic one) to indicate an ADDRESS byte, and not set (logic zero) to indicate a DATA byte.

Mode Bit: Peripheral-to-Master

The mode bit must be set on the last byte sent when data is sent from a Slave to the Master.

Petitioner Exhibit 1002-2746
CSC ServiceWorks – Ex. 1008
Page 22 of 270

2.2 Block Format

Master-to-Peripheral

A Communication Block for Master-to-Slave transmissions is defined as an Address byte, optional data bytes, and a CHK byte. A block is limited to a maximum of thirty-six (36) bytes.

The upper five bits (MSB) of the Address Byte will be used for addressing. That is, bits 7,6,5,4,3 of the previous byte description will be used for addressing.

The lower three bits (i.e. 2,1,0) of the Address Byte will contain peripheral specific commands. This will allow up to eight instructions to be embedded in the first byte of a block.

The VMC Master will respond to data from a peripheral with an Acknowledgment (ACK), Negative Acknowledgment (NAK), or Retransmit (RET). These are defined later in the document. The 5 mS time-out (t-response) described in the Bus Timing section of this document is the equivalent of a NAK.

If the addressed Slave does not respond within the 5 mS time-out (silence), the Master may repeat the same command, or send a different command, until it receives an answer or until the end of the Non-Response time, as defined in the peripheral sections. See Example in 2.5D. The RESET command should not be used as a recovery method to a 5 mS time-out (t-response) until after exceeding the Non-response time. The VMC may send commands to any other peripheral during this time.

Peripheral-to-Master

A Communication Block for Slave-to-Master transmissions consists of either a data block and a CHK byte, a acknowledgment (ACK), or a negative acknowledgment (NAK).

The 5 mS time-out (t-response) described in the Bus Timing section of this document is the equivalent of a NAK command. In addition, it is recommended that the peripheral use this time-out as the NAK when a reception error of the ADDRESS byte occurs. This will prevent several peripherals from trying to simultaneously respond with a NAK.

A data block consists of one or more data bytes followed by a CHK byte. The CHK byte is defined later in this document.

The data block and CHK byte are limited to a maximum size of 36 bytes.

A CHK byte is not required when a peripheral responds with NAK or ACK byte. ACK and NAK are defined later in this document.

Petitioner Exhibit 1002-2747
CSC ServiceWorks – Ex. 1008
Page 23 of 270

The peripheral must set the mode bit on the last byte sent to signify end of transmission. This will be either the CHK byte of a block, a NAK byte, or an ACK byte. The mode bit must not be set except for the conditions above.

A peripheral response of ACK or NAK signifies the end of the exchange.

When a peripheral responds with a data block, the VMC must respond with an ACK, NAK or RET. If the Master cannot respond within the 5 mS time-out (t-response) the peripheral must repeat the data block, or append it, at the next possible occasion (i.e. to a later POLL). The same behavior is to apply when the Master responds with NAK.

CHK Byte

A CHK byte must be sent at the end of each block of data. The CHK byte is a checksum calculated by adding the ADDRESS byte and all DATA bytes. The CHK byte is not included in the summation. The carry bit for CHK additions is ignored since the CHK byte is limited to eight bits.

The following example shows a CHK byte calculation for a possible response to a STATUS command sent to a USA changer slave. See section 5 for details of byte meanings.

02H	Changer feature level
00H	Country code for USA
01H	Country code for USA
05H	Coin scaling factor
02H	Decimal place
00H	Coin type routing
07H	Coin type routing
01H	Coin type 0 has value of 1 scaling factor
02H	Coin type 1 has value of 2 scaling factor
05H	Coin type 2 has value of 5 scaling factor
14H	Coin type 3 has value of 20 scaling factor
FFH	Coin type 4 is a token
12CH	Therefore the CHK byte would be equal to 2CH

A checksum will be performed on all full blocks of communication. A checksum will not be performed on ACK, NAK, or RET bytes.

Petitioner Exhibit 1002-2748
CSC ServiceWorks – Ex. 1008
Page 24 of 270

Response Codes

The following codes are reserved for the ACK, NAK and RET bytes:

ACK	00H	(acknowledgment/checksum correct)
RET	AAH	(Retransmit the previously sent data. **Only the VMC can transmit this byte**)
NAK	FFH	(Negative acknowledge)
		The VMC and peripheral must also recognize the 5 mS time-out (t-response) as a NAK.

NOTE: To improve system reliability it is recommended that when receiving ACK, NAK, or RET the receiving device counts the number of bits set in the byte. This method will require at least two bit errors in the byte before the byte can be mis-interpreted.

Bus Reset

The VMC may reset all peripherals by pulling the transmit line "active" for a minimum of 100 mS. This informs all peripherals to abort any activity and return to its power-on reset state. Details of this state for each peripheral are provided in later sections of this document. It is recommended that the VMC re-initialize each peripheral after this type of reset.

Petitioner Exhibit 1002-2749
CSC ServiceWorks – Ex. 1008
Page 25 of 270

2.3 Peripheral Addresses

The addresses below are defined. Note again that the bits shown are the upper five bits (7,6,5,4,3) of the Address Byte and will be used for all addressing including the File Transport Layer described in Section 2.6. The lower three bits (2,1,0) are used for the command.

Address		Definition
00000xxxB	(00H)	Reserved for VMC
00001xxxB	(08H)	Changer
00010xxxB	(10H)	Cashless Device #1
00011xxxB	(18H)	Communications Gateway
00100xxxB	(20H)	Display
00101xxxB	(28H)	Energy Management System
00110xxxB	(30H)	Bill Validator
00111xxxB	(38H)	Reserved for Future Standard Peripheral
01000xxxB	(40H)	Universal Satellite Device #1
01001xxxB	(48H)	Universal Satellite Device #2
01010xxxB	(50H)	Universal Satellite Device #3
01011xxxB	(58H)	Coin Hopper or Tube - Dispenser
01100xxxB	(60H)	Cashless Device #2
01101xxxB	(68H)	Reserved for Future Standard Peripherals
.	.	.
.	.	.
.	.	.
11011xxxB	(D8H)	Reserved for Future Standard Peripherals
11100xxxB	(E0H)	Experimental Peripheral #1
11101xxxB	(E8H)	Experimental Peripheral #2
11110xxxB	(F0H)	Vending Machine Specific Peripheral #1
11111xxxB	(F8H)	Vending Machine Specific Peripheral #2

Petitioner Exhibit 1002-2750
CSC ServiceWorks – Ex. 1008
Page 26 of 270

Experimental Peripheral Addresses

Experimental Peripheral addresses 11100xxxB (E0H) and 11101xxxB (E8H) are reserved for use by manufacturers when designing and field testing potential new MDB/ICP devices. These addresses are **temporary** and once the new device is approved by NAMA and the EVA, the device will be assigned a different permanent peripheral address. Use of the Experimental Peripheral addresses shall be limited to "in house" testing and "closed site" field trials. Manufacturers must understand that any devices in the field with Experimental Peripheral addresses must be recalled or updated to the permanent address if the device is approved by NAMA and the EVA. If not approved by NAMA and the EVA, the devices must be recalled or have their addresses changed to the Vending Machine Specific peripheral addresses described below.

Vending Machine Specific Peripheral Addresses

Vending Machine Specific peripheral addresses (addresses 11110xxxB (F0H) and 11111xxxB (F8H)) are reserved for Non-Standard or proprietary applications. These devices are allowed a unique set of commands.

All other peripherals are defined as Standard devices. These peripherals must follow the specifications to ensure compatibility between manufacturers.

Petitioner Exhibit 1002-2751
CSC ServiceWorks – Ex. 1008
Page 27 of 270

2.4 Software Operational Rules

2.4.1 Power Budget

The VMC must regulate the power budget. That is, peripherals must be enabled and disabled dependent on power availability. The power bus is defined later in this document.

2.4.2 Bytes

During multi-byte messages the most significant byte is sent first.

> Any bytes within a command or response that are not specifically defined should be left in a 0 state. For Level 03 or lower coin mechanisms, Level 01 bill validators, and Level 01 card readers, this is not a requirement but a suggestion.

2.4.3 Polling

The following are recommendations for the methods of VMC to peripheral software operation.

> Each peripheral should be polled every 25-200 milliseconds. This can be done by the POLL command or any other appropriate command.
>
> If a peripheral has not responded to a poll for its maximum Non-Response time, the VMC should continue to poll the peripheral at least every ten seconds with a RESET command. (See Example G in Section 2.5).

2.4.4 Levels

Due to potential conflicts between a VMC level and a peripheral level, neither the VMC nor the peripheral should issue a command or reply with a response that is not supported by the other device.

The VMC must initially determine (via the appropriate STATUS or SETUP command) the level of a peripheral before determining which commands it can issue to that device. **A VMC must only send commands that are supported by the peripheral.** For example, a Level 3 command may only be issued to a Level 3 or higher peripheral and must not be issued to a Level 1 or 2 peripheral.

The Cashless Payment and the Universal Satellite Device can also learn the respective level of the VMC for that device. This information is sent via the SETUP command. **It is the responsibility of the peripheral to only send responses that are supported by the VMC.** For example, a Level 3 response may only be sent to a Level 3 or higher

Petitioner Exhibit 1002-2752
CSC ServiceWorks – Ex. 1008
Page 28 of 270

VMC and must not be sent to a Level 1 or 2 VMC. Effectively, the VMC and peripheral should support the highest common level.

For total compatibility, VMCs and peripherals should support all lower levels. **For new designs after July 2000, it is strongly recommended that VMCs and peripherals must support all lower levels.** Commercial or regional issues may cause machine or peripheral manufacturers to implement only specific levels; however, this is a decision (and risk) made by the machine or peripheral manufacturer.

2.5 Typical Session Examples

A. The diagram below represents a typical transmission when a peripheral is idle.

VMC:

ADD* CHK

Peripheral:

ACK*

B. The diagram below represents a typical transmission when a peripheral has data to return.

VMC:

ADD* CHK ACK

Peripheral:

DAT DAT CHK*

C. The diagram below represents a typical transmission when the VMC has data to send.

VMC:

ADD* DAT DAT CHK

Peripheral:

ACK*

*Indicates mode bit set

Petitioner Exhibit 1002-2758
CSC ServiceWorks – Ex. 1008
Page 29 of 270

D. The diagram below represents a typical transmission when the VMC determines a CHK is not correct. The VMC will respond one of two ways:

Send a NAK to the peripheral to indicate that the information was not received correctly then perform other tasks. Note: When the Master answers with NAK (or silence which is treated equally) the slave has to repeat the response, in order to ensure the execution of the response (i.e. coin reception etc.).

OR

The VMC may send a retransmit (RET) command alerting the peripheral to retransmit the previously sent data.

VMC:

ADD* DAT CHK RET ACK

Peripheral:

DAT DAT CHK* DAT DAT CHK*

*Indicates mode bit set.

E. This diagram represents a situation where the peripheral does not respond within the 5 mS time-out (t-response).

VMC:

ADD* CHK ADD* CHK

Peripheral:

[silence…] ACK*

Petitioner Exhibit 1002-2754
CSC ServiceWorks – Ex. 1008
Page 30 of 270

F. This diagram represents a situation where the peripheral does not respond to a command and after its maximum Non-Response time, is reset by the controller.

Controller		Peripheral	Comment
Command X	→		
	←	Response	Normal response
Command Y	→		
	←	[silence…]	No response
Command Y	→		
	←	[silence…]	No response
Command Y	→		
	←	[silence…]	No response
			Peripheral does not response within its allocated Non-Response Time.
RESET	→		Software Reset
	←	[silence…]	Peripheral in initialization routine
RESET	→		
	←	ACK	Peripheral operational again
POLL	→		
	←	JUST RESET	Peripheral indicates finished RESET processing
ACK	→		
			Peripheral initialization sequence is performed as recommended in each peripheral section.

Petitioner Exhibit 1002-2755
CSC ServiceWorks – Ex. 1008
Page 31 of 270

G. This diagram represents a situation where the peripheral is disconnected or goes offline. The controller should send a RESET command every 10 seconds to determine if, and when, the peripheral becomes active again.

Controller		Peripheral	Comment
Command X	→		
	←	Response	Normal response
Command Y	→		
	←	[silence…]	No response
Command Y	→		
	←	[silence…]	No response
Command Y	→		
	←	[silence…]	No response
			Peripheral does not response within its allocated Non-Response Time.
RESET	→		Software Reset
	←	[silence…]	Peripheral offline
RESET	→		Software Reset
	←	[silence…]	Peripheral offline
			Wait 10 seconds
RESET	→		
	←	[silence…]	Peripheral offline
			Wait 10 seconds
RESET	→		
		[silence…]	Peripheral offline
			Wait 10 seconds
RESET	→		
		[silence…]	Peripheral offline

Petitioner Exhibit 1002-2756
CSC ServiceWorks – Ex. 1008
Page 32 of 270

2.6 File Transport Layer

The **F**ile **T**ransport **L**ayer (**FTL**) provides a method to send and/or receive high level information between peripherals or between a peripheral and the VMC. It is **not** intended to be used for standard vending credit and control functions. An example would be loading new validation parameters into a coin changer or bill validator.

Since the MDB/ICP interface is "driven" by the VMC, it has to be a network manager for all FTL data transfers. It acts as a temporary mailbox and data switch for FTL blocks; however, the information that is sent via FTL does not have to be interpreted by the VMC. The VMC simply uses the destination and source address information provided in the MDB/ICP command and response structure to forward the data to the proper recipient.

2.6.1 FTL Process Overview

If a peripheral needs to transfer data to another peripheral (or the VMC):
- The VMC must poll the peripheral,
- The peripheral must answer with a "REQUEST TO SEND",
- The VMC must get approval to forward data (if necessary),
- The VMC requests the first data block,
- The VMC ACKs the first block and forwards to destination,
- The process repeats until all blocks are sent.

If the VMC needs to transfer data to a peripheral:
- The VMC must send a "REQUEST TO SEND",
- The peripheral approves or denies the transfer request,
- If approved, the VMC sends the first data block,
- The peripheral ACKs the first data block,
- The process repeats until all blocks are sent.

If a peripheral (A) needs to request a transfer of data from another peripheral (B):
- The VMC must poll the peripheral A,
- Peripheral A must send a "REQUEST TO RECEIVE",
- The VMC forwards the request to peripheral B,
- Peripheral B decides to honor the request or not,
- If approved, peripheral B sends the first data block,
- The VMC forwards the data block to peripheral A,
- The process repeats until all blocks are sent.

2.6.2 FTL Detailed VMC Operation

Petitioner Exhibit 1002-2757
CSC ServiceWorks – Ex. 1008
Page 33 of 270

The VMC must act as a network manager, it is responsible for checking peripheral status and managing network resources as described below, it must:

- Be aware of which peripherals are active and support the FTL. If a file transfer is requested involving a peripheral that does not support it, the VMC should deny the transfer using RETRY/DENY defined later.
- Poll peripherals to become aware that a data transfer is requested.
- Read data blocks from selected peripherals.
- If VMC receives a NAK, it should attempt to finish current command/response up to 5 times. After that, it should abort file transfer as defined by the protocol.
- Send data blocks to destination device, if not the VMC itself.
- Repeat these steps for all data blocks, as needed.

2.6.3 FTL General Operation

- The FTL "session" would transfer a "file" using several "blocks". The "Dest" and "Src" are switched by the VMC directing each block to its destination.
- All responses can be sent immediately after receipt of command or the command can be ACK'ed and the response sent in a delayed fashion (meeting all appropriate time-outs). However, FTL responses must NOT be combined with responses to any other commands, at any time.
- File transfers less than 256 blocks are terminated by sending an empty data file (SEND BLOCK with no data). File transfers of exactly 256 blocks are terminated by block #FE followed by block #FF.
- It is recommended that files larger than one block:
  1) Include a CRC in their data. The transport layer is not responsible for checking for correct CRCs.
  2) Include a time out mechanism to prevent system dead locks. The transport layer is **not** responsible for checking for dead locked file transfers.
- To prevent a system dead lock, the VMC must poll other peripherals during all data transfers and service them accordingly.
- Since the VMC is not knowledgeable about the contents of the file transfer it should not disable any peripherals due to a transfer request. This will be the responsibility of the peripherals themselves. They may internally disable and report so to the VMC if possible, or they may just stop responding to the VMC until ready. The latter may cause the VMC to try to reset the peripheral.

2.6.4 FTL Command and Response Sets For All Components

The table below defines the VMC commands and peripheral responses that occur during an FTL data transfer. Note that the peripheral responses can either be immediate to the VMC's command or delayed and provided to a subsequent POLL. Definitions are provided on the following page.

Petitioner Exhibit 1002-2758
CSC ServiceWorks – Ex. 1008
Page 34 of 270

Command / Response	VMC Cmd[1]	Resp	Source Data (bytes)	Destination Response
REQ TO SEND	α7/FE	1F	Dest (1) Src (1) File ID (1) Length (1) Control (1)	OK TO SEND or RETRY/DENY
OK TO SEND	α7/FD	1E	Dest (1) Src (1)	SEND BLOCK (repeated until whole file is transferred)
SEND BLOCK	α7/FC	1D	Dest (1) Block # (1) Data (1 to 31)	ACK
RETRY/DENY	α7/FB	1C	Dest (1) Src (1) Retry delay (1)	ACK
REQ TO RCV	α7/FA	1B	Dest (1) Src (1) File ID (1) Max Length (1) Control (1)	SEND BLOCK (repeated until whole file is transferred) or RETRY/DENY

Note 1: The α7 represents the address of the destination device (defined in Section 2.3) logically OR'd with a hexadecimal 0x07.

Petitioner Exhibit 1002-2759
CSC ServiceWorks – Ex. 1008
Page 35 of 270

Dest **1 byte**

The destination address of the peripheral where the data block (**not the whole file**) is being sent to. All addresses refer to the standard MDB defined peripheral addresses as defined in Section 2.3. Note that 00000xxx (00H) will be used for the VMC. Examples are a changer (08H), audit system (18H), bill validator (30H), and universal satellite device #2 (48H).

Src **1 byte**

The source address of the peripheral where the data block (**not the whole file**) is being sent from. All addresses refer to the standard MDB defined peripheral addresses as defined in Section 2.3. Note that 00000xxx (00H) will be used for the VMC. Examples are the same as in the **Dest** above.

File ID **1 byte**

The type of information desired. NAMA will maintain a list of standard file ID's and a definition of what each file type means. Note that if a device responds with a "Retry delay" of FFH it should be interpreted that this device does not support the requested function.

Currently defined file IDs include:

00H: Manufacture ID information. This file must start with the manufactures three character manufactures code, anything after that would be up to the manufacture to define.

01H: DTS defined file. This file must follow the format defined in the EVA-DTS standard. This would include the DXS record as well as all data up to and including the DXE record.

0FH to 0FFH: This range of files may be used for Manufacturer Specific information. The content and format of these files are left up to the manufacturer to define.

Additional ID proposals must be evaluated by the NAMA MDB/ICP technical standard committee.

(Max) Length **1 byte**

The total number of blocks that will (can) be included in the entire file. This byte should be used as a counter to determine the amount of data blocks to be transferred.

Petitioner Exhibit 1002-2760
CSC ServiceWorks – Ex. 1008
Page 36 of 270

Control **1 byte**

This byte contains information that can be used by the VMC and peripherals to determine how the data transfer is conducted. Included controls are:

b0: Reset after transfer. The receiving peripheral should reset itself after the file transfer is complete.
b1: End of File. The last block of the current FTL session contains the end of this file. If clear (=0), then another FTL session will follow with additional blocks. If set (=1), then this is the last (or only) FTL session to be sent.
b2 - b7: Not used, must be set to 0

Block # **1 byte**

The sequential number of this block, within the total file, that is being requested/sent. All data blocks must be identified by a block number, counting up from 0 (first block) to 255.

Data Block **1 to 31 byte(s)**

The actual data portion of the block. All data must fit into a 31 byte, or less, string. The standard MDB CHK byte will signify the end of block. (Peripherals will have to use inter-byte time out when receiving blocks from the VMC.) Knowledge of the contents of this data is only required by the source and destination devices.

Retry Delay **1 byte**

A time delay that the sender should wait before trying to re-send the entire data file again. If a device is not capable of receiving a file in its current state, this byte should represent the number of seconds before it will be ready to receive the data. If the device simply refuses to accept the file it must answer with a “Retry Never” signified by a 00H retry delay. If the device is not present, block synchronization is lost, or other failure mode arises a “Retry Never” should be used to abort/deny the current file transfer.

Petitioner Exhibit 1002-2761
CSC ServiceWorks – Ex. 1008
Page 37 of 270

File Transport Layer Examples

Below are examples of data transfers between the VMC and a peripheral or between two different peripherals via the VMC.

SUCCESSFUL TRANSFER – VMC TO PERIPHERAL A			
Peripheral A	**VMC**	**Peripheral B**	**Comments**
	← REQ TO SEND (α7/FE)		Request to send "n" blocks
OK TO SEND (1E)	→		
	← ACK		
	← SEND BLOCK (α7/FC)		Repeated "n" times
ACK	→		

DENIED TRANSFER – VMC TO PERIPHERAL A			
Peripheral A	**VMC**	**Peripheral B**	**Comments**
	← REQ TO SEND (α7/FE)		
RETRY/00 (1C)	→		Denied
	← ACK		

SUCCESSFUL REQUEST – VMC TO PERIPHERAL A			
Peripheral A	**VMC**	**Peripheral B**	**Comments**
	← POLL (varies)		
REQ TO RCV (1B)	→		Request receive "n" blocks
	← ACK		
	← SEND BLOCK (α7/FC)		Repeated "n" times
ACK	→		

DENIED REQUEST – VMC TO PERIPHERAL A			
Peripheral A	**VMC**	**Peripheral B**	**Comments**
	← POLL (varies)		
REQ TO RCV (1B)	→		Request receive "n" blocks
	← ACK		
	← RETRY/00 (α7/FB)		Denied
ACK	→		

Petitioner Exhibit 1002-2762
CSC ServiceWorks – Ex. 1008
Page 38 of 270

VMC ABORTED TRANSFER – VMC TO PERIPHERAL A

Peripheral A		VMC	Peripheral B	Comments
	←	REQ TO SEND (α7/FE)		Request to send "n" blocks
OK TO SEND (1E)	→			
	←	ACK		
	←	SEND BLOCK (α7/FC)		Repeated "n" times
ACK	→			
	←	RETRY/00 (α7/FB)		Aborted!
ACK	→			

PERIPHERAL ABORT TRANSFER – VMC TO PERIPHERAL A

Peripheral A		VMC	Peripheral B	Comments
	←	REQ TO SEND (α7/FE)		Request to send "n" blocks
OK TO SEND (1E)	→			
	←	ACK		
	←	SEND BLOCK (α7/FC)		
RETRY/00 (1C)	→			Aborted!
	←	ACK		

SUCCESSFUL TRANSFER – PERIPHERAL A TO VMC

Peripheral A		VMC	Peripheral B	Comments
	←	POLL (varies)		
REQ TO SEND (1F)	→			Request to send "n" blocks
	←	ACK		
	←	OK TO SEND (α7/FD)		
SEND BLOCK (1D)	→			Repeated "n" times
	←	ACK		

Petitioner Exhibit 1002-2768
CSC ServiceWorks – Ex. 1008
Page 39 of 270

DENIED TRANSFER – PERIPHERAL A TO VMC

Peripheral A	VMC	Peripheral B	Comments
	← POLL (varies)		Request to send "n" blocks
REQ TO SEND (1F)	→		
	← ACK		
	← RETRY/00 (α7/FB)		Denied
ACK	→		

SUCCESSFUL TRANSFER – PERIPHERAL A TO PERIPHERAL B

Peripheral A	VMC	Peripheral B	Comments
	← POLL (varies)		
REQ TO SEND (1F)	→		Request to send "n" blocks
	← ACK		
	REQ TO SEND (1F) (α7/FE) →		
		← OK TO SEND (1E)	
	ACK →		
	← OK TO SEND (α7/FD)		
SEND BLOCK (1D)	→		Repeated "n" times
	← ACK		
	SEND BLOCK (α7/FC) →		
		← ACK	

DENIED TRANSFER – PERIPHERAL A TO PERIPHERAL B

Peripheral A	VMC	Peripheral B	Comments
	← POLL (varies)		
REQ TO SEND (1F)	→		Request to send "n" blocks
	← ACK		
	REQ TO SEND (1F) (α7/FE) →		
		← RETRY/00 (1C)	Denied
	ACK →		
	← RETRY/00 (α7/FB)		
ACK	→		

Petitioner Exhibit 1002-2764 CSC ServiceWorks – Ex. 1008
Page 40 of 270

SUCCESSFUL REQUEST - PERIPHERAL A TO PERIPHERAL B

Peripheral A	VMC	Peripheral B	Comments
	← POLL (varies)		
REQ TO RCV (1B)	→		Request receive "n" blocks
	← ACK		
	REQ TO RCV (α7/FA) →		
		← SEND BLOCK (1D)	Repeated "n" times
	ACK →		
	← SEND BLOCK (α7/FC)		
ACK	→		

DENIED REQUEST – PERIPHERAL A TO PERIPHERAL B

Peripheral A	VMC	Peripheral B	Comments
	← POLL (varies)		
REQ TO RCV (1B)	→		Request receive "n" blocks
	← ACK		
	REQ TO RCV (α7/FA) →		
		← RETRY/00 (1C)	Denied
	ACK →		
	← RETRY/00 (α7/FB)		
ACK	→		

Petitioner Exhibit 1002-2765
CSC ServiceWorks – Ex. 1008
Page 41 of 270

PERIPHERAL A TRANSFER TO PERIPHERAL B – ABORTED BY A

Peripheral A	VMC	Peripheral B	Comments
	← POLL (varies)		
REQ TO SEND (1F)	→		Request to send "n" blocks
	← ACK		
	REQ TO SEND (α7/FE) →		
		← OK TO SEND (1E)	
	ACK →		
	← OK TO SEND (α7/FD)		
SEND BLOCK (1D)	→		
	← ACK		
	SEND BLOCK (α7/FC) →		
		← ACK	
	. . .		Repeated "n" times
	← POLL (varies)		
RETRY/00 (1C)	→		Aborted!
	← ACK		
	RETRY/00 (α7/FB) →		
		← ACK	

Petitioner Exhibit 1002-2766
CSC ServiceWorks – Ex. 1008
Page 42 of 270

PERIPHERAL A TRANSFER TO PERIPHERAL B – ABORTED BY B

Peripheral A	VMC	Peripheral B	Comments
	← POLL (varies)		
REQ TO SEND (1F)	→		Request to send "n" blocks
	← ACK		
	REQ TO SEND (α7/FE) →		
		← OK TO SEND (1E)	
	ACK →		
	← OK TO SEND (α7/FD)		
SEND BLOCK (1D)	→		
	← ACK		
	SEND BLOCK (α7/FC) →		
		← ACK	
	. . .		Repeated "n" times
	← POLL (varies)REQ BLOCK (α7/FD)		
SEND BLOCK (1D)	→		
	← ACK		
	SEND BLOCK (α7/FC) →		
		← RETRY/00 (1C)	Aborted!
	ACK →		
	← RETRY/00 (α7/FB)		
ACK	→		

Petitioner Exhibit 1002-2767
CSC ServiceWorks – Ex. 1008
Page 43 of 270

Section 3

Bus Timing

3.1 Timing Definitions

Baud rate	=	The rate of bit transfer per second.
t inter-byte (max.)	=	The maximum time allowed between bytes in a block transmission.
t response (max.)	=	The maximum time any device, master or peripheral, will take to respond to a valid communication.
t break (VMC)	=	The minimum time of the Bus Reset signal sent by the VMC to reset all peripherals.
t setup	=	The minimum set-up time before the VMC attempts to communicate after a reset signal. Peripheral devices may choose to not respond for up to the non-response time defined in each peripheral section.

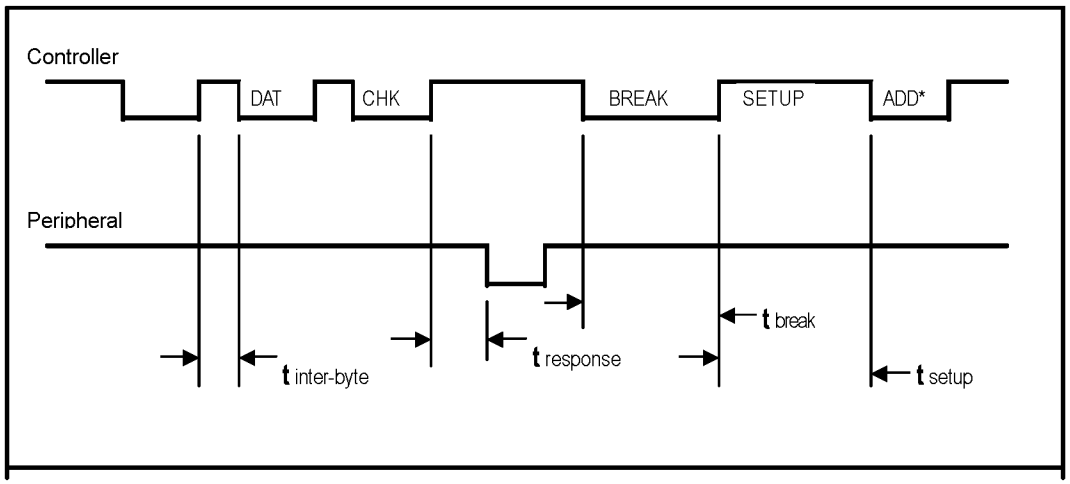
3.2 Timing Specifications

Baud Rate	=	9600 +1%/-2% NRZ
t inter-byte (max.)	=	1.0 mS
t response (max.)	=	5.0 mS
t break (min.)	=	100 mS
t setup (min.)	=	200 mS

Petitioner Exhibit 1002-2768
CSC ServiceWorks – Ex. 1008
Page 44 of 270

NOTE: All peripherals have the option of not responding to the VMC. Non-response timing is defined in the peripheral specification.

3.3 Timing Diagram



NOTE: * indicates that the mode bit is set

Petitioner Exhibit 1002-2769
CSC ServiceWorks – Ex. 1008
Page 45 of 270

Section 4

Hardware Specification

4.1 Bus Power Supply Definition

The information below defines the minimum VMC voltage output. The actual current ratings per peripheral will be defined in their respective sections.

Power supply filtering is optional, therefore if a peripheral requires more power, or tighter regulation, they may elect to supply their own power, or filtering, from available sources elsewhere in the machine.

VMC Voltage Output:

Minimum	=	20 VDC rms.(rectified and optionally filtered)
Nominal	=	34 VDC unreg.(rectified and filtered) 24 VDC rms.(rectified only)
Maximum	=	42.5* VDC(ripple voltage upper limit) * High line input may allow 45 VDC peak (max.).

4.2 Bus Transmitter / Receiver Specification

The following section describes the 5V, optically isolated, current loop system between the Master and the Slave.

VMC Master:

Transmit:

Minimum source current (active):	100 mA @ 4V
Maximum leakage current (inactive):	100 uA

NOTES: 1) The transmit line must be able to withstand a short while in the active mode.

2) 15 mA should be added for each peripheral over six.

Petitioner Exhibit 1002-2770
CSC ServiceWorks – Ex. 1008
Page 46 of 270

Receive:

Minimum input current (active):	15 mA @ 1V
Maximum input current (inactive):	1 mA

Peripheral Slave:

Receive:

Maximum input current (active):	15 mA @ 4V
Maximum input current (inactive):	100 uA

Transmit:

Minimum sink current (active):	15 mA @ 1V
Maximum leakage current (inactive):	30 uA

4.3 Connector Specification

Connector assemblies supplied by the NAMA approved suppliers, noted in Section 4.3.6, are intermateable and meet or exceed the minimum requirements identified in Sections 4.3.1, 4.3.2, 4.3.3, 4.3.4, and 4.3.5 when tested in the mated condition. NAMA must approve any supplier changes to the fit, form, or function. Discrete components, i.e. contacts, are not required to be inter-changeable between supplier products.

4.3.1. **Material**

4.3.1.1. Terminal: Phosphor Bronze
4.3.1.2. Plating: Tin or Tin/Lead
4.3.1.3. Housing: UL 94V-2 nylon

4.3.2. **Ratings**

Section	Item	Requirement
4.3.2.1.	Rated Voltage (Max)	600 Volts AC
4.3.2.2.	Maximum Rated Current (Six Circuit)	7 Amps
4.3.2.3.	Ambient Temperature Range (including terminal T-rise)	-40°C to +105°C

Petitioner Exhibit 1002-2771
CSC ServiceWorks – Ex. 1008
Page 47 of 270

4.3.3. **Electrical Performance**

Section	Item	Test Condition	Requirement
4.3.3.1.	Contact Resistance	Mate Connectors, measure by dry circuit, 20 mV max., 10 mA. Wire resistance shall be removed from the measured value.	10 mΩ Max.
4.3.3.2.	Insulation Resistance	Mate Connectors, apply 500V DC between adjacent terminal or ground.	1000 MΩ Min.
4.3.3.3.	Dielectric Strength	Mate Connectors, apply 1500V AC for 1 minute between adjacent terminal or ground.	No Breakdown.

4.3.4. **Mechanical Performance**

Section	Item	Test Condition		Requirement
4.3.4.1.	Insertion and Withdrawal Force	Insert and withdraw connectors at a speed rate of 25 +/- 3mm / minute.		Noted Below
	6 Pos Insertion Max.		6 Pos Withdrawal Min.	
	Initial	30th cycle	Initial	30th cycle
	41.2 N	38.2 N	2.9 N	2.4 N
4.3.4.2.	Crimping Pull Out Force	Mount the crimped terminal, apply axial force on the wire at a rate of 25 +/- 3mm minute.		
		16 AWG		88 N Min.
		18 AWG		88 N Min.
		20 AWG		59 N Min.
		22 AWG		39 N Min.
		24 AWG		29 N Min.
		26 AWG		20 N Min.
		28 AWG		10 N Min.
4.3.4.3.	Terminal Insertion Force	Insert the crimped terminal into the housing.		15 N Max.
4.3.4.4.	Terminal/Housing Retention Force	Apply axial pull out force at the speed rate of 25 +/- 3mm / minute.		22 N Min.
4.3.4.5.	Locking / Unlocking Force	Measure force to lock & unlock connector housings (without contacts) at a rate of 25 +/- 3mm / minute.		Lock: 30 N Max. Unlock: 50 N Min.

Petitioner Exhibit 1002-2772
CSC ServiceWorks – Ex. 1008
Page 48 of 270

4.3.5. **Environmental Performance**

Section	Item	Test Condition	Requirement	
4.3.5.1.	Repeated Insertion / Withdrawal	When mated up to 30 cycles repeatedly by rate of 10 cycles per minute.	Contact Resistance	20 mΩ Max.
4.3.5.2.	Temperature Rise	Carrying rated current load.	30°C Rise Max.	
4.3.5.3.	Vibration	Amplitude: 1.5mm P-P Sweep Time: 10-55-10 Hz in 1 minute. Duration: 2 hours in each X,Y,Z axis.	Appearance	No Damage
			Contact Resistance	20 mΩ Max.
			Discontinuity	1 μ sec. Max.
4.3.5.4.	Shock	50 G; 3 strokes in each X,Y,Z axis.	Appearance	No Damage
			Contact Resistance	20 mΩ Max.
			Discontinuity	1 μ sec Max.
4.3.5.5.	Heat Resistance	105 +/- 2°C, 96 hours	Appearance	No Damage
			Contact Resistance	20 mΩ Max.
4.3.5.6.	Cold Resistance	-40 +/- 3°C, 96 hours	Appearance	No Damage
			Contact Resistance	20 mΩ Max.
4.3.5.7.	Humidity	Temperature: 60 +/- 2°C Relative Humidity: 90% - 95% Duration: 96 hours	Appearance	No Damage
			Contact Resistance	20 mΩ Max.
			Dielectric Strength	No Breakdown
			Insulation Resistance	1000 MΩ Min.
4.3.5.8.	Temperature Cycling	5 Cycles: a) - 55°C ; 30 Minutes b) 105°C ; 30 Minutes	Appearance	No Damage
			Contact Resistance	20 mΩ Max.
4.3.5.9.	Salt Spray	48 +/- 4 hours exposure to salt spray from 5 +/- 1% solution at 35 +/- 2°C.	Appearance	No Damage
			Contact Res.	20 mΩ Max.
4.3.5.10.	SO_2 Gas	24 hour exposure to 50 +/- 5 ppm SO_2 gas at 40 +/- 2°C.	Appearance	No Damage
			Contact Res.	Max.

Petitioner Exhibit 1002-2778
CSC ServiceWorks – Ex. 1008
Page 49 of 270

4.3.6 Approved Suppliers and Part Numbers

4.3.6.1. Suppliers

Molex : Mini-Fit, Jr.™ Product
AMP: AMP-DUAC™ Product

4.3.6.2. Peripherals

Connector: Six (6) Circuit Receptacle Housing

Molex 39-01-2060
AMP P/N 106527-6

Terminals: Female Contacts (sockets), Tin

Molex 39-00-0065
AMP P/N 106528-2 or 106529-2

Strain Relief: The strain relief shall not exceed a Maximum Form Factor of 0.85 inch wide x 0.75 inch high x 1.90 inch long, excluding integrated hinges and wire ties.

Molex 15-04-0296
AMP P/N 1375618-1

4.3.6.3. Bus Harness

Connector: Six (6) Circuit Plug Housing

Molex 39-01-2061
AMP P/N 794550-6 or 794542-6

Terminals: Male Contacts (pins), Tin

Molex 39-00-0067
AMP P/N 794578-1 or 794576-1

4.3.6.4. VMC Connector (Direct PCB Mount)

Vertical Header: Male Contacts (pins), Tin

Molex 39-28-1063
AMP P/N 794664-6

Right Angle Header: Male Contacts (pins), Tin

Molex 39-30-1060
AMP P/N 794448-1

Petitioner Exhibit 1002-2774
CSC ServiceWorks – Ex. 1008
Page 50 of 270

4.3.6.5. Approved Parts – Alternate Form Factors

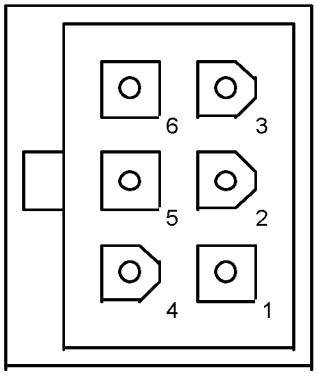
Select applications may require connector configurations with alternate form factors. Alternate form factor connectors may be used provided they are:

- provided by the Approved Suppliers listed
- part of the Approved Supplier Product Family portfolio
- intermateable with the approved connector part numbers listed
- meet the performance objectives set forth in this specification

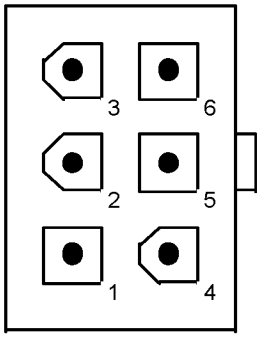
Petitioner Exhibit 1002-2775
CSC ServiceWorks – Ex. 1008
Page 51 of 270

Connector Pin-out:

Line 1 - 34 VDC
Line 2 - DC Power Return
Line 3 - N/C
Line 4 - Master Receive
Line 5 - Master Transmit
Line 6 - Communications Common



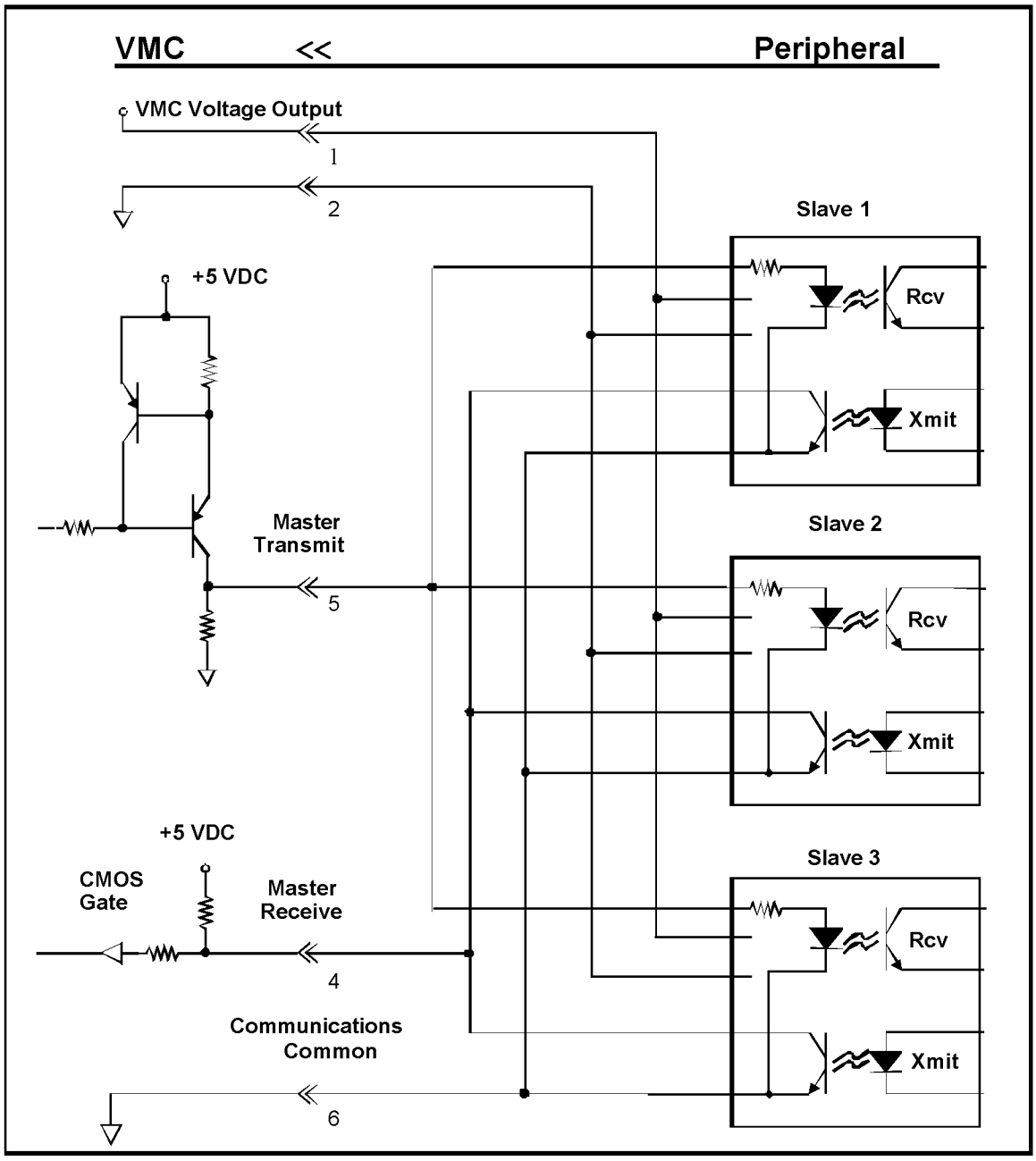
Peripheral Connector
Face View
Receptacle
(Sockets)



VMC / Bus Connector
Face View
Header
(Pins)

Petitioner Exhibit 1002-2776
CSC ServiceWorks – Ex. 1008
Page 52 of 270

4.4 Example Schematic



Petitioner Exhibit 1002-2777
CSC ServiceWorks – Ex. 1008
Page 53 of 270

Section 5

Coin Acceptor/Changer
VMC/Peripheral Communication Specifications

5.1 Introduction

This section defines the communication bytes sent and received by a coin accepting device ("Changer"). As defined in Section 2.3, the changer's address is 00001xxxB (08H).

Unless stated otherwise, all information is assumed to be in a binary format.

There are currently two levels of support defined for the coin mechanism interface, Level 2 and Level 3. The level of coin mechanism operation is sent to the VMC in the response to the STATUS command (defined later in this section). The following paragraphs will define how a VMC should differentiate between each level.

Level 2 Changers

For level 2 changers, VMC operation consists of monitoring inputs from the coin mechanism, accumulating credit, issuing a coin acceptance disable command when appropriate, and issuing appropriate payout commands based on the VMC resident payout algorithms and escrow rules.

Level 3 Changers

For level 3 changers, VMC operation is the same as defined above for level 2, with the addition of the EXPANSION command and its implications (defined later in this section). The VMC has the option of sending the EXPANSION command to the coin mechanism to determine the coin mechanism's manufacturer code, serial number, model/tuning revision, software version, and optional features. Based on the optional feature information the VMC will determine the appropriate operating mode (in other words, modes that both the coin mechanism and the VMC can support), enable any appropriate coin mechanism features by sending an appropriate feature enable command back to the coin mechanism, and enter the proper operating mode. This technique allows all VMCs and peripherals to accommodate existing feature capabilities and provides a means for upgrading Level 3 equipment.

Petitioner Exhibit 1002-2778
CSC ServiceWorks – Ex. 1008
Page 54 of 270

5.2 VMC Commands

Command	Hex Code	Description
RESET	08H	Command for changer to self-reset
SETUP *	09H	Request for changer setup information.
TUBE STATUS	0AH	Request for changer tube status.
POLL	0BH	Request for changer activity status.
COIN TYPE	0CH	Signifies coin types accepted and allowable coin dispensing. This command is followed by setup data. See command format section.
DISPENSE	0DH	Command to dispense a coin type. Followed by coin type to dispense. See command format section.
EXPANSION COMMAND	0FH	Command to allow addition of features and future enhancements. Changers at feature level 2 do not support this command.

NOTE: An EXPANSION command is always followed by a "sub-command." This command allows for feature additions.

* In Version 1.0 & 2.0, **SETUP** was called **STATUS.**

Petitioner Exhibit 1002-2779
CSC ServiceWorks – Ex. 1008
Page 55 of 270

5.3 VMC Command Format

VMC Command	Code	VMC Data
RESET	08H	No data bytes

This command is the vehicle that the VMC should use to tell the changer that it should return to its default operating mode. With the exception of the ACK response, it should abort all communication and disable all acceptance until otherwise instructed by the VMC.

The following initialization sequence is recommended for all new VMCs designed after July, 2000. It should be used after "power up", after issuing the RESET command, or after issuing the Bus Reset (pulling the transmit line "active" for a minimum of 100 mS).

POLL – 0Bh
To obtain "JUST RESET" response

SETUP – 09h
To obtain changer level and configuration information

EXPANSION IDENTIFICATION – 0F 00h (Level 03+ only)
To obtain additional changer information and options

EXPANSION FEATURE ENABLE – 0F 01h (Level 03+ only)
To enable desired options

EXPANSION SEND DIAG STATUS – 0F 05h (Level 03+ & option b1 only)
To request the changer to report its current state of operation

TUBE STATUS – 0Ah (Note 1)
To obtain tube status / change information

COIN TYPE – 0Ch
To enable desired coin acceptance and disable manual coin payout if desired

Note 1 – A minimum 500 msec delay is required between a reset (regardless of type) and the first **TUBE STATUS** command for certain models of the existing MDB coin changer field base.

Petitioner Exhibit 1002-2780
CSC ServiceWorks – Ex. 1008
Page 56 of 270

VMC Command	Code	Changer Response Data
SETUP	09H	23 bytes: Z1 - Z23

Z1 = Changer Feature Level - 1 byte

Indicates the feature level of the changer. This will distinguish the changers feature level to the VMC. Current defined levels:

Level 2: Supports "core" command set. These are: RESET, STATUS, TUBE STATUS, POLL, COIN TYPE, and DISPENSE. (Z1 = 02h)

Level 3: Supports level two and the EXPANSION command addition changer model number, manufacturer code, turning revision, etc. See the details of EXPANSION command later in this document. (Z1=03h)

Z2 - Z3 = Country / Currency Code - 2 bytes

The packed BCD country / currency code of the changer can be sent in two different forms depending on the value of the left most BCD digit.

If the left most digit is a 0, the International Telephone Code is used to indicate the country that the changer is set-up for. For example, the USA code is 00 01H (Z2 = 00 and Z3 = 01).

If the left most digit is a 1, the latest version of the ISO 4217 numeric currency code is used (see Appendix A1). For example, the code for the US dollar is 18 40H (Z2 = 18 and Z3 = 40) and for the Euro is 1978 (Z2 = 19 and Z3 = 78).

All new designs after July, 2000 must use the ISO 4217 numeric currency codes as listed in Appendix A1.

Z4 = Coin Scaling Factor - 1 byte

Petitioner Exhibit 1002-2781
CSC ServiceWorks – Ex. 1008
Page 57 of 270

All accepted coin values must be evenly divisible by this number. For example, this could be set to 05H for the USA nickel.

Z5 = Decimal Places - 1 byte

Indicates the number of decimal places on a credit display. For example, this could be set to 02H in the USA.

Petitioner Exhibit 1002-2782
CSC ServiceWorks – Ex. 1008
Page 58 of 270

Z6 - Z7 = Coin Type Routing - 2 bytes

Indicates what coin types can be routed to the Changer's tubes.

```
b15  b14  b13  b12  b11  b10  b9  b8 | b7  b6  b5  b4  b3  b2  b1  b0
Z6                                                              Z7
```

Bit is set to indicate a coin type can be routed to the tube. Valid coin types are 0 to 15.

Z8 - Z23 = Coin Type Credit - 16 bytes

Indicates the value of coin types 0 to 15. Values must be sent in ascending order. This number is the coin's monetary value divided by the coin scaling factor. Unused coin types are sent as 00H. Unsent coin types are assumed to be zero. It is not necessary to send all coin types. Coin type credits sent as FFH are assumed to be vend tokens. That is, their value is assumed to worth one vend.

The bytes position in the 16 byte string indicates the coin type(s). For example, the first byte sent would indicate the value of coin type 0, the second byte sent would indicate the value of coin type 1, and so on. For example, the USA coin types may be; Coin type 0 = nickel, Coin type 1 = dime, Coin type 2 = quarter, Coin type 3 = dollar.

VMC Command	**Code**	**Changer Response Data**
TUBE STATUS	0AH	18 bytes: Z1 - Z18

Z1 - Z2 = Tube Full Status - 2 bytes

Indicates status of coin tube for coin types 0 to 15.

```
b15  b14  b13  b12  b11  b10  b9  b8 | b7  b6  b5  b4  b3  b2  b1  b0
Z1                                                              Z2
```

A bit is set to indicate a full tube. For example, bit 7 = set would indicate the tube for coin type 7 is full.

Z3 - Z18 = Tube Status - 16 bytes

Indicates the greatest number of coins that the changer "knows" definitely are present in the coin tubes. A bytes position in the 16 byte string indicates the number of coins in a tube for a particular coin type. For example, the first byte sent indicates the number of coins in a tube for coin type 0. Unsent bytes are

Petitioner Exhibit 1002-2783
CSC ServiceWorks – Ex. 1008
Page 59 of 270

assumed to be zero. For tube counts greater than 255, counts should remain at 255.

NOTE: If a changer can detect a tube jam, defective tube sensor, or other malfunction, it will indicate the tube is "bad" by sending a tube full status and a count of zero for the malfunctioning coin type.

VMC Command	Code	Changer Response Data
POLL	0BH	16 bytes: Z1 - Z16

Z1 - Z16 = Changer Activity - 16 bytes

Indicates the changer activity. If there is nothing to report, the changer should send only an ACK. Otherwise, the only valid responses are:

Coins Dispensed Manually:

Z1	Z2
(1yyyxxxx)	(zzzzzzzz)

yyy = The number of coins dispensed.
xxxx = The coin type dispensed (0 to 15)
zzzzzzzz = The number of coins in the tube.

Coins Deposited:

Z1	Z2
(01yyxxxx)	(zzzzzzzz)

yy = Coin routing. 00: CASH BOX
01: TUBES
10: NOT USED
11: REJECT

xxxx = Coin type deposited (0 to 15).

zzzzzzzz = The number of coins in the tube for the coin type accepted.

Status:

(00000001) = Escrow request[1] - An escrow lever activation has been detected.

(00000010) = Changer Payout Busy[2] - The changer is busy activating payout devices.

(00000011) = No Credit[1] - A coin was validated but did not get to the place in the system when credit is given.

Petitioner Exhibit 1002-2784
CSC ServiceWorks – Ex. 1008
Page 60 of 270

(00000100) = Defective Tube Sensor[1] - The changer has detected one of the tube sensors behaving abnormally.

(00000101) = Double Arrival[1] - Two coins were detected too close together to validate either one.

(00000110) = Acceptor Unplugged[2] - The changer has detected that the acceptor has been removed.

(00000111) = Tube Jam[1] - A tube payout attempt has resulted in jammed condition.

(00001000) = ROM checksum error[1] - The changers internal checksum does not match the calculated checksum.

(00001001) = Coin Routing Error[1] - A coin has been validated, but did not follow the intended routing.

(00001010) = Changer Busy[2] - The changer is busy and can not answer a detailed command right now.

(00001011) = Changer was Reset[1] - The changer has detected an Reset condition and has returned to its power-on idle condition.

(00001100) = Coin Jam[1] - A coin(s) has jammed in the acceptance path.

(00001101) = Possible Credited Coin Removal[1] – There has been an attempt to remove a credited coin.

Note:

- changers must have a means to disable this code due to potential older VMC issues.
- virtually all VMCs designed prior to this code's introduction (10/16/02) will not support it.
- It is a vending machine system issue as to what is done when this code is received.

Slug:

(001xxxxx) = xxxxx is the number of slugs since the last activity.

NOTES: The Changer may send several of one type activity, up to 16 bytes total. This will permit zeroing counters such as slug, inventory, and status.

1 Sent once each occurrence.
2 Sent once each POLL

Petitioner Exhibit 1002-2785
CSC ServiceWorks – Ex. 1008
Page 61 of 270

File Transport Layer POLLed responses:

Note that all FTL responses are defined in Section 2.6. For the coin changer, the source address will always be the changer (08H) as defined in Section 2.3.

Z1

1B	REQ TO RCV	The coin changer is requesting to receive data from a device or VMC. Z2 = Destination address of response Z3 = Source address of response (08H) Z4 = File ID Z5 = Maximum length Z6 = Control
1C	RETRY/DENY	The coin changer is requesting a device or VMC to retry or deny the last FTL command. Z2 = Destination address of response Z3 = Source address of response (08H) Z4 = Retry delay
1D	SEND BLOCK	The coin changer is sending a block of data (maximum of 31 bytes) to a device or VMC. Z2 = Destination address of data Z3 = Block # Z4-Z34 = Data (maximum of 31 bytes)
1E	OK TO SEND	The coin changer is indicating that it is OK for a device or VMC to send it data. Z2 = Destination address of response Z3 = Source address of response (08H)
1F	REQ TO SEND	The coin changer is requesting to send data to a device or VMC. Z2 = Destination address of response Z3 = Source address of response (08H) Z4 = File ID Z5 = Maximum length Z6 = Control

VMC Command	**Code**	**VMC Data**

Petitioner Exhibit 1002-2786
CSC ServiceWorks – Ex. 1008
Page 62 of 270

COIN TYPE 0CH 4 bytes: Y1 - Y4

Y1 - Y2 = Coin Enable - 2 bytes

```
b15  b14  b13  b12  b11  b10  b9  b8 | b7  b6  b5  b4  b3  b2  b1  b0
Y1                                                              Y2
```

A bit is set to indicate a coin type is accepted. For example, bit 6 is set to indicate coin type 6, bit 15 is set to indicate coin type 15, and so on. To disable the changer, disable all coin types by sending a data block containing 0000H. All coins are automatically disabled upon reset.

Y3 - Y4 = Manual Dispense Enable - 2 bytes

```
b15  b14  b13  b12  b11  b10  b9  b8 | b7  b6  b5  b4  b3  b2  b1  b0
Y3                                                              Y4
```

A bit is set to indicate dispense enable. For example, bit 2 is set to enable dispensing of coin type 2. This command enables/disables manual dispensing using optional inventory switches. All manual dispensing switches are automatically enabled upon reset.

Petitioner Exhibit 1002-2787
CSC ServiceWorks – Ex. 1008
Page 63 of 270

VMC Command	Code	VMC Data
DISPENSE	0DH	1 byte: Y1

b7 b6 b5 b4 b3 b2 b1 b0
Y1

Bits b3, b2, b1, b0 indicate coin type to be dispensed. Valid codes are 0H to FH to indicate coin types 0 to 15.

Bits b7, b6, b5, b4 indicate the number of coins to be dispensed.

NOTE 1: If two coin types have the same value, the highest coin type should be paid out first.

NOTE 2: There is no defined limit on how long the actual dispense takes since the command allows for up to 15 coins to be paid out. The payout cycle begins when the changer ACKs the VMC's DISPENSE (0DH) command. This cycle typically lasts a minimum of 100 mS and ends when the changer stops dispensing the desired number of coins. VMCs should monitor the Changer Payout Busy response to the POLL command to determine when the entire payout cycle is completed.

However, it must be noted that other than ACKing the DISPENSE (0DH) command, the changer does not have to respond during the payout cycle provided the payout cycle is less than the changer's non-response time and the changer starts responding again prior to the end of the non-response time. Thus, it is acceptable for the changer to never report Changer Payout Busy, but simply start ACKing the POLL commands upon completion of a payout cycle provided the non-response time has not been exceeded.

Petitioner Exhibit 1002-2788
CSC ServiceWorks – Ex. 1008
Page 64 of 270

LEVEL THREE CAPABILITIES - EXPANSION COMMAND

The following describes the currently defined expansion commands.

Sub-command 00H is used for a changer that has the capability of reporting model number, serial number, and so on.

VMC Command	Code	Sub-Command	Changer Response Data
EXPANSION COMMAND	0FH	00H IDENTIFICATION	33 bytes: Z1 - Z33

Z1 - Z3 = Manufacturer Code - 3 bytes
Identification code for the equipment supplier. Sent as ASCII characters. Currently defined codes are listed in the **EVA** document entitled "***European Vending Association Data Transfer Standard***" (**EVA-DTS**), the Audit Data Lists section, sub-section 2, "Manufacturer Codes".

Z4 - Z15 = Serial Number - 12 bytes

Factory assigned serial number. All bytes must be sent as ASCII characters, zeros (30H) and blanks (20H) are acceptable.

Z16 - Z27 = Model #/Tuning Revision - 12 bytes

Manufacturer assigned model number and tuning number. All bytes must be sent as ASCII characters, zeros (30H) and blanks (20H) are acceptable. Each manufacturer should include information concerning the changer tuning revision.

Z28 - Z29 = Software Version - 2 bytes

Current software version. Must be sent in packed BCD.

Z30 - Z33 = Optional Features - 4 bytes

Each of the 32 bits indicate an optional features availability. If the bit is set the feature is available. Bits should be sent in descending order, i.e. bit 31 is sent first and bit 0 is sent last. Currently defined options are:

b0 - Alternative Payout method. This method allows changer designs that determine change payout. That is, the payout algorithm may reside in the changer instead of the VMC.

Petitioner Exhibit 1002-2780
CSC ServiceWorks – Ex. 1008
Page 65 of 270

b1 - Extended Diagnostic command supported. This command allows the VMC to request diagnostic status of the coin changer.

b2 - Controlled Manual Fill and Payout commands supported. These commands allows the VMC to request the number of coin inserted or dispensed while the changer was in a controlled manual fill or payback mode.

b3 - File Transport Layer (FTL) supported as defined in Section 2.6.

b4 - b31 Available for future use

VMC Command	Code	Sub-Command	VMC Data
EXPANSION COMMAND	0FH	01H FEATURE ENABLE	4 bytes: Y1 - Y4

This command is used to enable each of the optional features defined in Z30-Z33 above. To enable a feature a bit is set to one. **All optional features are disabled after reset.**

VMC Command	Code	Sub-command	VMC Data	Changer Response
EXPANSION COMMAND (Alternative Payout)	0FH	02H PAYOUT	Y1	None

Y1 = Value of coins to be paid out - 1 byte

This value is expressed as the number of coin scaling factors that would sum to the value. For example, in a USA system using a scaling factor of 05, if the change to be paid out is 75 cents, then Y1 will equal fifteen. That is, the sum of fifteen nickels equal 75 cents. The coin changer will determine which actual denominations of coins will be paid out. In the 75 cent example, the coins may be 3 quarters; or, 7 dimes & 1 nickel; or, 2 quarters & 2 dimes & 1 nickel, etc.

Petitioner Exhibit 1002-2790
CSC ServiceWorks – Ex. 1008
Page 66 of 270

VMC Command	Code	Sub-command	VMC Data	Changer Response
EXPANSION COMMAND (Alternative Payout)	0FH	03H PAYOUT STATUS	None	16 bytes: Z1-Z16

Z1 - Z16 = Number of each coin type paid out - 16 bytes

This is the changer's response to the last VMC Alternative PAYOUT command (0FH-02H). Bytes are sent in ascending order of coin types. A bytes position in the string indicates the coin type. That is, byte one is the number of coins for coin type 1, byte two is the number of coins for coin type two, and so on. Unsent bytes are assumed to be zero.

The changer clears payout data after an ACK response from the VMC.

The VMC should compare the value of the coins paid out to the (0FH-02H) Alternative PAYOUT command's Y1 .

NOTES: 1) If the changer's payout is busy it will respond to the Alternative PAYOUT STATUS command with an ACK only.

2) If no coins have been paid out, at least one zero valued data byte must be sent.

3) There is no defined limit on how long the actual payout takes. See Note 2 under the DISPENSE (0DH) command.

VMC Command	Code	Sub-command	Changer Response Data
EXPANSION COMMAND (Alternative Payout)	0FH	04H PAYOUT VALUE POLL	1 byte: Z1

Z1 = Changer Payout Activity - 1 byte

An interval value (scaled) which indicates the amount of paid out change since the previous PAYOUT VALUE POLL (or between the initial Alternative PAYOUT command (0FH-02H) and the first PAYOUT VALUE POLL).

Petitioner Exhibit 1002-2791
CSC ServiceWorks – Ex. 1008
Page 67 of 270

An 00H response indicates no coins were paid out since the previous PAYOUT VALUE POLL (or the initial Alternative PAYOUT command (0FH-02H)).

An ACK only indicates that the change payout is finished. This should be followed by the PAYOUT STATUS command (0FH-03H) to obtain the complete payout data.

NOTE: The initial intent of this command is to determine the amount of change paid out so that the credit display can be decremented as coins are dispensed.

VMC Command	Code	Sub-Command	Changer Response Data
EXPANSION	**0FH**	**05H**	**16 bytes: Z1-Z16**
COMMAND	**SEND DIAGNOSTIC STATUS**		

Send Current Diagnostic Status - This command requests the changer to report its current state of operation. The VMC should periodically transmit the command approximately every 1 to 10 seconds.

.

Z1-Z2 **= Current changer diagnostic information**

The changer reports its current state of operation in a 2 byte code. Z1 is the main code and Z2 is the sub-code. The code is reported as long as the condition exists and stops being reported as soon as the condition does not exist. Multiple 2 byte codes may be sent in response to a single command which could result in a maximum of eight 2 byte codes (16 bytes total).

The following tables identify the currently defined extended diagnostic codes:

Petitioner Exhibit 1002-2792
CSC ServiceWorks – Ex. 1008
Page 68 of 270

Z1 / Z2	Status	Cause(s) of Status / Error
01 / 00	Powering up	Changer powering up / initialization
02 / 00	Powering down	Changer powering down
03 / 00	OK	Changer fully operational and ready to accept coins
04 / 00	Keypad shifted	MODE key pressed and held so that LED flashes indicating keypad in shifted state. Reverts to normal mode if no key pressed for 15 seconds
05 / 10	Manual Fill / Payout active	Manual Fill or Manual Payout mode of operation in progress (under control of the changer). This response must be reported at least once to allow the VMC to request a manual fill or manual payout report.
05 / 20	New Inventory Information Available	Changer not in Manual inventory mode, but new inventory information available.
06 / 00	Inhibited by VMC	All coin acceptance inhibited at request of VMC, possibly due to product dispenser jams, completely sold out, etc.
10 / Z2	General changer error	Z2 defined as: **00** Non specific error. **01** Check sum error #1. A check sum error over a particular data range of configuration field detected. **02** Check sum error #2. A check sum error over a secondary data range or configuration field detected. **03** Low line voltage detected. The changer has disabled acceptance or payout due to a low voltage condition.

Petitioner Exhibit 1002-2798
CSC ServiceWorks – Ex. 1008
Page 69 of 270

Z1 / Z2	Status	Cause(s) of Status / Error
11 / Z2	Discriminator module error	Z2 defined as: **00** Non specific discriminator error. **10** Flight deck open. **11** Escrow Return stuck open. **30** Coin jam in sensor. **41** Discrimination below specified standard. **50** Validation sensor A out of range. The acceptor detects a problem with sensor A. **51** Validation sensor B out of range. The acceptor detects a problem with sensor B. **52** Validation sensor C out of range. The acceptor detects a problem with sensor C. **53** Operating temperature exceeded. The acceptor detects the ambient temperature has exceeded the changer's operating range, thus possibly affecting the acceptance rate. **54** Sizing optics failure. The acceptor detects an error in the sizing optics.
12 / Z2	Accept gate module error	Z2 defined as: **00** Non specific accept gate error. **30** Coins entered gate, but did not exit. **31** Accept gate alarm active. **40** Accept gate open, but no coin detected. **50** Post gate sensor covered before gate opened.
13 / Z2	Separator module error	Z2 defined as: **00** Non specific separator error **10** Sort sensor error. The acceptor detects an error in the sorting sensor.
14 / Z2	Dispenser module error	Z2 defined as: **00** Non specific dispenser error.
15 / Z2	Coin Cassette / tube module error	Z2 defined as: **00** Non specific cassette error. **02** Cassette removed. **03** Cash box sensor error. The changer detects an error in a cash box sensor. **04** Sunlight on tube sensors. The changer detects too much ambient light on one or more of the tube sensors.

Petitioner Exhibit 1002-2794
CSC ServiceWorks – Ex. 1008
Page 70 of 270

Diagnostic Status EVA-DTS Correlation

The Extended Diagnostic information reported may be used by the vending machine controller as desired (i.e., service mode displays); however, EVA-DTS **data elements could also be used for reporting to a host system. Examples are:**

- o **Via a translation of the Z1/Z2 code to one of the** Fault Lists **as described in Section 10 of the** EVA-DTS.

- o **Via the EA201 Event Identification element with the format** EAxxyy **where xx = Z1 and yy = Z2.**

- o **Via a customer / manufacture specific coding scheme using the** MA5xx **fields.**

VMC Command	Code	Sub-Command	Changer Response Data
EXPANSION	**0FH**	**06H**	**16 bytes Z1-Z16**
COMMAND	**SEND CONTROLLED MANUAL FILL REPORT**		

Send Controlled Manual Fill Report - **This command requests the changer to report the number of coins inserted during a changer controlled manual fill (controlled bulk fill) mode. While in this mode, the changer must not report coins inserted in response to the** POLL **command.**

Z1-Z16 **= number of controlled manual mode filled coins (by coin type)**

A single byte is reported for each coin type, 0 to 15. For example, Z1 = number of coins of coin type 0 added in a controlled manual fill mode. Any amount above 255 will be reported as 255, i.e. it will reach a maximum limit.

Only coin types *supported* are required to be reported. Counts for unsent coins types will be assumed to be unchanged.

Notes: **After power on, changer reset, closing of the machine door, or a change in controlled manual fill status in the changer (changer indicated it was in controlled manual fill mode via CM0510 then changed to any other state) the machine should request the controlled manual coin fill data from the changer using the above command.**

See EVA-DTS correlation at end of SEND CONTROLLED MANUAL PAYOUT REPORT **(0F-07H) command.**

Petitioner Exhibit 1002-2795
CSC ServiceWorks – Ex. 1008
Page 71 of 270

VMC Command	Code	Sub-Command	Changer Response Data
EXPANSION	**0FH**	**07H**	**16 bytes Z1-Z16**
COMMAND	**SEND CONTROLLED MANUAL PAYOUT REPORT**		

Send Controlled Manual Payout Report - **This command requests the changer to report the number of coins dispensed during a changer controlled manual payout (controlled bulk dispense) mode. Note that this does not include the coins dispensed via the individual dispense switches.**

If the new Controlled Manual Fill / Payout command is implemented in the coin mech and **enabled by the VMC (0Fh, 01h, bit 2 of Y1 to Y4), while in a controlled manual payout (dispense) mode, the changer** must not **report the coins paid out in response to the** POLL **command. Conversely, if the changer does not support the new command or the VMC does not enable it, the changer** should **report the coins paid out in response to the** POLL **command.**

Z1-Z16 **= number of controlled manual mode dispensed coins (by coin type)**

> **A single byte is reported for each coin type 0 to 15. For example, Z1 = number of coins of coin type 0 dispensed in a controlled manual payout mode. Any amount above 255 will be reported as 255, i.e. it will reach a maximum limit.**
>
> **Only coin types supported are required to be reported. Counts for unsent coin types will be assumed to be unchanged.**

Note: **After power on, changer reset, closing of the machine door, or a change in controlled manual payout status in the changer (changer indicated it was in controlled manual payout mode via CM0510 then changed to any other state) the machine should request the controlled manual coin payout data from the changer using the above command.**

Controlled Manual Fill / Payout EVA-DTS Correlation

The controlled manual fill and payout coin information may be used by the vending machine controller as desired (i.e., service mode displays); however, EVA-DTS **data elements could be used for reporting to a host system. Examples are:**

Petitioner Exhibit 1002-2796
CSC ServiceWorks – Ex. 1008
Page 72 of 270

	CA3XX	CA4XX	CA1704	CA1705
Controlled Manual Fill	0F06	n/a	0F06	n/a
VMC Tube Fill	VMC	n/a	VMC	n/a
Controlled Manual Payout	n/a	0F07*	n/a	0F07*
VMC Coin Payout	n/a	VMC	n/a	VMC
Manual Dispense Switches	n/a	0B	n/a	0B

***If extended** 0F06 **&** 0F07 **commands are implemented.**
If extended 0F06 **&** 0F07 **commands are not implemented in the coin mech or not enabled by the VMC, the coin mech will respond to the** POLL **command with the controlled manual payout coins.**

With the above, the CA3XX **&** CA4XX **fields can continue to be the primary fields for cash audit and the** CA1704 **&** CA1705 **fields can be used for indicating controlled manually filled / dispensed coins.**

Coin Tube Audit Fields

As a reference, below are the agreed CA17XX **data elements that provide detailed coin tube count information and controlled-manual coin tube insertion / dispense information. These were approved by the** EVA - DTS **Technical Sub Committee on January 27, 1997.**

Block Identifier Reference	Data Contents	Charac-teristic	Length Min	Length Max	Element
CA17	Coin Type Number (per MDB coin type)	N	01	03	CA1701
	Value of Coin	N	01	08	CA1702
	Number of Coins in Tube	N	01	08	CA1703
	Number of Coins Inserted during Controlled-Manual Fill	N	01	08	CA1704
	Number of Coins Dispensed during Controlled-Manual Payout	N	01	08	CA1705

Petitioner Exhibit 1002-2797
CSC ServiceWorks – Ex. 1008
Page 73 of 270

Definitions:

CA1701 **The coin type number as referred to in the MDB Interface Specification. If not an MDB system, the number represents the coin's position in the coin set starting with the lowest value coin accepted. Note if two or more vintage of the same coin is accepted, the oldest one is first.**

For example, the Canadian coin types may be:

0 Old Nickel	**3 Quarter**
1 New Nickel	**4 $1 Dollar**
2 Dime	**5 $2 Dollar**

CA1702 **The cash value of the coin (units base).**

For example, the Canadian coin types would be:

Nickel	**5**	**$1 Dollar**	**100**
Dime	**10**	**$2 Dollar**	**200**
Quarter	**25**		

CA1703 **The number of coins in the coin tube (or tubes if multiple tubes per coin) that are reported by the coin mech during normal vending operations. Note that this is the "best known tube count" and may be inaccurate if coins were manually added or removed by hand.**

CA1704 **The number of coins inserted while the changer was in a Controlled manual fill mode. Controlled manual fill indicates that the coins are being inserted under the control of the coin mech or VMC. Coins are not being loaded by hand through the tops of the tubes.**

CA1705 **The number of coins dispensed while the changer was in a controlled manual payout mode. Controlled manual payout indicates that the coins are being dispensed under the control of the coin mech or VMC. Coins are not being removed by hand by "dumping" the tubes.**

Petitioner Exhibit 1002-2798
CSC ServiceWorks – Ex. 1008
Page 74 of 270

VMC Command	Code	Sub-command	VMC Data	Changer Response
EXPANSION COMMAND	0FH	FAH **FTL** REQ TO RCV	Y1-Y5	Z1 - Zn (immediate or POLLed)

The VMC is requesting to receiv e data from the changer whose destination address will always be (08H). Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 = Destination address of command (08H)
Y2 = Source address of command
Y3 = File ID
Y4 = Maximum length
Y5 = Control

Z1 = 1DH which indicates SEND BLOCK
Z2 = Destination address of data
Z3 = Block #
Z4 - Z34 = Data (maximum of 31 bytes)

or

Z1 = 1CH which indicates RETRY / DENY
Z2 = Destination address of response
Z3 = Source address of response (08H)
Z4 = Retry delay

VMC Command	Code	Sub-command	VMC Data	Changer Response
EXPANSION COMMAND	0FH	FBH **FTL** RETRY / DENY	Y1-Y3	None

The VMC is retrying, denying, or aborting a data transfer to/from the changer whose destinat ion address will always be (08H). Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 = Destination address of command (08H)
Y2 = Source address of command
Y3 = Retry delay

Petitioner Exhibit 1002-2799
CSC ServiceWorks – Ex. 1008
Page 75 of 270

VMC Command	Code	Sub-command	VMC Data	Changer Response
EXPANSION	0FH	FCH	Y1-Y33	None
COMMAND	**FTL** SEND BLOCK			

The VMC is sending data to the changer whose destination address will always be (08H). Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 = Destination address of command & data (08H)
Y2 = Block #
Y3 - Y33 = Data (maximum of 31 bytes)

VMC Command	Code	Sub-command	VMC Data	Changer Response
EXPANSION	0FH	FDH	Y1-Y2	Z1-Z34 (immediate or POLLed)
COMMAND	**FTL** OK TO SEND			

The VMC is indicating that it is OK for the changer to transfer data. The destination address will always be the changer (08H). Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 = Destination address of command (08H)
Y2 = Source address of command

Z1 = 1DH which indicates SEND BLOCK
Z2 = Destination address of data
Z3 = Source address of data
Z4 - Z34 = Data (maximum of 31 bytes)

Petitioner Exhibit 1002-2800
CSC ServiceWorks – Ex. 1008
Page 76 of 270

VMC Command	Code	Sub-command	VMC Data	Changer Response
EXPANSION COMMAND	0FH	FEH **FTL** REQ TO SEND	Y1-Y5	Z1 (immediate or POLLed)

The VMC is requesting to send data to the changer whose destination address will always be (08H). Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 = Destination address of command (08H)
Y2 = Source address of command
Y3 = File ID
Y4 = Maximum length
Y5 = Control

Z1 = 1EH which indicates OK TO SEND
Z2 = Destination address of response
Z3 = Source address of response (08H)

or

Z1 = 1CH which indicates RETRY / DENY
Z2 = Destination address of response
Z3 = Source address of response (08H)
Z4 = Retry delay

VMC Command	Code	Sub-command	VMC Data	Changer Response
EXPANSION COMMAND	0FH	FFH DIAGNOSTICS	Y1-Yn	Z1-Zn

Y1 - Yn = Device manufacturer specific instruction for implementing various manufacturing or test modes. Y1 - Yn implies that any number of bytes can be used for the VMC data to the peripheral.

Z1 - Zn = Device manufacturer specific responses after receiving manufacturing or test instructions. Z1 - Zn implies that any number of bytes can be used for the changer response data from the peripheral.

Petitioner Exhibit 1002-2801
CSC ServiceWorks – Ex. 1008
Page 77 of 270

5.4 Changer Non-Response Time

The maximum non-response time for the changer is two seconds.

5.5 Changer Power Requirements

The current draw for any changer must fall within the following limits. All measurements are at the minimum VMC Voltage Output.

Idle mode = 200 mA. (max.) continuous

Coin acceptance = 1.8 A. (max.) for up to 2 seconds

(For coin changers using solenoid based payout mechanisms - typical of 3 tube changers sold in the US market. Vending machines sold into the US market are required to supply this power.)

1.0 A. (max.) for up to 2 seconds

(For coin changers using motorized payout mechanisms - typical of 4 tube changers.)

Coin payout = 3.6 A. (max.) for 100 mS. with 400 mS. idle current between pulses during the coin payout cycle.

(For coin changers using solenoid based payout mechanisms - typical of 3 tube changers sold in the US market. Vending machines sold into the US market are required to supply this power.)

1.8 A. (max.) during the coin payout cycle.

(For coin changers using motorized payout mechanisms - typical of 4 tube changers.

See Note 2 under the DISPENSE (0DH) command for further information on the coin payout cycles.)

Note: If both peripherals are supported, vending machines should be able to provide sufficient power to simultaneously supply the above power requirements for both the coin changer **Coin Acceptance** and bill validator **Bill Transport** as specified in Section 6.5.

Petitioner Exhibit 1002-2802
CSC ServiceWorks – Ex. 1008
Page 78 of 270

Section 6

Bill Validator
VMC/Peripheral Communication Specifications

6.1 Introduction

This section defines the communication bytes sent and received between a Bill Validator and the VMC. As defined in Section 2.3, the bill validator's address is 00110xxxB (30H).

Unless stated otherwise, all information is assumed to be in a binary format.

There are currently two levels of support defined for the bill validator interface, Level 1 and Level 2. The level of bill validator operation is sent to the VMC in the response to the STATUS command (defined later in this section). The following paragraphs will define how a VMC should differentiate between each level.

Level 1 Bill Validators

Level 1 bill validators support all standard functions, but do not support any optional features.

Level 2 Bill Validators

Level 2 bill validators support all standard functions plus various optional features as defined in Section 6.3 under the Expansion command 37-02H. Based on the optional feature information the VMC will determine the appropriate operating mode (in other words, modes that both the bill validator and the VMC can support), enable any appropriate features by sending an appropriate feature enable command back to the bill validator, and enter the proper operating mode. This technique allows all VMCs and peripherals to accommodate existing feature capabilities and provides a means for upgrading Level 2 equipment.

Petitioner Exhibit 1002-2803
CSC ServiceWorks – Ex. 1008
Page 79 of 270

6.2 VMC Commands

Command	Hex Code	Description
RESET	30H	Command for bill validator to self-reset.
SETUP *	31H	Request for bill validator setup information.
SECURITY	32H	Sets Validator Security Mode
POLL	33H	Request for Bill Validator activity Status.
BILL TYPE	34H	Indicates Bill Type enable or disable. Command is followed by set-up data. See command format.
ESCROW	35H	Sent by VMC to indicate action for a bill in escrow.
STACKER	36H	Indicates stacker full and the number of bills.
EXPANSION COMMAND	37H	Command to allow addition of features and future enhancements. Level 1 and above bill validators must support this command.

NOTE: The expansion command is always followed by a sub-command.

* In Version 1.0 & 2.0, **SETUP** was called **STATUS.**

Petitioner Exhibit 1002-2804
CSC ServiceWorks – Ex. 1008
Page 80 of 270

6.3 VMC Command Format

VMC Command	Code	VMC Data
RESET	30H	No data bytes

This command is the vehicle that the VMC should use to tell the validator that it should return to its default operating mode. It should reject any bills in the validation process, return any bills in the escrow position, and disable all other activity until otherwise instructed by the VMC.

The following initialization sequence is recommended for all new VMCs designed after July, 2000. It should be used after "power up", after issuing the RESET command, or after issuing the Bus Reset (pulling the transmit line "active" for a minimum of 100 mS).

POLL – 33h
To obtain "JUST RESET" response

SETUP – 31h
To obtain bill validator level and configuration information

EXPANSION IDENTIFICATION – 37 00h (Level 01+)
To obtain additional bill validator information

EXPANSION IDENTIFICATION w/ OPTION BITS – 37 02h (Level 02+ only)
To obtain additional bill validator information and options

EXPANSION FEATURE ENABLE – 37 01h (Level 02+ only)
To enable desired options

STACKER – 36h
To obtain stacker status and number of bills

BILL TYPE – 34h
To enable desired bill acceptance and desired bill escrow capability

Petitioner Exhibit 1002-2805
CSC ServiceWorks – Ex. 1008
Page 81 of 270

VMC Command	Code	Validator Response Data
SETUP	31H	27 bytes: Z1 - Z27

Z1 = Bill Validator Feature Level - 1 byte

Indicates current feature level of the bill validator. Currently defined levels are:

Level **1** - does not support option bits (Z1 = 01h)
Level **2** - supports option bits (Z1 = 02h)

Z2 - Z3 = Country / Currency Code - 2 bytes

The packed BCD country / currency code of the bill validator can be sent in two different forms depending on the value of the left most BCD digit.

If the left most digit is a 0, the International Telephone Code is used to indicate the country that the validator is set-up for. For example, the USA code is 00 01H (Z2 = 00 and Z3 = 01).

If the left most digit is a 1, the latest version of the ISO 4217 numeric currency code is used (see Appendix A1). For example, the code for the US dollar is 18 40H (Z2 = 18 and Z3 = 40) and for the Euro is 1978 (Z2 = 19 and Z3 = 78).

All new designs after July, 2000 must use the ISO 4217 numeric currency codes as listed in Appendix A1.

Z4 - Z5 = Bill Scaling Factor - 2 bytes

All accepted bill values must be evenly divisible by this number. For example, this could be set to 0064H for the USA.

Z6 = Decimal Places - 1 byte

Indicates the number of decimal places on a credit display. For example, this could be set to 02H for the USA.

Z7 - Z8 = Stacker Capacity - 2 bytes

Indicates the number of bills that the stacker will hold. For example, 400 bill capacity = 0190H.

Petitioner Exhibit 1002-2806
CSC ServiceWorks – Ex. 1008
Page 82 of 270

Z9 - Z10 = Bill Security Levels - 2 bytes
Indicates the security level for bill types 0 to 15. Since not all validators support multiple security levels, validators that do not have this feature must report a "high" security level.

Z11 = Escrow/No Escrow - 1 byte
Indicates the escrow capability of the bill validator. If Z11 = 00H, the bill validator does not have escrow capability. If Z11 = FFH, the bill
validator has escrow capability.

Z12 - Z27 = Bill Type Credit - 16 bytes
Indicates the value of the bill types 0 to 15. Values must be sent in ascending order. This number is the bill's monetary value divided by the bill scaling factor. Unused bill types are sent as 00H. Unsent bill types are assumed to be zero. FFH bills are assumed to be vend tokens.

VMC Command	Code	VMC Data
SECURITY	32H	2 Bytes: Y1 - Y2

Y1 - Y2 = Bill Type(s) - 2 bytes

b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1	b0
Y1								Y2							

A bit is set to indicate the type of bill(s) which are set to a "high" security level. Note that validators that do not support dual security levels should report a "high" security level in the response bytes Z9-Z10 to the STATUS (31H) command.

VMC Command	Code	Validator Response Data
POLL	33H	16 bytes: Z1 - Z16

Z1 - Z16 = Bill Validator Activity - 16 bytes

Indicates the validator activity, for example, the type and number of bills accepted, and stacker position. If there is nothing to report, the validator should send only an ACK. Otherwise, the only valid responses are:

Bills Accepted:

Indicates the type and number of bills accepted and stacker status.

Z1	
(1yyyxxxx)	**NOTE:** These responses should be used to add or subtract credit.

Petitioner Exhibit 1002-2807 CSC ServiceWorks – Ex. 1008
Page 83 of 270

yyy = Bill Routing;
- 000: BILL STACKED
- 001: ESCROW POSITION
- 010: BILL RETURNED
- 011: NOT USED
- 100: DISABLED BILL REJECTED

xxxx = Bill Type (0 to 15)

Status:

(00000001) = Defective Motor[3] - One of the motors has failed to perform its expected assignment.

(00000010) = Sensor Problem[3] - One of the sensors has failed to provide its response.

(00000011) = Validator Busy[2] - The validator is busy and can not answer a detailed command right now.

(00000100) = ROM Checksum Error[3] - The validators internal checksum does not match the calculated checksum.

(00000101) = Validator Jammed[3] - A bill(s) has jammed in the acceptance path.

(00000110) = Validator was reset[1] - The validator has been reset since the last POLL.

(00000111) = Bill Removed[1] - A bill in the escrow position has been removed by an unknown means. A BILL RETURNED message should also be sent.

(00001000) = Cash Box out of position[3] - The validator has detected the cash box to be open or removed.

(00001001) = Unit Disabled[2] - The validator has been disabled, by the VMC or because of internal conditions.

(00001010) = Invalid Escrow request[1] - An ESCROW command was requested for a bill not in the escrow position.

(00001011) = Bill Rejected[1] - A bill was detected, but rejected because it could not be identified.

(00001100) = Possible Credited Bill Removal[1] – There has been an attempt to remove a credited (stacked) bill.

Note:
- validators must have a means to disable this code due to potential older VMC issues.
- virtually all VMCs designed prior to this code's introduction (10/16/02) will not support it.
- It is a vending machine system issue as to what is done when this code is received.

Petitioner Exhibit 1002-2808
CSC ServiceWorks – Ex. 1008
Page 84 of 270

(010xxxxx) = Number of attempts to input a bill while validator is disabled.[1]

NOTE: The validator may send several of one type activity up to 16 bytes total.

1 Sent once each occurrence.
2 Sent once each POLL
3 Sent once each occurrence. The unit is then disabled until the condition is removed. Validator will respond with unit disabled until repaired or replaced.

Petitioner Exhibit 1002-2809
CSC ServiceWorks – Ex. 1008
Page 85 of 270

File Transport Layer POLLed responses:

Note that all FTL responses are defined in Section 2.6. For the bill validator, the source address will always be the validator (30H) as defined in Section 2.3.

Z1

1B	REQ TO RCV	The bill validator is requesting to receive data from a device or VMC. Z2 = Destination address of response Z3 = Source address of response (30H) Z4 = File ID Z5 = Maximum length Z6 = Control
1C	RETRY/DENY	The bill validator is requesting a device or VMC to retry or deny the last FTL command. Z2 = Destination address of response Z3 = Source address of response (30H) Z4 = Retry delay
1D	SEND BLOCK	The bill validator is sending a block of data (maximum of 31 bytes) to a device or VMC. Z2 = Destination address of data Z3 = Block # Z4-Z34 = Data (maximum of 31 bytes)
1E	OK TO SEND	The bill validator is indicating that it is OK for the device or VMC to send it data. Z2 = Destination address of response Z3 = Source address of response (30H)
1F	REQ TO SEND	The bill validator is requesting to send data to a device or VMC. Z2 = Destination address of response Z3 = Source address of response (30H) Z4 = File ID Z5 = Maximum length Z6 = Control

Petitioner Exhibit 1002-2810
CSC ServiceWorks – Ex. 1008
Page 86 of 270

VMC Command	Code	VMC Data
BILL TYPE	34H	4 bytes: Y1 - Y4

Y1 - Y2 = Bill Enable - 2 bytes

Indicates what type of bills are accepted.

```
b15  b14  b13  b12  b11  b10  b9  b8 | b7  b6  b5  b4  b3  b2  b1  b0
Y1                                                              Y2
```

Bill types are 0 to 15. A bit is set to indicate acceptance of bill type.

NOTE: Sending 0000H disables the bill validator.

Y3 - Y4 = Bill Escrow Enable:

```
b15  b14  b13  b12  b11  b10  b9  b8 | b7  b6  b5  b4  b3  b2  b1  b0
Y3                                                              Y4
```

Bill types are 0 to 15. A bit is set to indicate enable of escrow for a bill type.

NOTE: On power-up or reset all bill acceptance and escrow are disabled.

VMC Command	Code	VMC Data
ESCROW	35H	1 byte: Y1

Y1 = Escrow status - 1 byte

If Y1 = 0;	Return bill in the escrow position.
If Y1 = xxxxxxx1;	Stack the bill ("x" indicates don't care)

NOTE: After an ESCROW command the bill validator should respond to a POLL command with the BILL STACKED, BILL RETURNED, or INVALID ESCROW message within 30 seconds. If a bill becomes jammed in a position where the customer may be able to retrieve it, the bill validator should send a BILL RETURNED message.

Petitioner Exhibit 1002-2811
CSC ServiceWorks – Ex. 1008
Page 87 of 270

VMC Command	Code	Validator Response Data
STACKER	36H	2 bytes: Z1 - Z2

Indicates stacker full condition and the number of bills in the stacker.

Z1 Z2

(Fxxxxxxx) (xxxxxxxx)
F = 1 if stacker is full, 0 if not.

xxxxxxxxxxxxxxx = The number of bills in the stacker.

LEVEL ONE and TWO+ CAPABILITIES - EXPANSION COMMAND

In order to allow existing VMCs to operate with original Level 1 or new Level 2 bill validators, a separate identification sub-command has been introduced to handle the additional 4 bytes of Option Bit information.

The original sub-command 00H is used for obtaining Z1 to Z29 identification information from bill validators. This information includes the model number, serial number, software version, etc, but **not the option bits**. Note that if a Level 2+ bill validator is sent the 00H sub-command, it must **not** report the Z30 to Z33 option bytes.

Sub-command 01H is used for Level 2+ bill validators to enable option bits reported in the expansion command 02H sub-command below.

The new sub-command 02H is used for obtaining Z1 to Z33 identification information from Level 2+ bill validators. This information includes the model number, serial number, software version, etc, and the **option bits (Z30-Z33).**

VMC Command	Code	Sub-Command	Validator Response Data
EXPANSION	37H	00H	29 bytes: Z1 - Z29
COMMAND	LEVEL 1 IDENTIFICATION WITHOUT OPTION BITS		

Z1 - Z3 = Manufacturer Code - 3 bytes
Identification code for the equipment supplier. Sent as ASCII characters. Currently defined codes are listed in the **EVA** document entitled " ***European Vending Association Data Transfer Standard***' (**EVA-DTS**), the Audit Data Lists section, sub-section 2, "Manufacturer Codes".

Petitioner Exhibit 1002-2812
CSC ServiceWorks – Ex. 1008
Page 88 of 270

Z4 - Z15 = Serial Number - 12 bytes
Factory assigned serial number. All bytes must be sent as ASCII characters, zeros (30H) and blanks (20H) are acceptable.

Z16 - Z27 = Model #/Tuning Revision - 12 bytes
Manufacturer assigned model number. All bytes must be sent as ASCII characters, zeros (30H) and blanks (20H) are acceptable.

Z28 - Z29 = Software Version - 2 bytes
Current software version. Must be sent in packed BCD.

VMC Command	Code	Sub-Command	VMC Data
EXPANSION COMMAND	37H	01H LEVEL 2+ FEATURE ENABLE	4 bytes: Y1 - Y4

This command is used to enable each of the Level 2+ optional features defined in the Level 2+ Identification response bytes Z30-Z33 below. To enable a feature a bit is set to one. **All optional features are disabled after reset.**

VMC Command	Code	Sub-Command	Validator Response Data
EXPANSION COMMAND	37H	02H LEVEL 2+ IDENTIFICATION WITH OPTION BITS	33 bytes: Z1 – Z33

Z1 - Z3 = Manufacturer Code - 3 bytes
Identification code for the equipment supplier. Sent as ASCII characters. Currently defined codes are listed in the **EVA** document entitled " ***European Vending Association Data Transfer Standard***' (**EVA-DTS**), the Audit Data Lists section, sub-section 2, "Manufacturer Codes".

Z4 - Z15 = Serial Number - 12 bytes
Factory assigned serial number. All bytes must be sent as ASCII characters, zeros (30H) and blanks (20H) are acceptable.

Z16 - Z27 = Model #/Tuning Revision - 12 bytes
Manufacturer assigned model number. All bytes must be sent as ASCII characters, zeros (30H) and blanks (20H) are acceptable.

Z28 - Z29 = Software Version - 2 bytes
Current software version. Must be sent in packed BCD.

Z30 - Z33 = Optional Features - 4 bytes
Each of the 32 bits indicate an optional features availability. If the bit is set the feature is available. Bits should be sent in descending

Petitioner Exhibit 1002-2818
CSC ServiceWorks – Ex. 1008
Page 89 of 270

order, i.e. bit 31 is sent first and bit 0 is sent last. Currently defined options are:

b0 - File Transport Layer (FTL) supported as defined in Section 2.6.
b1 - b31 Available for future use

VMC Command	Code	Sub-command	VMC Data	Validator Response
EXPANSION COMMAND	37H	FAH **FTL** REQ TO RCV	Y1-Y5	Z1 (immediate or POLLed)

The VMC is requesting to receive data from the bill validator whose destination address will always be (30H). Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 = Destination address of command (30H)
Y2 = Source address of command
Y3 = File ID
Y4 = Maximum length
Y5 = Control

Z1 = 1DH which indicates SEND BLOCK
Z2 = Destination address of data
Z3 = Block #
Z4 - Z34 = Data (maximum of 31 bytes)
or
Z1 = 1CH which indicates RETRY / DENY
Z2 = Destination address of response
Z3 = Source address of response (30H)
Z4 = Retry delay

VMC Command	Code	Sub-command	VMC Data	Validator Response
EXPANSION COMMAND	37H	FBH **FTL** RETRY / DENY	Y1-Y3	None

The VMC is retrying, denying, or aborting a data transfer to/from the bill validator whose destination address will always be (30H). Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 = Destination address of command (30H)
Y2 = Source address of command
Y3 = Retry delay

VMC Command	Code	Sub-command	VMC Data	Validator Response
EXPANSION COMMAND	37H	FCH **FTL** SEND BLOCK	Y1-Y33	None

Petitioner Exhibit 1002-2814 – Ex. 1008
Page 90 of 270

The VMC is sending data to the bill validator whose destination address will always be (30H). Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 = Destination address of command & data (30H)
Y2 = Block #
Y3 - Y33 = Data (maximum of 31 bytes)

VMC Command	Code	Sub-command	VMC Data	Validator Response
EXPANSION COMMAND	37H	FDH **FTL** OK TO SEND	Y1-Y2	Z1-Z34 (immediate or POLLed)

The VMC is indicating that it is OK for the bill validator to transfer data. The destination address will always be the validator (30H). Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 = Destination address of command (30H)
Y2 = Source address of command

Z1 = 1DH which indicates SEND BLOCK
Z2 = Destination address of data
Z3 = Source address of data
Z4 - Z34 = Data (maximum of 31 bytes)

VMC Command	Code	Sub-command	VMC Data	Validator Response
EXPANSION COMMAND	37H	FEH **FTL** REQ TO SEND	Y1-Y5	Z1 (immediate or POLLed)

The VMC is requesting to send data to the bill validator whose destination address will always be (30H). Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 = Destination address of command (30H)
Y2 = Source address of command
Y3 = File ID
Y4 = Maximum length
Y5 = Control

Petitioner Exhibit 1002-2815
CSC ServiceWorks – Ex. 1008
Page 91 of 270

Z1 = 1EH which indicates OK TO SEND
Z2 = Destination address of response
Z3 = Source address of response (30H)

or

Z1 = 1CH which indicates RETRY / DENY
Z2 = Destination address of response
Z3 = Source address of response (30H)
Z4 = Retry delay

VMC Command	Code	Sub-Command	VMC Data	Val Response
EXPANSION COMMAND	37H	FFH DIAGNOSTICS	Y1-Yn	Z1 - Zn

Y1 - Yn = Device manufacturer specific instruction for implementing various manufacturing or test modes. Y1 - Yn implies that any number of bytes can be used for the VMC data to the peripheral.

Z1 - Zn = Device manufacturer specific responses after receiving manufacturing or test instructions. Z1 - Zn implies that any number of bytes can be used for the bill validator response data from the peripheral.

6.4 Bill Validator Non-Response Time

The maximum non-response time for the bill validator is five seconds.

6.5 Bill Validator Power Requirements

The current draw for any bill validator must fall within the following limits. All measurements are at the minimum VMC Voltage Output.

Idle mode = 200 mA. (avg.) continuous

Bill transport = 2.5 A. (max.) up to 10 seconds

Note: If both peripherals are supported, vending machines should be able to provide sufficient power to simultaneously supply the above power requirements for both the bill validator **Bill Transport** and coin mechanism **Coin Acceptance** as specified in Section 5.5.

Petitioner Exhibit 1002-2816
CSC ServiceWorks – Ex. 1008
Page 92 of 270

(this page intentionally left blank)

Petitioner Exhibit 1002-2817
CSC ServiceWorks – Ex. 1008
Page 93 of 270

Section 7

Cashless Device(s)
VMC/Peripheral Communication Specifications

7.1 Introduction

This section defines the communications bytes sent and received between the cashless device(s) and the Vending Machine Controller (VMC). As defined in Section 2.3, there are two cashless device addresses; Cashless #1, 00010xxxB (10H) and Cashless #2, 1100xxxB (60H). The second address has been assigned to allow for two unique forms of cashless devices to be resident in the vending machine simultaneously. An example would be a card based system as Cashless Device #1 (10H) and a mobile phone based system as Cashless Device #2 (60H). **Everything defined in this section will be common to the two cashless devices – only the addresses will be different.**

Unless otherwise stated, all monetary values used by the cashless devices and the VMC will be sixteen bit (Level 01 & 02) or thirty-two bit (Level 03 if 32 bit option enabled), unsigned binary numbers. The numbers will be sent most significant byte first and scaled using the parameters provided by the cashless device's READER CONFIGURATION DATA response.

7.2 State Definitions

MDB cashless devices may be viewed as state machines. These states are as follows:

1) Inactive
2) Disabled
3) Enabled
4) Session Idle
5) Vend
6) Revalue (Level 02/03 cashless devices)
7) Negative Vend (Level 03 cashless devices)

7.2.1 Inactive

This is the state of the cashless device at power up or after a reset. While in the Inactive state, cashless devices will NOT be accepted for vending purposes. The cashless device cannot leave this state until all Setup information is received from the VMC.

7.2.2 Disabled

The cashless device automatically enters this state from the Inactive state when it has received the Setup information specified in 7.4.1. It will also enter the Disabled state from the Enabled state when it receives the READER DISABLE command. While in the Disabled state, payment medias will NOT be accepted for vending purposes. The cashless device will remain in this state until either a READER ENABLE command is received (when it will enter the Enabled state) or a RESET is received (when it will enter the Inactive state). For power management purposes, current consumption will not exceed idle mode specification during disabled state.

7.2.3 Enabled

In this state, cashless devices may be used for MDB transactions. The cashless device will remain in this state until a valid payment media is read (when it will enter the Session Idle state),

Petitioner Exhibit 1002-2818
CSC ServiceWorks – Ex. 1008
Page 94 of 270

a READER DISABLE command is received (when it will return to the Disabled state) or a RESET is received (when it will enter the Inactive state).

7.2.4 Session Idle

In the Enabled state, when a valid payment media is processed, the cashless device will issue a BEGIN SESSION response to a VMC POLL and enter the Session Idle state. This indicates that the cashless device is available for vending activities. The only structured exit from the Session Idle state is through the SESSION COMPLETE message from the VMC. The SESSION COMPLETE command will cause the cashless device to respond with an END SESSION message and enable/disable itself appropriately. Vend / Negative Vend / Revalue commands will cause the cashless device to leave the Session Idle state and enter the Vend / Negative Vend / Revalue state when products are selected and purchased.

7.2.5 Vend

This state is entered from the Session Idle state upon reception of a VEND REQUEST message from the VMC. The entire Vend state is an uninterruptable command/response sequence. The cashless device will return to the Session Idle state upon completion of this sequence.

7.2.6 Revalue (Level 02 / 03 Cashless Devices)

This state is entered from the Session Idle state upon reception of a REVALUE REQUEST message from the VMC. The entire Revalue state is an uninterruptable command/response sequence. The cashless device will return to the Session Idle state upon completion of this sequence.

7.2.7 Negative Vend Request (Level 03 Cashless Devices)

This state is entered from the Session Idle state upon reception of a NEGATIVE VEND REQUEST message from the VMC. The entire Negative Vend Request state is an uninterruptable command/response sequence. The cashless device will return to the Session Idle state upon completion of this sequence.

7.3 Command Protocol

After the VMC has issued a command, no new commands may be issued until all data generated in response to that command has been received from the cashless device. The complete response may be an ACK only (e.g. the READER ENABLE command). Alternatively, it may consist of an informational response (e.g. READER CONFIGURATION DATA).

Petitioner Exhibit 1002-2810
CSC ServiceWorks – Ex. 1008
Page 95 of 270

The cashless device may provide an informational response in two ways. It may respond immediately with the requested data, or the cashless device may ACK the VMC command. If ACKed, the VMC must issue POLLs until the cashless device responds with the requested data, or until the Application Maximum Response Time (defined in READER CONFIGURATION response) has elapsed.

The cashless device will define the currency type at the beginning of each session. The currency type will be used for all following transactions in that session. If the VMC does not support this currency type, it will end the session.

Below are the uninterruptable VMC commands which require an informational cashless device response and their associated result:

VMC Command	Cashless Device Response	Result
SETUP/CONFIGURATION DATA =>	READER CONFIGURATION DATA	
EXPANSION/REQUEST ID =>	PERIPHERAL ID	
READER CANCEL =>	CANCELLED	
VEND REQUEST... VEND CANCEL =>	VEND DENIED*	
VEND REQUEST =>	VEND DENIED*	
VEND REQUEST =>	VEND APPROVED =>	VEND SUCCESS*
VEND REQUEST =>	VEND APPROVED =>	VEND FAILURE*
NEGATIVE VEND REQUEST =>	NEGATIVE VEND DENIED*	
NEGATIVE VEND REQUEST =>	NEGATIVE VEND APPROVED =>	NEGATIVE VEND SUCCESS*
NEGATIVE VEND REQUEST =>	NEGATIVE VEND APPROVED =>	NEGATIVE VEND FAILURE*
REVALUE REQUEST=>	REVALUE APPROVED/DENIED*	
SESSION COMPLETE =>	END SESSION	

*These VEND / NEGATIVE VEND / REVALUE REQUEST response sequences constitute the Vend / Negative Vend / Revalue Request states.

Below are the uninterruptable POLLed cashless device which require an informational response

from the VMC:

VMC Command & Data	Cashless Device Response	Result
POLL =>	DATA ENTRY REQUEST + DISPLAY REQUEST (optional)	
POLL =>	DATA ENTRY CANCEL	Cancelled
DATA ENTRY RESPONSE w/ FFs =>		Cancelled

Any command may be issued by the VMC at anytime providing the above command protocol is observed. There are four exceptions to this rule:

Petitioner Exhibit 1002-2820
CSC ServiceWorks – Ex. 1008
Page 96 of 270

1) VEND REQUEST, REVALUE REQUEST, and NEGATIVE VEND REQUEST response sequences may only be initiated in the Session Idle state.

2) The VMC may issue a VEND CANCEL command after issuing a VEND REQUEST, but before receiving a VEND APPROVED/DENIED response. In this case the cashless device will issue a VEND DENIED response to satisfy the original VEND REQUEST response requirement.
3) The cashless device may issue DISPLAY REQUESTs in response to POLLs at any time, if the VMC's display is available for use.
4) The RESET command is allowed at any time, it is not subject to any restrictions.

If a VMC command is received by the cashless device while it is in one of the preceding uninterruptable states, the following will occur:

The cashless device will ACK the offending command (no data response will be forthcoming). The cashless device will respond to the next poll with the "COMMAND OUT OF SEQUENCE" response (0BH).

It should be pointed out to cashless device developers that a command out of sequence will always cause the VMC to issue a RESET command to the cashless device.

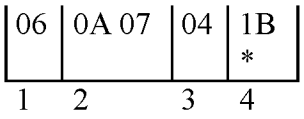
7.3.1 Multi-Message Response Format

The multi-message response format permits the cashless device to send multiple messages in response to a single command or POLL. Because all messages are of a fixed length, there is no confusion determining where one message ends and the next message begins. (The total message length is subject to the 36 byte limit imposed by Section 2 of this standard.)

For example, if a cashless device fails to correctly write a payment media after a VEND REQUEST, it may need to report:

1) VEND DENIED
2) MALFUNCTION/ERROR subcode 07h
3) SESSION CANCEL REQUEST

The multi-message response (hex) would look like this:



The first byte above (marked 1) is the VEND DENIED message. The next two bytes (marked 2) are the MALFUNCTION/ERROR message. The third and final message is the CANCEL SESSION REQUEST (marked 3). An eight bit checksum with the mode bit set (marked 4) finishes the message.

Petitioner Exhibit 1002-2821
CSC ServiceWorks – Ex. 1008
Page 97 of 270

It is important to note that the controller must service the messages in the order in which they are received. This is necessary to ensure that command protocol is maintained.

Petitioner Exhibit 1002-2822
CSC ServiceWorks – Ex. 1008
Page 98 of 270

7.3.2 Coin Mechanism Escrow Return Actions

If present, the cashless device return button is controlled by the cashless device and it is the responsibility of the cashless device to terminate a vend sequence if the return button is pressed during a vend sequence.

The reaction of the VMC to the coin mechanism escrow return will vary depending upon the state of the system at the time it is pressed. If escrow return is allowed then a coin mechanism escrow return should be interpreted as VEND CANCEL or END OF SESSION.

1) In the Enabled state, the VMC should send a READER CANCEL command to the cashless device. This allows the user to abort a pre-approved on-line authorisation request.

2) In the Session Idle state, the VMC should send a SESSION COMPLETE command to the cashless device. This will return the cashless device to the Enabled state. The escrow return may cause the system to enter the revalue state prior to the VMC sending the "SESSION COMPLETE" command.

3) In the Vend state, before the cashless device has sent a VEND APPROVED or a VEND DENIED, the VMC should send a VEND CANCEL command to the cashless device. This will cancel the vend and cause the cashless device to refund the payment media if necessary.

4) In all other cases, no message is sent from the VMC to the cashless device.

Petitioner Exhibit 1002-2828
CSC ServiceWorks – Ex. 1008
Page 99 of 270

TABLE 1: COMMANDS & RESPONSES

Command	Code	Sub-command / Data	Response	VMC / Cashless Level Support
Reset	10H 60H	(none)	No Data *	(Level 01+)
Setup	11H 61H	00H - Config Data	01H - Reader Config Data	(Level 01+)
		01H - Max/Min Prices	No Data *	(Level 01+)
Poll	12H 62H	(none)	00H - Just Reset	(Level 01+)
			01H - Reader Config Data	(Level 01+)
			02H - Display Request	(Level 01+)
			03H - Begin Session	(Level 01+)
			04H - Session Cancel Request	(Level 01+)
			05H - Vend Approved	(Level 01+)
			06H - Vend Denied	(Level 01+)
			07H - End Session	(Level 01+)
			08H - Cancelled	(Level 01+)
			09H - Peripheral ID	(Level 01+)
			0AH - Malfunction / Error	(Level 01+)
			0BH - Cmd Out Of Sequence	(Level 01+)
			0DH - Revalue Approved	(Level 02+) (option)
			0EH - Revalue Denied	(Level 02+) (option)
			0FH - Revalue Limit Amount	(Level 02+) (option)
			10H - User File Data	(Level 02) **
			11H - Time/Date Request	(Level 02+) (option)
			12H - Data Entry Request	(Level 03+) (option)
				(Level 03+) (option)
			13H - Data Entry Cancel	(For Future Use)
			14H -1AH	(Level 03+) (option)
			1BH - FTL REQ TO RCV	(Level 03+) (option)
			1CH - FTL RETRY / DENY	(Level 03+) (option)
			1DH - FTL SEND BLOCK	(Level 03+) (option)
			1EH - FTL OK TO SEND	(Level 03+) (option)
			1FH - FTL REQ TO SEND	(For Future Use)
				(Level 01+)

Petitioner Exhibit 1002-2824
CSC ServiceWorks – Ex. 1008
Page 100 of 270

			20H - FEH FFH - Diagnostic Response	
Vend	13H 63H	00H - Vend Request	05H - Vend Approved 06H - Vend Denied	(Level 01+) (Level 01+)
		01H - Vend Cancel	06H - Vend Denied	(Level 01+)
		02H - Vend Success	No Data *	(Level 01+)
		03H - Vend Failure	No Data *	(Level 01+)
		04H - Session Complete	07H - End Session	(Level 01+)
		05H - Cash Sale	No Data *	(Level 01+)
		06H - Negative Vend Request	05H – Vend Approved 06H – Vend Denied	(Level 03+) option) (Level 03+) (option)
Reader	14H 64H	00H - Reader Disable	No Data *	(Level 01+)
		01H - Reader Enable	No Data *	(Level 01+)
		02H - Reader Cancel	08H - Cancelled	(Level 01+)
		03H - Data Entry Response	No Data *	(Level 03+) (option)
Revalue (option)	15H 65H	00H - Revalue Request	0DH - Revalue Approved 0EH - Revalue Denied	(Level 02+) (option) (Level 02+) (option)
		01H - Revalue Limit Request	0FH - Revalue Limit Amount 0EH - Revalue Denied	(Level 02+) (option) (Level 02+) (option)
Expansion	17H 67H	00H - Request ID	09H - Peripheral ID	(Level 01+)
		01H - Read User File	10H - User File Data	(Level 02) **
		02H - Write User File	No Data *	(Level 02) **
		03H - Write (option) Time/Date	No Data *	(Level 02+) (option)
		04H - Optional Feature Enabled	No Data	(Level 03+)
		FAH - FTL (option) REQ TO RCV	1DH - SEND BLOCK 1CH - RETRY / DENY	(Level 03+) (option) (Level 03+) (option)
		FBH - FTL (option) RETRY / DENY	No Data	(Level 03+) (option)
		FCH - FTL (option) SEND BLOCK	No Data	(Level 03+) (option)
		FDH - FTL (option) OK TO SEND	1DH - SEND BLOCK	(Level 03+) (option)
		FEH - FTL (option) REQ TO SEND	1EH - OK TO SEND 1CH - RETRY/DENY	(Level 03+) (option) (Level 03+) (option)
		FFH - Diagnostics	FFH - Diagnostic Response	(Level 01+)

* No Data response = peripheral just responds with ACK or NAK

**** Obsolete Command – Do not use for new designs. Use EXPANSION - Diagnostics.**

The term (option) indicates that the command/response is a feature enabled by option bits.

Petitioner Exhibit 1002-2825
CSC ServiceWorks – Ex. 1008
Page 101 of 270

NOTE: Cashless device responses which are part of request / response sequences are listed more than once in the above table since the cashless device may respond either immediately to the request (within 5 milliseconds) or to a later POLL.

7.4 VMC/ Cashless Device Command/Response Formats

In the following section, the term "Reader" will indicate either Cashless Device #1 or #2.

7.4.1 Reset and Initialising

RESET **(10H / 60H)**

Reader response:

No Data response

If this command is received by a cashless device it should terminate any ongoing transaction (with an appropriate credit adjustment, if appropriate), eject the payment media (if applicable), and go to the Inactive state.

All Level 02 and above VMCs must follow the RESET command with the following cashless device initializing sequence: (Any new Level 01 VMCs are recommended to follow the sequence.)

Note that the example shows commands for Cashless Device #1 (10H) only. They would be the same for Cashless Device #2 (address 60H).

POLL – 12h

To obtain "JUST RESET" response

SETUP CONFIGURATION DATA – 11 00h

To send the VMC's configuration data and obtain the cashless device's data

SETUP MAX/MIN PRICE – 11 01h

To send the maximum and minimum prices in the VMC. These prices must be sent as Level 01/02 16 bit credit.

Petitioner Exhibit 1002-2826
CSC ServiceWorks – Ex. 1008
Page 102 of 270

EXPANSION REQUEST ID – 17 00h

To obtain additional cashless device information and options (options in Level 03+ only)

EXPANSION ENABLE OPTIONS – 17 04h (Level 03+ only)

To enable desired options

SETUP MAX/MIN PRICE – 11 01h (Level 03+ and option bits 1 & 2 only)

If 32 bit currency option and/or multi currency – multi lingual is enabled (i.e. bits 1 & 2 of expansion enable options), perform **SETUP MAX/MIN PRICE** again to get 32 bit credit and/or user currency – user language (this conditions will be known as EXPANDED CURRENCY MODE in the rest of the document).

READER ENABLE – 14 01h

To enable cashless device (if desired)

7.4.2 SETUP - Config Data

SETUP (11H / 61H)	Config Data (00H) Y1	VMC Feature Level Y2	Columns on Display Y3	Rows On Display Y4	Display Info Y5

Y1 : Configuration data.
VMC is sending its configuration data to reader.

Y2 : VMC Feature Level.
Indicates the feature level of the VMC. The available feature levels are:

01 - The VMC is not capable or will not perform the advanced features as specified in Table 1: COMMANDS & RESPONSES following Section 7.3.2. The reader will not provide advanced information to the VMC, but can do the advanced features internally (transparently to the VMC). The reader has no revaluation capability.

02 - The VMC is capable and willing to perform the advanced features as specified in Table 1: COMMANDS & RESPONSES following Section 7.3.2. The reader will provide advanced information to the VMC (if possible) and will not do the advanced features internally.

03 - The VMC is able to support level 02, but also supports some or all of the optional features listed in the EXPANSION ID command (i.e., file transfer, 32 bit credit, multi-currency / language features, negative vend, and / or data entry).

Y3 : Columns on Display. The number of columns on the display. Set to 00H if the display is not available to the reader.

Petitioner Exhibit 1002-2827
CSC ServiceWorks – Ex. 1008
Page 103 of 270

Y4 : Rows on Display.
The number of rows on the display

Y5 : Display Information - xxxxxyyy
xxxxx = Unused
yyy = Display type
000 : Numbers, upper case letters, blank and decimal point.
001 : Full ASCII
010-111: Unassigned

Reader Response:

Reader Config Data (01H) Z1	Reader Feature Level Z2	Country Code High Z3	Country Code Low Z4	Scale Factor Z5	Decimal Places Z6	Application Maximum Response Time Z7	Miscellaneous Options Z8

Z1 : READER - Configuration data.
Indicates the payment media reader is responding to a SETUP – Configuration data request from the VMC.

Z2 : Reader Feature Level.
Indicates the feature level of the reader. Currently feature levels are:

01 - The reader is not capable or will not perform the advanced features as specified in Table 1: COMMANDS & RESPONSES following Section 7.3.2. The reader will not provide advanced information to the VMC, but can do the advanced features internally (transparently to the VMC). The reader has no revaluation capability.

02 - The reader is capable and willing to perform the advanced features as specified in Table 1: COMMANDS & RESPONSES following Section 7.3.2. The reader will provide advanced information to the VMC (if possible) and will not do the advanced features internally.

03 - The reader is able to support level 02, but also supports some or all of the optional features listed in the EXPANSION ID command (i.e., file transfer, 32 bit credit, multi-currency / language features, negative vend, and / or data entry).

Z3-Z4 : Country / Currency Code - packed BCD.
The packed BCD country / currency code of the reader can be sent in two different forms depending on the value of the left most BCD digit.

If the left most digit is a 0, the International Telephone Code is used to indicate the country that the reader is set-up for. For example, the USA code is 00 01H (Z3 = 00 and Z4 = 01).

If the left most digit is a 1, the latest version of the ISO 4217 numeric currency code is used (see Appendix A1). For example, the code for the US dollar is 18 40H (Z2 = 18 and Z3 = 40) and for the Euro is 1978 (Z3 = 19 and Z4 = 78). Use FFFFh if the country code in unknown.

Petitioner Exhibit 1002-2828
CSC ServiceWorks – Ex. 1008
Page 104 of 270

For level 3 cashless devices, it is mandatory to use the ISO 4217 numeric currency code (see Appendix A1).

Z5 : Scale Factor.
The multiplier used to scale all monetary values transferred between the VMC and the reader.

Z6 : Decimal Places.
The number of decimal places used to communicate monetary values between the VMC and the payment media reader.

All pricing information sent between the VMC and the payment media reader is scaled using the scale factor and decimal places. This corresponds to:

$$ActualPrice = P \cdot X \cdot 10^{-Y}$$

where P is the scaled value send in the price bytes, and X is the scale factor, and Y is the number of decimal places. For example if there are 2 decimal places and the scale factor is 5, then a scaled price of 7 will mean an actual of 0.35.

Z7 : Application Maximum Response Time - seconds.
The maximum length of time a reader will require to provide a response to any command from the VMC. The value reported here supercedes the payment reader's default NON-RESPONSE time defined in section 7.5 if the value reported here is greater.

Z8 : Miscellaneous Options – xxxxyyyy

xxxx: Unused (must be set to 0)

yyyy: Option bits

b0=0: The payment media reader is NOT capable of restoring funds to the user's payment media or account. Do not request refunds.

b0=1: The payment media reader is capable of restoring funds to the user's payment media or account. Refunds may be requested.

b1=0: The payment media reader is NOT multivend capable.

Terminate session after each vend.

b1=1: The payment media reader is multivend capable. Multiple items may be purchased within a single session.

b2=0: The payment media reader does NOT have a display.

b2=1: The payment media reader does have its own display.

b3=0: The payment media reader does NOT support the VEND/CASH SALE subcommand.

b3=1: The payment media reader does support the VEND/CASH SALE subcommand.

b4-b7=0 **Any future options must be covered by the EXPANSION COMMAND option bits.**

Petitioner Exhibit 1002-2820
CSC ServiceWorks – Ex. 1008
Page 105 of 270

7.4.3 SETUP – Max / Min Prices

SETUP (11H / 61H)	Max / Min Prices (01H) Y1	Maximum Price Y2-Y3	Minimum Price Y4-Y5

Level 01 / 02 / 03 Readers

Y1 : Max / Min prices
Indicates the VMC is sending the price range to the reader.

Y2 - Y3 : Maximum Price – scaled
This information should be sent as soon as the VMC prices have been established and any time there is a change in the maximum price, If the VMC does not know the maximum price, FFFFh should be sent.

Y4 -Y5 : Minimum Price – scaled
This information should be sent as soon as the VMC prices have been established and any time there is a change in the minimum price. If the VMC does not know the minimum price, 0000h should be sent.

SETUP (11H / 61H)	Max / MinPrices (01H) Y1	Maximum Price Y2-Y5	Minimum Price Y6-Y9	Currency Code Y10-Y11

Level 03 (EXPANDED CURRENCY MODE) Readers

Y1 : Max / Min prices
Indicates the VMC is sending the price range to the reader.

Y2 – Y5 : Maximum Price – scaled
This information should be sent as soon as the VMC prices have been established and any time there is a change in the maximum price, If the VMC does not know the maximum price, FFFFFFFFh should be sent.

Y6 –Y9 : Minimum Price – scaled
This information should be sent as soon as the VMC prices have been established and any time there is a change in the minimum price. If the VMC does not know the minimum price, 00000000h should be sent.

Y10-Y11 Currency Code
The currency code used during this command per ISO 4217 (see Appendix A1). The value is configured as packed BCD with the leading digit a 1 (one). For example, the code for the US dollar would be 1840 (Z10 = 18 and Z11 = 40). and for the Euro is 1978 (Z10 = 19 and Z11 = 78).

Reader response:

Petitioner Exhibit 1002-2830
CSC ServiceWorks – Ex. 1008
Page 106 of 270

No Data response

7.4.4 POLL

POLL (12H / 62H)

The POLL command is used by the VMC to obtain information from the payment media reader. This information may include user actions (CANCEL SESSION REQUEST), hardware malfunctions (MALFUNCTION /ERROR), software malfunctions (COMMAND OUT OF SEQUENCE) or information explicitly requested by the controller (READER CONFIGURATION DATA). An ACK response indicates that no error states exist, and either no information request is pending or pending information is not yet ready for transmission.

In addition to an ACK, the VMC may receive the following POLL responses from the payment media reader.

Petitioner Exhibit 1002-2831
CSC ServiceWorks – Ex. 1008
Page 107 of 270

Reader responses:

Just Reset (00H) Z1

Z1 : JUST RESET
Indicates the payment media reader has been reset.
Note: the difference between ACK and JUST RESET responses is:
00H 00H* =JUST RESET
00H* =ACK
*mode bit=1

Reader Config Info (01H) Z1	Reader Feature Level Z2	Country Code High Z3	Country Code Low Z4	Scale Factor Z5	Decimal Places Z6	Application Maximum Response Time Z7	Miscellaneous Options Z8

See paragraph 7.4.2 for a detailed explanation of this response.

Display Request (02H) Z1	Display Time Z2	Display Data Z3-Z34

Z1 : DISPLAY REQUEST
The payment media reader is requesting a message to be displayed on the VMC's display.

Z2 : Display Time - 0.1 second units
The requested display time. Either the VMC or the payment media reader may overwrite the message before the time has expired.

Z3-Z34 : Display Data – ASCII
The message to be displayed. Formatting (leading and/or trailing blanks) is the responsibility of the payment media reader.

The number of bytes must equal the product of Y3 and Y4 up to a maximum of 32 bytes in the setup/configuration command.

Petitioner Exhibit 1002-2832
CSC ServiceWorks – Ex. 1008
Page 108 of 270

Begin Session (03H)	Funds Available
Z1	Z2-Z3

Level 01 Readers

Z1 : BEGIN SESSION (**level 01 readers**)
Allow a patron to make a selection, but do not dispense product until funds are approved.

Z2-Z3 : Funds Available - scaled

a. Lesser of the user's payment media or account balance or FFFEh units.

b. Not yet determined - FFFFh.

Begin Session (03H)	Funds Available	Payment media ID	Payment Type	Payment Data
Z1	Z2-Z3	Z4-Z7	Z8	Z9-Z10

Level 02 / 03 Readers

Z1 : BEGIN SESSION (**level 02/03 readers**)
Allow a patron to make a selection, but do not dispense product until funds are approved.

Z2-Z3 : Funds Available – scaled

a. Lesser of the user's payment media or account balance or FFFEh units.

b. Not yet determined - FFFFh.

Z4-Z7 : Payment media ID.
00000000h-FFFFFFFEh=Payment media identification number. FFFFFFFFh = unknown payment media ID.

Z8 : Type of payment:
00xxxxxxb = normal vend card (refer EVA-DTS Standard, Appendix A.1.1 Definitions)
x1xxxxxxb = test media
1xxxxxxxb = free vend card
xx000000b -0 VMC default prices.
xx000001b -1 User Group (Z9 = EVA-DTS Element DA701)
Price list number (Z10 = EVA-DTS Element LA101)*
xx000010b -2 User Group (Z9 = EVA-DTS Element DA701)
Discount group index (Z10 = EVA-DTS Element MA403)
xx000011b -3 Discount percentage factor (Z9=00, Z10 = 0 to 100**,

Petitioner Exhibit 1002-2838
CSC ServiceWorks – Ex. 1008
Page 109 of 270

report as positive value in EVA-DTS Element MA404)

xx000100b -4 Surcharge percentage factor (Z9=00, Z10 = 0 to 100**, report as negative value in EVA-DTS Element MA404)

* User Group is a segmentation of all authorized users. It allows selective cost allocation. A User Group usually has no direct relation to a price list.
Price Lists are tables of prices. Each Price List contains an individual price for each product.
Discount Group indicates the Price List on which the Percentage Factor will be applied.
If the User Group, the Price List or Discount Group is unknown

by the VMC, the normal prices are used (Z8 is defaulted to 00h).

Minimum value for Z9 and Z10 is 0.

** Percentages are expressed in binary (00 to 64h)

Note:
These functions may NOT be supported by all VMCs.

Z9-Z10 : Payment data as defined above.

Begin Session (03H)	Funds Available	Payment media ID	Payment Type	Payment Data	User Language	User Currency Code	Card Options
Z1	Z2-Z5	Z6-Z9	Z10	Z11-Z12	Z13-Z14	Z15-Z16	Z17

Level 03 (EXPANDED CURRENCY MODE) Readers

Z1 : BEGIN SESSION (**level 03 readers / EXPANDED CURRENCY MODE**)
Allow a patron to make a selection, but do not dispense product until funds are approved.

Z2-Z5 : Funds Available – scaled
a. Lesser of the user's payment media or account balance or FFFFFFFEh units.
b. Not yet determined - FFFFFFFFh.

Z6-Z9 : Payment media ID.
00000000h-FFFFFFFEh=Payment media identification number. FFFFFFFFh = unknown payment media ID.

Petitioner Exhibit 1002-2834 CSC ServiceWorks – Ex. 1008
Page 110 of 270

Z10 : Type of payment:
00xxxxxxb = normal vend card (refer EVA-DTS Standard, Appendix A.1.1 Definitions)
x1xxxxxxb = test media
1xxxxxxxb = free vend card
xx000000b -0 VMC default prices.
xx000001b -1 User Group (Z11 = EVA-DTS Element DA701)
Price list number (Z12 = EVA-DTS Element LA101)*
xx000010b -2 User Group (Z11 = EVA-DTS Element DA701)
Discount group index (Z12 = EVA-DTS Element MA403)
xx000011b -3 Discount percentage factor (Z11=00, Z12 = 0 to 100**, report as positive value in EVA-DTS Element MA404)
xx000100b -4 Surcharge percentage factor (Z11=00, Z12 = 0 to 100**, report as negative value in EVA-DTS Element MA404)

* User Group is a segmentation of all authorized users. It allows selective cost allocation. A User Group usually has no direct relation to a price list.
Price Lists are tables of prices. Each Price List contains an individual price for each product.
Discount Group indicates the Price List on which the Percentage Factor will be applied.
If the User Group, the Price List or Discount Group is unknown

by the VMC, the normal prices are used (Z10 is defaulted to

00h).

Minimum value for Z11 and Z12 is 0.

** Percentages are expressed in binary (00 to 64h)

Note:
These functions may NOT be supported by all VMCs.

Z11-Z12: Payment data as defined above.

Z13-Z14 User language to use during this session (2 ASCII characters per ISO 639:latest version). The user language is read from the patrons card and, if supported, should be used instead of the VMC default language (taken according to the setup command International Telephone code) up to the next "session complete". If the VMC is not able to support this language, the default setting should be used.

Z15-Z16 User currency code to use during this session per ISO 4217 (see Appendix A1). The value is configured as packed BCD with the leading digit a 1 (one). For example, the code for the US dollar would be 1840 (Z15 = 18 and Z16 = 40).

Petitioner Exhibit 1002-2835
CSC ServiceWorks – Ex. 1008
Page 111 of 270

and for the Euro is 1978 (Z6 = 19 and Z7 = 78).

Z17 Card options (overrides any previous default settings for reader)

- b0=0: The VMC displays the credit if it is programmed to do so
- b0=1: The VMC **must not display** the credit (privacy purpose – user option)
- b1=0: The actual inserted patrons card has no refund capability
- b1=1: The actual inserted patrons card has refund capability (Note: a reader with refund capability may be used with both type of cards)
- b2=0 The actual inserted patrons card has no revalue capability
- b2=1 The actual inserted patrons card has revalue & negative vend capability
- b3-b7: Reserved for future extensions (unused bits must be set to 0)

Refund means the ability to put money back on the inserted patrons card up to the value of the last transaction. Revalue means the ability to put money back on the inserted patrons card up to any value.

The card reader will define the currency type at the beginning of each card session. **The currency type will be used for all following transactions in that session. If the VMC does not support this currency type, it will end the session.**

Session Cancel Request (04H)
Z1

Z1 : SESSION CANCEL REQUEST
The payment media reader is requesting the VMC to cancel the session. The VMC should initiate an eventual SESSION COMPLETE. This response is sent to the VMC whenever the payment media is removed or a request for removal from the reader is made by the user (e.g. if a return button on the reader is pressed).

Vend Approved (05H)	Vend Amount
Z1	Z2-Z3

Level 01 / 02 / 03 Readers

Refer to paragraph 7.4.5 for detailed explanation.

Vend Approved (05H)	Vend Amount

Petitioner Exhibit 1002-2836
CSC ServiceWorks – Ex. 1008
Page 112 of 270

Z1	Z2-Z5

Level 03 (EXPANDED CURRENCY MODE) Readers

Refer to paragraph 7.4.5 for detailed explanation.

Vend Denied (06H) Z1

Refer to paragraph 7.4.5 for detailed explanation.

End Session (07H) Z1

Refer to paragraph 7.4.9 for detailed explanation.

Cancelled (08H) Z1

Refer to paragraph 7.4.14 for detailed explanation.

Peripheral ID (09H) Z1	Manufacturer Code Z2-Z4	Serial Number Z5-Z16	Model Number Z17-Z28	Software Version Z29-Z30

Level 01 / 02 / 03 Readers (If VMC indicates Level 01 or 02)

Z1 : PERIPHERAL ID
Reader is sending peripheral ID information.

Z2 - Z4 : Manufacturer Code - ASCII
Identification code for the equipment supplier. Currently defined codes are listed in the **EVA** document entitled "***European Vending Association Data Transfer Standard***" (**EVA-DTS**), the Audit Data Lists section, sub-section 2, "Manufacturer Codes".

Z5-Z16 : Serial Number – ASCII
Factory assigned serial number.

Z17-Z28 : Model Number - ASCII

Petitioner Exhibit 1002-2837
CSC ServiceWorks – Ex. 1008
Page 113 of 270

Manufacturer assigned model number.

Z29-Z30 : Software Version - packed BCD
Current software version.

Peripheral ID (09H) Z1	Manufacturer Code Z2-Z4	Serial Number Z5-Z16	Model Number Z17-Z28	Software Version Z29-Z30	Optional Feature bits Z31 - Z34

Level 03 Readers (If VMC indicates Level 03)

Z1 : PERIPHERAL ID
Reader is sending peripheral ID information.

Z2 - Z4 : Manufacturer Code - ASCII
Identification code for the equipment supplier. Currently defined codes are listed in the **EVA** document entitled "***European Vending Association Data Transfer Standard***" (**EVA-DTS**), the Audit Data
Lists section, sub-section 2, "Manufacturer Codes".

Z5-Z16 : Serial Number – ASCII
Factory assigned serial number.

Z17-Z28 : Model Number - ASCII
Manufacturer assigned model number.

Z29-Z30 : Software Version - packed BCD
Current software version.

Z31- Z34 Optional Feature Bits. Each of the 32 bits indicate an optional feature availability. Bits should be sent in descending order, i.e. bit 31 is sent first and bit 0 is sent last. Options **must be enabled by the VMC** using the Expansion Optional Feature Bit Enable (17H-04H) command and **all features are disabled after a reset**. Currently defined options are:

b0 - File Transport Layer supported
b1 - 0 = 16 bit monetary format, 1 = 32 bit monetary format
b2 - multi currency / multi lingual
b3 - negative vend
b4 - data entry
b5 to b31 not used (should be set to 0)

Note: If 32 bit monetary format (b1) and or multi currency / multi lingual (b2) options are enabled, this condition will be known as **EXPANDED CURRENCY MODE** in the rest of the document.

Petitioner Exhibit 1002-2838
CSC ServiceWorks – Ex. 1008
Page 114 of 270

Malfunction / Error	Error Code
(0AH) Z1	Z2

Z1 : MALFUNCTION/ERROR
The payment media reader is reporting a malfunction or error.

Z2 : Error Code – xxxxyyyy

xxxx	error types
0000:	Payment media Error1
0001:	Invalid Payment media1
0010:	Tamper Error1
0011:	Manufacturer Defined Error1
0100:	Communications Error2
0101:	Reader Requires Service2
0110:	Unassigned2
0111:	Manufacturer Defined Error2
1000:	Reader Failure3
1001:	Communications Error3
1010:	Payment media Jammed3
1011:	Manufacturer Defined Error
1100:	Refund error – internal reader credit lost
1101-1111:	Unassigned

1 Transient error - Reported once
2 Non-transient error - Reported every POLL until cleared. Reader still functional.
3 Non-transient error - Reported every POLL until cleared. Reader not presently functional.

yyyy = Manufacturer defined subcode

Transient Error Handling
The error will be reported to the VMC until it has been ACKnowledged. The error state will be cleared in the reader, and normal operations will continue.

Non-transient Error Handling
The error will be reported to the VMC at each POLL as long as it exists. If the reader is still functional, multi-message responses will allow normal responses in addition to the error report.

Petitioner Exhibit 1002-2839
CSC ServiceWorks – Ex. 1008
Page 115 of 270

Note: Refund error is sent from the media reader when it is not able to refund money to the payment media following a failed or cancelled vend. The reader internally cancels the credit and the credit is lost.

Command Out of Sequence (0BH) Z1

Level 01 Readers

Z1 : COMMAND OUT OF SEQUENCE (Level 01 readers)
The payment media reader has received a command that is not executable in its current state, or that violates one of the uninterruptable sequences. The offending command should be ACKed but not acted upon the reader. The VMC will send the RESET command to the reader upon reception of this response. Note that the reader will continue with any credit update process prior to resetting.

Command Out of Sequence (0BH) Z1	Status Z2

Level 02 / 03 Readers

Z1 : COMMAND OUT OF SEQUENCE. (Level 02/03 readers)
The payment media reader has received a command that is not executable in its current state, or that violates one of the uninterruptable sequences. The offending command should be ACKed but not acted upon the reader. The VMC will send the RESET command to the reader upon reception of this response. Note that the reader will continue with any credit update process prior to resetting.

Z2 : Status
The state of the payment media reader.
01: Inactive state
02: Disabled state
03: Enabled state
04: Session idle state
05: Vend state
06: Revalue state
07: Negative Vend state

Revalue

Petitioner Exhibit 1002-2840
CSC ServiceWorks – Ex. 1008
Page 116 of 270

Approved (0DH) Z1

Level 02 / 03 Readers

Refer to paragraph 7.4.16 for detailed explanation.

Revalue Denied (0EH) Z1

Level 02 / 03 Readers

Refer to paragraph 7.4.16 for detailed explanation.

Revalue Limit Amount (0FH) Z1	Revalue Limit Amount Z2-Z3

Level 02 / 03 Readers

Refer to paragraph 7.4.17 for detailed explanation.

Petitioner Exhibit 1002-2841
CSC ServiceWorks – Ex. 1008
Page 117 of 270

Revalue Limit Amount (0FH) Z1	Revalue Limit Amount Z2-Z5

Level 03 (EXPANDED CURRENCY MODE) Readers

Refer to paragraph 7.4.17 for detailed explanation.

User File Data (10H) Z1	Number of User File Z2	Length Of User File Z3	User Data Z4-Zn

Level 02 Readers

Obsolete Response – Do not use for new designs!! (Use EXPANSION – Diagnostics)

Refer to paragraph 7.4.19 for detailed explanation.

Time/Date Request (11H) Z1

Level 02 / 03 Readers

Z1 : TIME DATE REQUEST
In certain circumstances it will be necessary to synchronize the real time clock of the card reader with real time clock of the VMC. The card reader will respond with TIME/DATE REQUEST to a POLL command of the VMC. The VMC will follow with the EXPANSION-WRITE TIME/DATE FILE to the card reader. Refer to paragraph 7.4.19.

Petitioner Exhibit 1002-2842
CSC ServiceWorks – Ex. 1008
Page 118 of 270

Data Entry Request Response (12H) Z1	Data Entry Length and Repeat Bit Z2

Level 03 Readers (if Data Entry option enabled)

Z1 : DATA ENTRY REQUEST
The reader is making a DATA ENTRY REQUEST.

Z2 : DATA ENTRY LENGTH and REPEAT BIT
rnnnnnnnn
r – Repeat Bit (0 = initial request / 1 = repeated requests
nnnnnnn – number of requested characters / keys

Depending on the type of data being entered, it is a higher level system decision on whether or not the data is displayed on either the vending machine or card reader. If the data is not displayed (a recommendation for certain types of sensitive data) the vending machine or card reader display can still be optionally used to indicate a prompt and/or representation of the data entered for user feedback (i.e., asterisks *****).

If the card reader uses the vending machine's display for Data Entry information, it **must concatenate** the DATA ENTRY REQUEST Response (12H) with the DISPLAY REQUEST response (02H). Upon receipt of the response pair, the vending machine controller will give its display to the card reader for the duration of the Data Entry session plus the amount of time specified in the Z2 Display Time following the end of the session (regardless of a normal or cancelled session). In essence, the vending machine controller will not write anything to its display during the Data Entry session plus the Z2 time. The reader will be able to update the Data Entry information on the vending machine's display by sending additional DISPLAY REQUEST responses during the Data Entry session.

Please see additional DATA ENTRY procedures in Section 7.4.15.

Data Entry Cancel (13H) Z1

Level 03 Readers (if Data Entry option enabled)

Z1 : DATA ENTRY CANCEL
The user has pushed the reader's RETURN button before completing the DATA

ENTRY. The VMC should terminate all DATA ENTRY activity in progress.

Petitioner Exhibit 1002-2848
CSC ServiceWorks – Ex. 1008
Page 119 of 270

FTL
REQ TO RCV
(1BH)
Z1

Level 03 Readers (if File Transport Layer option enabled)

Z1 : **FTL** REQ TO RCV
The reader is requesting to receive data from a device or VMC.

Z2 : **FTL** Destination Address
The destination address of the response as defined in Section 2.6.

Z3 : **FTL** Source Address (Reader = 10H / 60H)
The source address of the response as defined in Section 2.6.

Z4 : **FTL** File ID
The type of information desired as defined in Section 2.6.

Z5 : **FTL** Maximum Length
The total number of blocks in the file as defined in Section 2.6.

Z6 : **FTL** Control
Data transfer control information as defined in Section 2.6.

FTL
RETRY/DENY
(1CH)
Z1

Level 03 Readers (if File Transport Layer option enabled)

Z1 : **FTL** RETRY / DENY
The reader is requesting a device or VMC to retry or deny the last FTL command.

Z2 : **FTL** Destination Address
The destination address of the response as defined in Section 2.6.

Z3 : **FTL** Source Address (Reader = 10H / 60H)
The source address of the response as defined in Section 2.6.

Z4 : **FTL** Retry Delay
The retry delay as defined in Section 2.6.

Petitioner Exhibit 1002-2844
CSC ServiceWorks – Ex. 1008
Page 120 of 270

FTL
SEND
BLOCK
(1DH)
Z1

Level 03 Readers (if File Transport Layer option enabled)

Z1 : **FTL** SEND BLOCK
The reader is sending a block of data (maximum of 31 bytes) to a device or VMC.

Z2 : **FTL** Destination Address
The destination address of the response as defined in Section 2.6.

Z3 : **FTL** Block #
The sequential number of the block as defined in Section 2.6.

Z4- Z34 : **FTL** Data (maximum of 31 bytes)
The actual data portion of the block as defined in Section 2.6.

FTL
OK TO SEND
(1EH)
Z1

Level 03 Readers (if File Transport Layer option enabled)

Z1 : **FTL** OK TO SEND
The reader is indicating that it is OK for the device or VMC to send it data.

Z2 : **FTL** Destination Address
The destination address of the response as defined in Section 2.6.

Z3 : **FTL** Source Address (Reader = 10H / 60H)
The source address of the response as defined in Section 2.6.

Petitioner Exhibit 1002-2845
CSC ServiceWorks – Ex. 1008
Page 121 of 270

FTL REQ TO SEND (1FH) Z1

Level 03 Readers (if File Transport Layer option enabled)

Z1 : **FTL** REQ TO SEND
The reader is requesting to send data to a device or VMC.

Z2 : **FTL** Destination Address
The destination address of the response as defined in Section 2.6.

Z3 : **FTL** Source Address (Reader = 10H / 60H)
The source address of the response as defined in Section 2.6.

Z4 : **FTL** File ID
The type of information desired as defined in Section 2.6.

Z5 : **FTL** Maximum Length
The total number of blocks in the file as defined in Section 2.6.

Z6 : **FTL** Control
Data transfer control information as defined in Section 2.6.

Diagnostics Response (FFH) Z1	User Defined Data Z2-Zn

Refer to paragraph 7.4.28 for detailed explanation.

7.4.5 VEND - Request

	Vend Request (00H) Y1	Item Price Y2-Y3	Item Number Y4-Y5
Vend (13H / 63H)			

Level 01 / 02 / 03 Readers

Y1 : VEND REQUEST
The patron has made a selection. The VMC is requesting vend approval from the payment media reader before dispensing the product.

Y2-Y3 : Item Price - scaled
The price of the selected product.

Petitioner Exhibit 1002-2846
CSC ServiceWorks – Ex. 1008
Page 122 of 270

Y4-Y5 : Item Number
The item number of the selected product. This number is defined by the manufacturer, and set to FFFFh for undefined or not implemented.

Reader response:

Vend Approved (05H) Z1	Vend Amount Z2-Z3

Z1 : VEND APPROVED
Allow the selected product to be dispensed.

Z2-Z3 : Vend Amount - scaled
This is the amount deducted from the user's payment media or account. This may not match the amount specified in the VEND REQUEST command; it may be surcharged or discounted.
FFFFh - an electronic token was used.

NOTE: The VMC must use Vend Amount to update the credit on the screen. The Reader must fill this field with the used amount for the transaction.

Vend Denied (06H) Z1

Z1 : VEND DENIED
Approval denied for the patron's selection. Do not dispense any products.

	Vend Request (00H) Y1	Item Price Y2-Y5	Item Number Y6-Y7
Vend (13H / 63H)			

Level 03 (EXPANDED CURRENCY MODE) Readers

Y1 : VEND REQUEST
The patron has made a selection. The VMC is requesting vend approval from the payment media reader before dispensing the product.

Y2-Y5 : Item Price – scaled
The price of the selected product.

Y6-Y7 : Item Number
The item number of the selected product. This number is defined by the

Petitioner Exhibit 1002-2847
CSC ServiceWorks – Ex. 1008
Page 123 of 270

manufacturer, and set to FFFFh for undefined or not implemented.

Reader Response:

Vend Approved (05H) Z1	Vend Amount Z2-Z5

Level 03 (EXPANDED CURRENCY MODE) Readers

Z1 : VEND APPROVED
Allow the selected product to be dispensed.

Z2-Z5 : Vend Amount - scaled
This is the amount deducted from the user's payment media or account. This may not match the amount specified in the VEND REQUEST command; it may be surcharged or discounted.
FFFFFFFFh - an electronic token was used.

NOTE: The VMC must use Vend Amount to update the credit on the screen. The Reader must fill this field with the used amount for the transaction.

Petitioner Exhibit 1002-2848
CSC ServiceWorks – Ex. 1008
Page 124 of 270

7.4.6 VEND - Cancel

Vend (13H / 63H)	Vend Cancel (01H) Y1

Y1 : VEND CANCEL
This command can be issued by the VMC to cancel a VEND REQUEST command before a VEND APPROVED/DENIED has been sent by the payment media reader. The payment media reader will respond to VEND CANCEL with a VEND DENIED and return to the Session Idle state.

Reader response:

Vend Denied (06H) Z1

See paragraph 7.4.5 for explanation.

7.4.7 VEND - Success

Vend (13H / 63H)	Vend Success (02H) Y1	Item Number Y2-Y3

Y1 : VEND SUCCESS
The selected product has been successfully dispensed.

Y2-Y3 : Item number
The item number of the selected product. This number is defined by the manufacturer, and set to FFFFh for undefined or not implemented.

NOTE A reset between VEND APPROVED and VEND SUCCESS shall be interpreted as a VEND SUCCESS.

Reader response:

No Data response

Petitioner Exhibit 1002-2849
CSC ServiceWorks – Ex. 1008
Page 125 of 270

7.4.8 VEND - Failure

Vend (13H / 63H)	Vend Failure (03H) Y1

Y1 : VEND FAILURE
A vend has been attempted at the VMC but a problem has been detected and the vend has failed. The product was not dispensed. Funds should be refunded to user's account.

Reader response:

No Data response

Vend failure sequence

In order to ensure that a reader refunds after a Vend Failure command, the VMC must send at least a single Poll command to obtain the reader possible answers:

ACK	Refund Complete
MALFUNCTION ERROR code 1100yyyy	Refund error-internal reader credit lost
SILENCE	Refund in progress. VMC must repoll reader until ACK or Malfunction error answer for maximum NON Response time.

7.4.9 SESSION COMPLETE

Vend (13H / 63H)	Session Complete (04H) Y1

Y1 : SESSION COMPLETE
This tells the payment media reader that the session is complete and to return to the Enabled state. SESSION COMPLETE is part of a command/response sequence that requires an END SESSION response from the reader.

Reader response:

End Session (07H) Z1

Z1 : END SESSION
This command is issued in response to a SESSION COMPLETE command. The

Petitioner Exhibit 1002-2850
CSC ServiceWorks – Ex. 1008
Page 126 of 270

END SESSION response indicates the reader has returned to the Enabled state. If "END SESSION" is not received by the VMC within a the maximum application non-response time, the VMC must issue a "RESET" command.

7.4.10 CASH SALE

Vend (13H / 63H)	Cash Sale (05H) Y1	Item Price Y2-Y3	Item Number Y4-Y5

Level 01 / 02 / 03 Readers

Y1 : CASH SALE
A cash sale (cash only or cash and cashless) has been successfully completed by the VMC.

Y2-Y3 : Item Price – scaled
The price of the selected product or cash portion of the price.

Y4-Y5 : Item Number
The item number of the selected product. This number is defined by the manufacturer, and set to FFFFh for undefined or not implemented.

Note: This command is issued for cash auditing applications and is sent to the payment media reader if the SETUP/CONFIGURATION bit (b3) is enabled anytime a valid cash transaction is completed via a coin mechanism or bill validator.

Reader response:

No Data response

Vend (13H)	Cash Sale (05H) Y1	Item Price Y2-Y5	Item Number Y6-Y7	Item Currency Y8-Y9

Level 03 (EXPANDED CURRENCY MODE) Readers

Y1 : **CASH SALE**
A cash sale (cash only or cash and cashless) has been successfully completed by the VMC.

Petitioner Exhibit 1002-2851
CSC ServiceWorks – Ex. 1008
Page 127 of 270

Y2-Y5 : Item Price – scaled
The price of the selected product or cash portion of the price.

Y6-Y7 : Item Number
The item number of the selected product. This number is defined by the manufacturer, and set to FFFFh for undefined or not implemented.

Y8-Y9 : Item Currency
The currency for the item price used during the vend. This value may be converted within the reader to the readers balancing currency. The item currency is sent using the numeric code as defined in ISO 4217 (see Appendix A1). The value is configured as packed BCD with the leading digit a 1 (one). For example, the code for the US dollar would be 1840 (Z10 = 18 and Z11 = 40). and for the Euro is 1978 (Z10 = 19 and Z11 = 78).

Note: This command is issued for cash auditing applications and is sent to the payment media reader if the SETUP/CONFIGURATION bit (b3) is enabled anytime a valid cash transaction is completed via a coin mechanism or bill validator.

Reader response:

No Data response

7.4.11 Negative Vend Request

Vend (13H / 63H)	Neg.Vend Request (06H) Y1	Item Value Y2-Y3	Item Number Y4-Y5

Level 03 Reader

Y1 : NEGATIVE VEND REQUEST
The patron has inserted an item. The VMC is requesting negative vend approval from the payment media reader before accepting the returned product.

Y2-Y3 : Item value – scaled
The value of the inserted product (16 Bit).

Y4-Y5 : Item Number
The item number of the inserted product. This number is defined by the manufacturer, and set to FFFFh for undefined or not implemented.

Petitioner Exhibit 1002-2852
CSC ServiceWorks – Ex. 1008
Page 128 of 270

Reader response:

Vend Approved (05H) Z1	Vend Amount Z2-Z3

Level 03 (EXPANDED CURRENCY MODE disabled) Readers

Z1 : VEND APPROVED
Allow the returned product to be accepted, i.e. this means, the reader will be able to credit the value to the patrons card, when a vend success will follow the approved.

Z2-Z3 : Vend Amount – scaled
This is the amount of credit, which will be added to the user's payment media or account. This may not match the amount specified in the NEGATIVE VEND REQUEST command; it may be surcharged or discounted.
FFFFh - an electronic token will be credited.

Vend (13H / 63H)	Neg.Vend Request (06H) Y1	Item Value Y2-Y5	Item Number Y6-Y7

Level 03 (EXPANDED CURRENCY MODE) Readers

Y1 : NEGATIVE VEND REQUEST
The patron has inserted an item. The VMC is requesting negative vend approval from the payment media reader before accepting the returned product.

Y2-Y5 : Item value – scaled
The value of the inserted product.

Y6-Y7 : Item Number
The item number of the inserted product. This number is defined by the manufacturer, and set to FFFFh for undefined or not implemented.

Reader response:

Petitioner Exhibit 1002-2858
CSC ServiceWorks – Ex. 1008
Page 129 of 270

Vend Approved (05H) Z1	Vend Amount Z2-Z5

Level 03 (EXPANDED CURRENCY MODE) Readers

Z1 : VEND APPROVED
Allow the returned product to be accepted, i.e. this means, the reader will be able to credit the value to the patrons card, when a vend success will follow the approved.

Z2-Z5 : Vend Amount – scaled
This is the amount of credit, which will be added to the user's payment media or account. This may not match the amount specified in the NEGATIVE VEND REQUEST command; it may be surcharged or discounted.

FFFFFFFFh - an electronic token will be credited.

Vend Denied (06H) Z1

Z1 : VEND DENIED
Approval denied for the returned product. Do not accept the product or return it if possible.

Note: This command is used in the uninterruptable vend sequence like the normal REQUEST VEND and is followed by the normal responses VEND APPROVED or VEND DENIED, for the reader to confirm the credit update possibility and the final VEND SUCCESS or VEND FAILURE command to update the patron's credit.

Designers of cashless devices must pay special attention in implementing this command, especially for non locking readers. Credit should only be generated on the media upon final reception of VEND SUCCESS to avoid unwanted credit in the system.

Petitioner Exhibit 1002-2854 CSC ServiceWorks – Ex. 1008
Page 130 of 270

Designers of both the VMC and the readers have to deal with fault conditions of such a system carefully. A normal sequence description is added to the example vend sessions with hints to different application features.

Petitioner Exhibit 1002-2855
CSC ServiceWorks – Ex. 1008
Page 131 of 270

7.4.12 READER - Disable

Reader (14H / 64H)	Disable (00H) Y1

Y1 : READER DISABLE
This informs the payment media reader that it has been disabled, i.e. it should no longer accept a patron's payment media for the purpose of vending. Vending activities may be re-enabled using the READER ENABLE command. The payment media reader should retain all SETUP information.

NOTE Any transaction in progress will not be affected and should continue to its normal completion.

Reader response:

No Data response

7.4.13 READER - Enable

Reader (14H / 64H)	Enable (01H) Y1

Y1 : READER ENABLE
This informs the payment media reader that is has been enabled, i.e. it should now accept a patron's payment media for vending purposes. This command must be issued to a reader in the Disabled state to enable vending operations.

Reader response:

No Data response

Petitioner Exhibit 1002-2856
CSC ServiceWorks – Ex. 1008
Page 132 of 270

7.4.14 READER - Cancel

Reader (14H / 64H)	Cancel (02H) Y1

Y1 : READER CANCEL
This command is issued to abort payment media reader activities which occur in the Enabled state. It is the first part of a command/response sequence which requires a CANCELLED response from the reader.

Reader response:

Cancelled (08H) Z1

Z1 : CANCELLED
This is the reader's response to the READER CANCEL command from the VMC. This command comprises a command/response sequence. Its use is only appropriate in the Enabled state.

7.4.15 DATA ENTRY – Response (Key Entries)

The purpose of the overall Data Entry request / response sequence is to allow the machine user to enter data (i.e., a card validation number) using the selection buttons on the vending machine.

The DATA ENTRY request / response sequence can occur in the Enabled state only. It is the responsibility of the reader to enforce this rule.

Depending on the type of data being entered, it is a higher level system decision on whether or not the data is displayed on either the vending machine or card reader. If the data is not displayed (a recommendation for certain types of sensitive data) the vending machine or card reader display can still be optionally used to indicate a prompt and/or representation of the data entered for user feedback (i.e., asterisks *****). **Please see additional information on the vending machine's display usage for Data Entry in the DATA ENTRY REQUEST Response (12H) description in the 7.4.4 POLL section.**

The DATA ENTRY RESPONSE key entries are sent to the reader as they are pressed.

Depending on the user's speed of entry and vending machine controller cycle time, the data may

Petitioner Exhibit 1002-2857 CSC ServiceWorks – Ex. 1008
Page 133 of 270

be sent either as a digit at a time, a sub group of digits, or the entire length of digits as specified in the Z2 Data Entry Length byte in the DATA ENTRY REQUEST response. For example, if the Data Entry Length is 6 digits, but only 2 are initially (and quickly) entered, the vending machine controller will send the 2 that are available via the DATA ENTRY RESPONSE Y2-Y9 command. The balance will be sent via other DATA ENTRY RESPONSE Y2-Y9 commands when available.

It is up to the reader to merge the received DATA ENTRY RESPONSE data and optionally update the display as required. The session is ended after the VMC sends the final DATA ENTRY RESPONSE data (no SESSION COMPLETE command is required). Note that the VMC display will remain available to the reader for the amount of time requested in the previous DISPLAY REQUEST response.

If the data entry process is cancelled by the VMC for any reason, the VMC will send the DATA ENTRY RESPONSE with all data bytes (Y2-Y9) set to FFh. This will terminate the DATA ENTRY REQUEST and return the reader to the Enabled state.

For ease of command message processing, the Data Entry Data has been fixed at 8 characters (Y2-Y9). Unused bytes must be sent as 00h to pad out the entire command to byte Y9.

Reader (14H / 64H)	Data Entry Response (03H) Y1	Data Entry Data Y2-Y9

Level 03 Readers (if option enabled)

Y1 : DATA ENTRY RESPONSE
The VMC is providing a DATA ENTRY RESPONSE to the reader.

Y2-Y9 : DATA ENTRY DATA
Data should be in ASCII, one character per byte. Data should be left justified (first character / key in Y2, second in Y3, etc.). The number of data bytes must equal eight (8) and unused data bytes must be sent as 00h.

If the data entry process is cancelled by the VMC for any reason, the VMC will send this message with all DATA ENTRY data bytes set to FFh.

Petitioner Exhibit 1002-2858
CSC ServiceWorks – Ex. 1008
Page 134 of 270

Note: The reader must translate the VMC key information into the appropriate key needed for the application

Reader response:

No Data response

Note: If the reader has additional display information to send to the VMC following the DATA ENTRY RESPONSE, it should send it via a DISPLAY REQUEST response to one of the next POLL commands from the VMC.

Petitioner Exhibit 1002-2859
CSC ServiceWorks – Ex. 1008
Page 135 of 270

7.4.16 REVALUE - Request (Level 02 / 03 Readers)

Revalue (15H / 65H)	Revalue Request (00H) Y1	Revalue Amount Y2-Y3

Level 02 / 03 Readers

Y1 : REVALUE REQUEST (Level 02 Readers)
A balance in the VMC account because coins or bills were accepted or some balance is left after a vend. With this command the VMC tries to transfer the balance to the payment media.

Y2-Y3 : Revalue amount - scaled.
The revalue amount should not exceed the revalue limit value given by the command REVALUE LIMIT REQUEST.

Revalue (15H / 65H)	Revalue Request (00H) Y1	Revalue Amount Y2-Y5

Level 03 (EXPANDED CURRENCY MODE) Readers

Y1 : REVALUE REQUEST (Level 03 Readers)
A balance in the VMC account because coins or bills were accepted or some balance is left after a vend. With this command the VMC tries to transfer the balance to the payment media.

Y2-Y5 : Revalue Amount - scaled.
The revalue amount should not exceed the revalue limit value given by the command REVALUE LIMIT REQUEST.

Reader response:

Revalue Approved (0DH) Z1

Level 02 / 03 Readers

Z1 : REVALUE APPROVED (Level 02 / 03 Readers)
A balance is in the VMC account because coins or bills were accepted or some balance is left after a vend. The VMC has issued a REVALUE REQUEST to the payment media reader to transfer the balance to the payment media. The payment media reader accepted the request and added its value to the payment media balance. The reader then responds with a REVALUE APPROVED, so the VMC

Petitioner Exhibit 1002-2860
CSC ServiceWorks – Ex. 1008
Page 136 of 270

may clear the account.

Revalue Denied (0EH) Z1

Level 02 Readers

Z1 : REVALUE DENIED (Level 02 / 03 Readers)
A balance is in the VMC account because coins or bills were accepted or some balance is left after a vend. The VMC has issued a REVALUE REQUEST to the payment media reader to transfer the balance to the payment media. The payment media reader does not accept the request and responds with a REVALUE DENIED, so the VMC has to pay out change. It is a quite common situation if there is no payment media inserted at this moment.

7.4.17 REVALUE - Limit Request (Level 02 / 03 Readers)

Revalue (15H / 65H)	Revalue Limit Request (01H) Y1

Level 02 / 03 Readers

Note: If revaluing, follow the BEGIN SESSION with this command.

Y1 : REVALUE LIMIT REQUEST (Level 02 Readers)
In a configuration with a bill and/or coin acceptor and payment media reader connected to a VMC, the VMC must know the maximum amount the payment media reader eventually will accept by a REVALUE REQUEST. Especially if the bill acceptor accepts a wide range of bills. Otherwise the VMC may be confronted by the situation where it accepted a high value bill and is unable to pay back cash or revalue it to a payment media. (see also below)

Reader response:

Revalue Limit Amount (0FH) Z1	Revalue Limit Amount Z2-Z3

Level 02 / 03 (EXPANDED CURRENCY MODE disabled) Readers

Z1 : REVALUE LIMIT AMOUNT (Level 02 / 03 Readers)

Petitioner Exhibit 1002-2861 CSC ServiceWorks – Ex. 1008
Page 137 of 270

The patron intends to revalue the payment media with a bill of some value. The VMC must know what kind of bills to accept, so it will issue a REVALUE LIMIT REQUEST to get the amount the payment media reader will accept. The payment media reader will respond with the scaled value, calculated with the maximum allowed payment media balance minus the current balance of the payment media. The payment media reader responds with REVALUE DENIED if there is no payment media available upon this request.

Z2-Z3 : Revalue limit value - scaled.

Reader response:

Revalue Limit Amount (0FH)	Revalue Limit Amount
Z1	Z2-Z5

Level 03 (EXPANDED CURRENCY MODE) Readers

Z1 : REVALUE LIMIT AMOUNT (Level 03 Readers)
The patron intends to revalue the payment media with a bill of some value. The VMC must know what kind of bills to accept, so it will issue a REVALUE LIMIT REQUEST to get the amount the payment media reader will accept. The payment media reader will respond with the scaled value, calculated with the maximum allowed payment media balance minus the current balance of the payment media. The payment media reader responds with REVALUE DENIED if there is no payment media available upon this request.

Z2-Z5 : Revalue Limit Value - scaled.

7.4.18 EXPANSION - Request ID

	Request ID (00H)	Manufacturer Code	Serial Number	Model Number	Software Version
Expansion (17H / 67H)	Y1	Y2-Y4	Y5-Y16	Y17-Y28	Y29-Y30

Y1 : REQUEST ID
The VMC is requesting payment media reader identification information. The information included above (Y2-Y30) provides the payment media reader with VMC identification information.

Y2-Y4 : Manufacturer Code - ASCII
Identification code for the equipment supplier. Currently defined codes are listed in the EVA document entitled "The Data Transfer Standard EVA-DTS" document, the Audit Data Dictionary section, chapter 4,

Petitioner Exhibit 1002-2862
CSC ServiceWorks – Ex. 1008
Page 138 of 270

"Manufacturer Codes".

Y5-Y16 : Serial Number - ASCII
Factory assigned serial number.

Y17-Y28 : Model Number - ASCII
Manufacturer assigned model number.

Y29-Y30 : Software Version - packed BCD
Current software version.

Reader response:

Peripheral ID (09H)	Manufacture Code	Serial Number	Model Number	Software Version
Z1	Z2-Z4	Z5-Z16	Z17-Z28	Z29-Z30

Level 01 / 02 / 03 Readers (If VMC indicates Level 01 or 02)

Peripheral ID (09H)	Manufacture Code	Serial Number	Model Number	Software Version	Optional Feature Bits
Z1	Z2-Z4	Z5-Z16	Z17-Z28	Z29-Z30	Z31-Z34

Level 03 Readers (If VMC indicates Level 03)
See paragraph 7.4.4 for a detailed explanation of this response.

7.4.19 EXPANSION - Read User File (Level 02 Readers)

Obsolete Command – Do not use for new designs!! (Use EXPANSION - Diagnostics)

	Read User File (01H)	Number of User File
Expansion (17H / 67H)	Y1	Y2

Level 02 Readers

Y1= READ USER FILE
The VMC request's the user file. The length of the file is variable with a maximum length of 32 bytes. The contents of the data are defined by the VMC manufacturer. If the payment media reader does support this command it will respond with USER FILE DATA.

Y2= Number of User File.
The File identification number. The number and size of the data files are defined

Petitioner Exhibit 1002-2868
CSC ServiceWorks – Ex. 1008
Page 139 of 270

by the payment media reader manufacturer. The maximum number of user files are FFh.

Reader response:

User Data File (10H) Z1	Number of User File Z2	Length of User File Z3	User Data Z4-Zn

Z1 : USER FILE DATA (only level 02 readers)
The VMC requires user data and has issued a EXPANSION - READ USER FILE to the payment media reader.

Z2 : Number of User File.
The File identification number. The number and size of data files are defined by the payment media reader manufacturer. The maximum number of user files are FFh.

Z3 : Length of user file
The length of the user file. The maximum length of the user file is 32 bytes. If the user file don't exists the length will be set to 00h.

Z4-Zn : Data defined by the VMC manufacturer.

7.4.20 EXPANSION - Write User File (Level 02 Readers)

Obsolete Command – Do not use for new designs!! (Use EXPANSION - Diagnostics)

Expansion (17H / 67H)	Write User File (02H) Y1	Number of User File Y2	Length of User File Y3	User Data Y4-Yn

Y1 : WRITE USER FILE
The VMC request's to write the user file. The length of the file is variable with a maximum length of 32 bytes. The contents of the data are defined by the VMC manufacturer. If the command is supported but the payment media reader is unable to write the payment media (writing problem or data too long) it will respond with MALFUNCTION/ERROR.

Y2 : Number of User File.
The File identification number. The number and size of data files are defined by the payment media reader manufacturer. The maximum number of user files are FFh.

Y3 : Length of user file

Petitioner Exhibit 1002-2864 CSC ServiceWorks – Ex. 1008
Page 140 of 270

The length of the user file. The maximum length of the user file is 32 bytes.

Y4-Yn : Data defined by the VMC manufacturer.

Reader response:

No Data response

7.4.21 EXPANSION - Write Time/Date File (Level 02/03 readers)

Expansion (17H / 67H)	Write Time/ Date File (03H) Y1	Time Date Y2-Y11

Y1 : WRITE TIME/DATE FILE
The VMC requests to write the Time/Date file.

Y2- Y11: Time/Date to synchronize the card reader real time clock. The date bytes are BCD encoded.

Y2 = Years (Range: 00..99)
Y3 = Months (Range: 01..12)
Y4 = Days (Range: 01..31)
Y5 = Hours (Range: 00..23)
Y6 = Minutes (Range: 00..59)
Y7 = Seconds (Range: 00..59)
Y8 = Day of Week (Range: 01..07, Monday = 1..Sunday = 7)
Y9 = Week Number (Range: 01..53)
Y10 = Summertime (Range: 00..01, Summertime = 1)
Y11 = Holiday (Range: 00..01, Holiday = 1)

If any item of the time/date is not supported use FFH instead.

7.4.22 EXPANSION – Enable Options (Level 03 readers)

Expansion (17H / 67H)	Optional Feature Bit Enable (04H) Y1	Optional Feature Bits Y2-Y5

Level 03 Readers

Y1 : OPTIONAL FEATURE BIT ENABLE
The VMC can enable which level 3 features it desires.

Y2 - Y5: Individual expanded feature bits as sent by reader in response to the 17H-00H EXPANSION REQUEST ID command. To enable a feature, a bit is set to one.

Petitioner Exhibit 1002-2865 CSC ServiceWorks – Ex. 1008
Page 141 of 270

Bits should be sent in descending order, i.e. bit 31 is sent first and bit 0 is sent last. **All features are disabled after a reset**.

b0 - File Transport Layer supported
b1 - 0 = 16 bit monetary format, 1 = 32 bit monetary format
b2 - multi currency / multi lingual
b3 - negative vend
b4 - data entry
b5 to b31 not used (should be set to 0)

Note: If 32 bit monetary format (b1) and or multi currency / multi lingual (b2) options are enabled, this condition will be known as **EXPANDED CURRENCY MODE** in the rest of the document.

7.4.23 EXPANSION – FTL REQ TO RCV

Expansion (17H / 67H)	FTL (FAH) Y1	REQ TO RCV Y2-Y6

Level 03 Readers (if File Transport Layer option enabled)

The VMC is requesting to receive data from the reader whose destination address will always be 10H or 60H. Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 : **FTL** REQ TO RCV
The VMC is requesting to receive data from the reader.

Y2 : **FTL** Destination Address (Reader = 10H / 60H as defined in Section 2.6.

Y3 : **FTL** Source Address
The source address of the command as defined in Section 2.6.

Y4 : **FTL** File ID
The type of information desired as defined in Section 2.6.

Y5 : **FTL** Maximum Length
The total number of blocks in the file as defined in Section 2.6.

Y6 : **FTL** Control
Data transfer control information as defined in Section 2.6.

Reader response:

Petitioner Exhibit 1002-2866
CSC ServiceWorks – Ex. 1008
Page 142 of 270

Two responses are possible from the reader, either the SEND BLOCK (1DH) which transmits the initial (or only) part of the data or the RETRY / DENY (1CH). Note that the response can either be immediate or delayed.

FTL (1DH) SEND BLOCK Z1	SEND BLOCK Information Z2-Z34

Z1 : 1DH response which indicates SEND BLOCK

Z2 : Destination address of data as defined in Section 2.6

Z3 : Block # of data as defined in Section 2.6

Z4-Z34: Data (maximum of 31 bytes)

or

FTL (1CH) RETRY / DENY Z1	RETRY / DENY Information Z2-Z4

Z1 : 1CH response which indicates RETRY / DENY

Z2 : Destination address of response as defined in Section 2.6

Z3 : Source address of response (10H / 60H) as defined in Section 2.6

Z4 : Retry delay

7.4.24 EXPANSION – FTL RETRY / DENY

Expansion (17H)	FTL (FBH) Y1	RETRY / DENY Y2-Y4

Level 03 Readers (if File Transport Layer option enabled)

The VMC is retrying, denying, or aborting a data transfer to/from the reader whose destination address will always be 10H or 60H. Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 : **FTL** RETRY / DENY

Petitioner Exhibit 1002-2867
CSC ServiceWorks – Ex. 1008
Page 143 of 270

The VMC is requesting to retry, deny, or abort a data transfer.

Y2 : **FTL** Destination Address (Reader = 10H / 60H)
The destination address of the command as defined in Section 2.6.

Y3 : **FTL** Source Address
The source address of the command as defined in Section 2.6.

Y4 : **FTL** Retry Delay
The time delay required of the sender as defined in Section 2.6.

Reader response:

None

7.4.25 EXPANSION – FTL SEND BLOCK

Expansion (17H / 67H)	FTL (FCH) Y1	SEND BLOCK Y2-Y34

Level 03 Readers (if File Transport Layer option enabled)

The VMC is sending data to the reader whose destination address will always be 10H or 60H. Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 : **FTL** SEND BLOCK
The VMC is requesting to send data.

Y2 : **FTL** Destination Address (Reader = 10H / 60H)
The destination address of the command / data as defined in Section 2.6.

Y3 : **FTL** Block #
The block # of data as defined in Section 2.6

Y4-Y34 **FTL** Data (maximum of 31 bytes)
The actual data block as defined in Section 2.6.

Reader response:

None

7.4.26 EXPANSION – FTL OK TO SEND

Expansion	FTL	OK TO SEND

Petitioner Exhibit 1002-2868 CSC ServiceWorks – Ex. 1008
Page 144 of 270

(17H / 67H)	(FDH) Y1	 Y2-Y3

Level 03 Readers (if File Transport Layer option enabled)

The VMC is indicating that it is OK for the reader to transfer data. The destination address will always be the reader 10H or 60H. Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 : **FTL** OK TO SEND
The VMC is indicating it is OK to send data.

Y2 : **FTL** Destination Address (Reader = 10H / 60H)
The destination address of the command / data as defined in Section 2.6.

Y3 : **FTL** Source Address
The source address of the command as defined in Section 2.6.

Reader response:

One response is possible from the reader which transmits the initial (or only) part of the data.

Note that the response can either be immediate or delayed.

FTL (1DH) SEND BLOCK Z1	SEND BLOCK Information Z2-Z34

Z1 : 1DH response which indicates SEND BLOCK

Z2 : Destination address of data as defined in Section 2.6

Z3 : Block # of data as defined in Section 2.6

Z4-Z34: Data (maximum of 31 bytes)

7.4.27 EXPANSION – FTL REQ TO SEND

Expansion (17H / 67H)	FTL (FEH) Y1	REQ TO SEND Y2-Y6

Level 03 Readers (if File Transport Layer option enabled)

Petitioner Exhibit 1002-2869
CSC ServiceWorks – Ex. 1008
Page 145 of 270

The VMC is requesting to send data to the reader whose destination address will always be 10H or 60H. Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 : **FTL** REQ TO SEND
The VMC is requesting to send data to the reader.

Y2 : **FTL** Destination Address (Reader = 10H / 60H)
The destination address of the command as defined in Section 2.6.

Y3 : **FTL** Source Address
The source address of the command as defined in Section 2.6.

Y4 : **FTL** File ID
The type of information desired as defined in Section 2.6.

Y5 : **FTL** Maximum Length
The total number of blocks in the file as defined in Section 2.6.

Y6 : **FTL** Control
Data transfer control information as defined in Section 2.6.

Reader response:

Two responses are possible from the reader, either the OK TO SEND (1EH) which allows the data transfer to start or the RETRY / DENY (1CH). Note that the response can either be immediate or delayed.

FTL (1EH) OK TO SEND Z1	OK TO SEND Information Z2-Z3

Z1 : 1EH response which indicates OK TO SEND

Z2 : Destination address of response as defined in Section 2.6

Z3 : Source address of response (10H / 60H) as defined in Section 2.6

or

Petitioner Exhibit 1002-2870
CSC ServiceWorks – Ex. 1008
Page 146 of 270

FTL (1CH) RETRY / DENY Z1	RETRY / DENY Information Z2-Z4

Z1 : 1CH response which indicates RETRY / DENY

Z2 : Destination address of response as defined in Section 2.6

Z3 : Source address of response (10H / 60H) as defined in Section 2.6

Z4 : Retry delay

7.4.28 EXPANSION - Diagnostics

Expansion (17H / 67H)	Diagnostics (FFH) Y1	User Defined Data Y2-Yn

Y1 : DIAGNOSTICS.
Device manufacturer specific instruction for implementing various manufacturing or test modes.

Y2-Yn : User Defined Data.
The data portion of this command is defined by the manufacturer and is not part of this document.

Reader response:

Diagnostics Response (FFH) Z1	User Defined Z2-Zn

Z1 : DIAGNOSTICS RESPONSE

Z2-Zn : User Defined Data.
The data portion of this response is defined by the manufacturer and is not part of this document.

Petitioner Exhibit 1002-2871
CSC ServiceWorks – Ex. 1008
Page 147 of 270

7.5 Cashless Device Non-Response Time

The default maximum non-response time for a cashless device is 5 seconds. This is the maximum time for which a cashless device will not respond to a command or a POLL with ACK, NAK or a message. The "Application Maximum Response Time" reported in byte Z7 of the Reader Configuration Data (7.4.2) supersedes this default value if Z7 is greater.

7.6 Cashless Device Power Requirements

The current draw for any cashless device must fall within the following limits. All measurements are at the minimum VMC Voltage Output.

Idle mode = 300 mA. (avg.) continuous

Transport or Read/Write cycle = 1.5 A @ 50% maximum duty cycle up to 5 seconds.

Petitioner Exhibit 1002-2872
CSC ServiceWorks – Ex. 1008
Page 148 of 270

7.7 Example Vend Sessions

EXAMPLE VEND SESSION #1
(Valid Single Vend)

Controller		Cashless Device	State
POLL	→		
	←	BEGIN SESSION	(Session Idle)
ACK	→		
VEND REQUEST	→		
	←	ACK	(Vend)
POLL	→		
	←	VEND APPROVED	
ACK	→		
VEND SUCCESS	→		
	←	ACK	(Session Idle)
SESSION COMPLETE	→		
	←	ACK	
POLL	→		
	←	END SESSION	(Enabled)

Petitioner Exhibit 1002-2878
CSC ServiceWorks – Ex. 1008
Page 149 of 270

EXAMPLE VEND SESSION #2
(Valid Multiple Vend)

Controller		Cashless Device	State
POLL	→		
	←	BEGIN SESSION	(Session Idle)
ACK	→		
VEND REQUEST	→		
	←	ACK	(Vend)
POLL	→		
	←	VEND APPROVED	
ACK	→		
VEND SUCCESS	→		
	←	ACK	(Session Idle)
VEND REQUEST	→		
	←	ACK	(Vend)
POLL	→		
	←	VEND APPROVED	
ACK	→		
VEND SUCCESS	→		
	←	ACK	(Session Idle)
SESSION COMPLETE	→		
	←	ACK	
POLL	→		
	←	END SESSION	(Enabled)

Petitioner Exhibit 1002-2874
CSC ServiceWorks – Ex. 1008
Page 150 of 270

EXAMPLE VEND SESSION #3
(Session cancelled by user with reader return button)

Controller		Cashless Device	State
POLL	→		
	←	BEGIN SESSION	(Session Idle)
ACK	→		
	User pushes reader RETURN button		
POLL	→		
	←	SESSION CANCEL	
ACK	→		
SESSION COMPLETE	→		
	←	ACK	
POLL	→		
	←	END SESSION	(Enabled)

Petitioner Exhibit 1002-2875
CSC ServiceWorks – Ex. 1008
Page 151 of 270

EXAMPLE VEND SESSION #4a
(Session cancelled by user via coin mechanism escrow return button before product was selected)

Controller		Cashless Device	State
POLL	→		
	←	BEGIN SESSION	(Session Idle)
ACK	→		
	User pushes coin mech. escrow return		
SESSION COMPLETE	→		
	←	ACK	
POLL	→		
	←	END SESSION	(Enabled)

Petitioner Exhibit 1002-2876
CSC ServiceWorks – Ex. 1008
Page 152 of 270

EXAMPLE VEND SESSION #4b
(Session cancelled by user via coin mechanism escrow return button after product was selected)

Controller		Cashless Device	State
POLL	→		
	←	BEGIN SESSION	(Session Idle)
ACK	→		
VEND REQUEST	→		
	←	ACK	(Vend)

User pushes coin mech. escrow return

CANCEL VEND	→		
	←	ACK	
POLL	→		
	←	VEND DENIED	(Session Idle)
SESSION COMPLETE	→		
	←	ACK	
POLL	→		
	←	END SESSION	(Enabled)

Petitioner Exhibit 1002-2877
CSC ServiceWorks – Ex. 1008
Page 153 of 270

EXAMPLE VEND SESSION #5
(VMC Failure/product not dispensed
Refund positive)

Controller		Cashless Device	State
POLL	→		
	←	BEGIN SESSION	(Session Idle)
ACK	→		
VEND REQUEST	→		
	←	ACK	(Vend)
Reader deducts purchase price from payment media			
POLL	→		
	←	VEND APPROVED	
VMC fails to dispense product			
VEND FAILURE	→		
	←	ACK	
POLL	→		
	←	Silence during the refund operation	
POLL	→		
	←	ACK	C
SESSION COMPLETE	→		
	←	ACK	
POLL	→		
	←	END SESSION	(Enabled)

Petitioner Exhibit 1002-2878
CSC ServiceWorks – Ex. 1008
Page 154 of 270

EXAMPLE VEND SESSION #5A
(VMC Failure/product not dispensed
Refund fail)

Controller		Cashless Device	State
POLL	→		
	←	BEGIN SESSION	(Session Idle)
ACK	→		
VEND REQUEST	→		
	←	ACK	(Vend)
Reader deducts purchase price from payment media			
POLL	→		
	←	VEND APPROVED	
VMC fails to dispense product			
VEND FAILURE	→		
	←	ACK	
POLL	→		
	←	Silence during the refund operation	
POLL	→		
	←	MALFUNCTION ERROR code	
		1100yyyy=refund fail	(Level 02 / 03)
		ACK	(Level 01)
SESSION COMPLETE	→		
	←	ACK	
POLL	→		
	←	END SESSION	(Enabled)

Petitioner Exhibit 1002-2870
CSC ServiceWorks – Ex. 1008
Page 155 of 270

EXAMPLE VEND SESSION #6
(Vend denied by reader)

Controller		Cashless Device	State
POLL	→		
	←	BEGIN SESSION	(Session Idle)
ACK	→		
VEND REQUEST	→		
	←	ACK	(Vend)

Insufficient funds or payment media/account error

POLL	→		
	←	VEND DENIED	(Session Idle)

VMC makes no attempt to dispense product

SESSION COMPLETE	→		
	←	ACK	
POLL	→		
	←	END SESSION	(Enabled)

Petitioner Exhibit 1002-2880
CSC ServiceWorks – Ex. 1008
Page 156 of 270

EXAMPLE VEND SESSION #7
(Command Out of Sequence Error)

Controller		Cashless Device	State
POLL	→		
	←	BEGIN SESSION	(Session Idle)
ACK	→		
VEND REQUEST	→		
	←	ACK	(Vend)
EXPANSION ID REQUEST	→		
	←	ACK	
POLL	→		
	←	COMMAND OUT OF SEQUENCE	(Session Idle)
ACK	→		
RESET	→	{**Mandatory**}	
	←	ACK	
			(Inactive)

Petitioner Exhibit 1002-2881
CSC ServiceWorks – Ex. 1008
Page 157 of 270

EXAMPLE VEND SESSION #8a
(Reader busy for longer than max. non response time)

Controller		Cashless Device	State
POLL	→		
	←	BEGIN SESSION	(Session Idle)
ACK	→		
VEND REQUEST	→		
	←	ACK	(Vend)
POLL	→		
		[silence…]	(Reader busy)
POLLs (numerous)	→		
	←	[silence…]	(continued POLLs w/ no response)
POLL	→		
	←	ACK	(restart Non-Response timer)
POLLs (numerous)	→		
	←	[silence…]	(continued POLLs w/ no response)
POLL	→		
	←	[silence…]	(Reader almost finished)
POLL	→		
	←	VEND APPROVED	(Reader ready)
ACK	→		
VEND SUCCESS	→		
	←	ACK	(Session Idle)
VEND REQUEST	→		
	←	ACK	(Vend)
POLL	→		
	←	VEND APPROVED	
ACK	→		
VEND SUCCESS	→		
	←	ACK	(Session Idle)
SESSION COMPLETE	→		
	←	ACK	
POLL	→		
	←	END SESSION	(Enabled)

Petitioner Exhibit 1002-2882
CSC ServiceWorks – Ex. 1008
Page 158 of 270

EXAMPLE VEND SESSION #8b
(Reader busy for shorter than max. non response time)

Controller		Cashless Device	State
POLL	→		
	←	BEGIN SESSION	(Session Idle)
ACK	→		
VEND REQUEST	→		
	←	ACK	(Vend)
POLL	→		
	←	[silence...]	(Reader busy)
POLLs (numerous)	→		
	←	[silence...]	(Continued POLLs w/ no response)
POLL	→		
	←	[silence...]	(Reader almost finished)
POLL	→		
	←	VEND APPROVED	(Reader ready)
ACK	→		
VEND SUCCESS	→		
	←	ACK	(Session Idle)
VEND REQUEST	→		
	←	ACK	(Vend)
POLL	→		
	←	VEND APPROVED	
ACK	→		
VEND SUCCESS	→		
	←	ACK	(Session Idle)
SESSION COMPLETE	→		
	←	ACK	
POLL	→		
	←	END SESSION	(Enabled)

NOTE

If the peripheral omits to respond within the maximum non-response time, it is considered to be off-line.

Petitioner Exhibit 1002-2888
CSC ServiceWorks – Ex. 1008
Page 159 of 270

EXAMPLE VEND SESSION #8c
(No Response, Reader busy at Vend Request.)

Controller		Cashless Device	State/ Comment
POLL	→		
	←	BEGIN SESSION	
ACK	→		
VEND REQUEST	→		
	←	[silence…]	Reader busy. The reader may not send the response within the t-response(max) timeout or hasn't received the command completely due to line breakdown
VEND REQUEST	→		VMC repeats the command: As the VMC isn't sure, that the slave has received the command free of errors it repeats it. The command itself is not yet performed by the reader as long the ACK hasn't been sent.
	←	[silence…]	Reader busy
VEND REQUEST	→		
	←	ACK	(Vend) The reader will now perform the command. The response isn't available at the moment, thus the VEND REQUEST is only acked
POLL (numerous)	→		VMC polls the reader to obtain the data in VEND APPROVED
	←	ACK	The reader may send a ACK or [silence] to each POLL
POLL	→		
	←	VEND APPROVED	The response to the VEND REQUEST is now available. It must be sent within the time defined by the APPLICATION MAXIMUM RESPONSE TIME. This is measured from the ACK following the VEND REQUEST.
ACK	→		

Petitioner Exhibit 1002-2884
CSC ServiceWorks – Ex. 1008
Page 160 of 270

EXAMPLE VEND SESSION #9
(Pre-approved authorization aborted by coin mechanism escrow return button before BEGIN SESSION)

Controller		Cashless Device	State
User swipes payment media			
			(Enabled)
POLL	→		
	←	ACK	
READER CANCEL	→		
	←	ACK	
(If applicable, reader aborts HOST communications, ejects payment media, etc...)			
POLL	→		
	←	CANCELLED	

Petitioner Exhibit 1002-2885
CSC ServiceWorks – Ex. 1008
Page 161 of 270

EXAMPLE VEND SESSION #10
(Single Negative Vend)

Controller		Cashless Device	State
POLL	→		
	←	BEGIN SESSION	(Session Idle)
ACK	→		
	User inserted a payment media, and inserted then a product, which was detected valid, or pressed a selection button to identify the desired product which will be inserted later on		
NEGATIVE VEND REQUEST	→		
	←	ACK	(Vend)
POLL	→		
	←	VEND APPROVED	
	The payment reader is able to add the desired value to the credit		
ACK	→		
	The product is now fully accepted from the machine or the user has finally finished insertion of a valid product		
VEND SUCCESS	→		
	←	ACK	(Session Idle)
	The payment media reader has added the credit		
SESSION COMPLETE	→		
	←	ACK	
POLL	→		
	←	END SESSION	(Enabled)

Normally, can or bottle return-vendors may check the product first, before the patron inserts his card. It is up to the VMC, to delay the negative vend request, until the session idle state is reached. In many return-vendors, from this state, the product is already fully accepted. Therefore, there is no need for the further sequences, this means, vend accepted, vend success will follow each other immediately.

If the payment media reader is not able to update the credit, there will be two conditions:

- The return vendor is able to escrow the product after the vend denied. In this case the session complete is sent, the product is return and the credit remains unchanged.
- The return vendor is not able to escrow the product after vend denied. In this case, session complete should be sent and there should be an update credit within the system (VMC), which could be returned by other means (i.e. return coins, tokens, etc).

Petitioner Exhibit 1002-2886
CSC ServiceWorks – Ex. 1008
Page 162 of 270

If a return vendor is able to escrow the product again, this vendor normally accepts the product finally only a vend accepted was sent. In this case there may happen some fault condition which allows no final acceptance of the product. The return vendor then closes the session with vend failed instead of vend success, indicating to the reader not to update the system credit, or, if the payment media is no longer present, request re-insertion of the media.

EXAMPLE DATA ENTRY SESSION #1
(Three key Data Entry w/ Prompt & Asterisks for Entries)

Controller		Cashless Device	State
		Previously Enabled	Enabled
POLL	→		
	←	DATA ENTRY REQUEST + DISPLAY REQUEST (prompt)	
ACK	→		
	User pushes Selection Key 1		
DATA ENTRY RESPONSE (Key 1)	→		
	←	ACK	
POLL	→		
	←	DISPLAY REQUEST (prompt + *)	
ACK	→		
	User pushes Selection Key 2		
DATA ENTRY RESPONSE (Key 2)	→		
	←	ACK	
POLL	→		
	←	DISPLAY REQUEST (prompt + **)	
ACK	→		
	User pushes Selection Key 3		
DATA ENTRY RESPONSE (Key 3)	→		
	←	ACK	(Enabled)
POLL	→		
	←	DISPLAY REQUEST (prompt + *** or "Entry OK")	
ACK	→		

Note: After Display Request Time expires, VMC regains control of display

Petitioner Exhibit 1002-2887 CSC ServiceWorks – Ex. 1008
Page 163 of 270

POLL	→		
	←	BEGIN SESSION	(Session Idle)
ACK	→		

Petitioner Exhibit 1002-2888
CSC ServiceWorks – Ex. 1008
Page 164 of 270

EXAMPLE DATA ENTRY SESSION #2
(Data Entry with Reader Cancel)

Controller		Cashless Device	State
		Previously Enabled	Enabled
POLL	→		
	←	DATA ENTRY REQUEST + DISPLAY REQUEST (prompt)	
ACK	→		
		User pushes (valid) Selection Key	
DATA ENTRY RESPONSE (Key 1)	→		
	←	ACK	
POLL	→		
	←	DISPLAY REQUEST (prompt + *)	
ACK	→		
		User pushes (invalid) Selection Key	
DATA ENTRY RESPONSE (Key 2)	→		
	←	ACK	
POLL	→		
	←	DATA ENTRY CANCEL	
ACK	→		(Enabled)
POLL	→		
	←	DISPLAY REQUEST ("Error")	
ACK	→		
		After VMC Display Request Time expires, regains control of display	

Note that the above scenario is only an example and it may not be prudent to cancel a session after the first wrong entry. (Someone could fraudulently obtain a password by trying the maximum of selection keys at each position.)

Petitioner Exhibit 1002-2880
CSC ServiceWorks – Ex. 1008
Page 165 of 270

EXAMPLE DATA ENTRY SESSION #3
(Data Entry with VMC Cancel)

Controller		Cashless Device	State
		Previously Enabled	Enabled
POLL	→		
	←	DATA ENTRY REQUEST + DISPLAY REQUEST (prompt)	
ACK	→		
		User pushes Selection Key	
DATA ENTRY RESPONSE (Key 1)	→		
	←	ACK	
POLL	→		
	←	DISPLAY REQUEST (prompt + *)	
ACK	→		
		User walks away & VMC times out	
DATA ENTRY RESPONSE (FF's)	→		
	←	ACK	(Enabled)
POLL	→		
	←	DISPLAY REQUEST ("Try Again")	
ACK	→		
		After VMC Display Request Time expires, regains control of display	

Petitioner Exhibit 1002-2890
CSC ServiceWorks – Ex. 1008
Page 166 of 270

(this page intentionally left blank)

Petitioner Exhibit 1002-2891
CSC ServiceWorks – Ex. 1008
Page 167 of 270

Petitioner Exhibit 1002-2892
CSC ServiceWorks – Ex. 1008
Page 168 of 270

Section 8
Communications Gateway VMC/Peripheral Communication Specifications

8.1 Introduction

This section defines the communications bytes sent and received between a Communications Gateway (Comms Gateway) and the VMC. The Comms Gateway address is 00011xxxB (18H).

Unless otherwise stated, all information is assumed to be in a binary format.

After the VMC has issued a command, the Comms Gateway must respond with a reply. The reply may be an ACK or a detailed message response. If the command format expects a response, the Comms Gateway may: 1) respond with an ACK, to acknowledge receiving the command, and send the response later as a response to a POLL, or 2) immediately respond with the expected message.

The Comms Gateway response to a command from the VMC may be an ACK, a single message, or if there is more data to send it may be a multi message reply, up to the MDB maximum of 36 bytes.

The following command / response set has been defined to provide a means to transfer vending information system data from the VMC to the Comms Gateway in one of two ways;

1) Entire DTS files (including DXS, ST, SD1, G85, SE, and DXE records) are transferred using the file transport layer (FTL) of MDB.

2) Activity “Reports” are sent from the VMC to the Comms Gateway every time something happens in the vending system, it is then the Comms Gateways responsibility to store and assemble the DTS file. (DXS, ST, SD1, G85, SE and DXE data are not sent.) Obviously, a combination of these two methods can be designed to meet specific needs also.

Petitioner Exhibit 1002-2898
CSC ServiceWorks – Ex. 1008
Page 169 of 270

8.2 VMC Commands

VMC Cmd	Code	VMC Data	Comm Gateway response
RESET	18H		00H - Just RESET (1)
SETUP	19H	Feature level (1) Scale factor (1) Decimal places (1)	01H - Comms Gateway Config (1) Feature level (1) Max. App. Resp. (2)
POLL	1AH		00H - Just RESET (1)
			01H - Comms Gateway Config (1) Feature level (1) Max. App. Resp. (2)
			02H - Request transmit (1)
			03H - Data transmitted (1)
			04H - Error (1) Error code (n)
			05H - DTS Event Acknowledge (1)
			06H - Peripheral ID: (1) Mfg. code (3) Serial number (12) Model number (12) Software ver. (2) Opt. features (4)
			07H - Radio Signal Strength (2)
			1BH - FTL REQ to RCV (option) (1)
			1CH - FTL RETRY / DENY (option) (1)
			1DH - FTL SEND BLOCK (option) (1)
			1EH - FTL OK to SEND (option) (1)
			1FH - FTL REQ to SEND (option) (1)
			FFH - Diagnostics (n)
REPORT	1BH	Type = 01, Transaction (1) Transaction Type (1) Selection (Row/Col.) (2) Price (2) Cash in, Coin tubes (2) Cash in, Cashbox (2) Cash in, Bills (2) Value in, Cashless #1 (2) Value in, Cashless #2 (2) Revalue to Cashless #1 (2) Revalue to Cashless #2 (2) Cash out (2) Discount Amount (2) Surcharge Amount (2) User Group # (1) Price List (1) Date (4) Time (2)	

Petitioner Exhibit 1002-2894
CSC ServiceWorks – Ex. 1008
Page 170 of 270

		Type = 02, DTS Event (1) DTS Event Code (10) Date (4) Time (2) Duration (4) Activity (1) Terminal ID (12)	05-DTS Event Acknowledge (1)
		Type = 03, Asset ID (1) Asset Type = 0n (1) Manufacture Code (3) Serial Number (12) Model Number (12) Software Version (2) Type = 03, Asset ID (1) Asset Type = 8n (1) Asset Number (20)	
		Type = 04, Currency ID (1) VMC Currency Code (2) VMC Currency (1) VMC Decimal Point (1)	
		Type = 05, Product ID (1) Product Identification (20) Selection Presence (1)	
CONTROL	1CH	00H - Disable (1)	
		01H - Enable (1)	
		02H - Transmit (1)	
EXPANSION	1FH	00H - Identification	06H - Peripheral ID: (1) Mfg. code (3) Serial number (12) Model number (12) Software ver. (2) Opt. features (4)
		01H - Feature enable (1) Features enabled (4)	
		FAH - FTL (option) REQ TO RCV	1DH - SEND BLOCK 1CH - RETRY / DENY
		FBH - FTL (option) RETRY / DENY	No Data
		FCH - FTL (option) SEND BLOCK	No Data
		FDH - FTL (option) OK TO SEND	1DH - SEND BLOCK
		FEH - FTL (option) REQ TO SEND	1EH - OK TO SEND 1CH - RETRY/DENY
		FFH - Diagnostics (n)	FFH - Diagnostics (n)

Petitioner Exhibit 1002-2895
CSC ServiceWorks – Ex. 1008
Page 171 of 270

8.3 Communications Gateway Command Format

VMC Command	Code/Sub-code	VMC Data	Comms Gateway Response
RESET	18H	No data	Z1

This command is the vehicle that the VMC should use to tell the Comms Gateway that it should perform its initialization procedure. With the exception of the ACK response, it should abort all communication and revert to the internally stored operational parameters.

Z1 = 00 JUST RESET

Indicates the Comms Gateway has been reset internally or on command from the VMC.

The following initialization sequence is recommended. It should be used after "power up", after issuing the RESET command, or after issuing the Bus Reset (pulling the transmit line "active" for a minimum of 100 mS).

POLL – 18H
To obtain "JUST RESET" response

SETUP – 19H
To obtain Comms Gateway level and configuration information

EXPANSION IDENTIFICATION – 1F 00H
To obtain additional identification information and options

EXPANSION FEATURE ENABLE – 1F 01H
To enable desired options

CONTROL / ENABLE – 1CH / 01H
To enable / alert the Comms Gateway to start collecting data and / or monitoring for REPORT commands situations.

VMC Command	Code/Sub-code	VMC Data	Comms Gateway Response
SETUP	19H	Y1 - Y3	Z1 - Z4

Y1 = VMC feature level

Indicates the highest Comms Gateway feature level that the VMC supports. Currently the highest feature level is 03, with no requirement to support previous (obsolete) levels 1 and 2.)

Petitioner Exhibit 1002-2896
CSC ServiceWorks – Ex. 1008
Page 172 of 270

Y2 = Scale factor

The multiplier used to scale all monetary values transferred between the VMC and the Comms Gateway.

Y3 = Decimal places

The number of decimal places used to communicate monetary values between the VMC and the Comms Gateway.

Z1 = 01 COMMS GATEWAY CONFIGURATION

The Comms Gateway is responding to a SETUP command. This response includes the following data;

Z2 = Comms Gateway feature level

The feature level of the Comms Gateway. Currently the highest feature level is 03, with no requirement to support previous (obsolete) levels 1 and 2.)

Z3 - Z4 = Application maximum response time

The maximum length of time, in seconds, that an Comms Gateway may be unable to respond to any commands. This includes the time communicating over an external network. The VMC should continue POLLing the Comms Gateway during this time in an attempt to re-synchronize communications earlier. When the Comms Gateway is ready to communicate over the bus again, it should respond to the next POLL with COMPLETE (if communicating externally) or ACK. This time essentially replaces the standard MDB non-response time, as such it's default value is equal to the defined non-response time (5 seconds).

VMC Command	Code/Sub-code	VMC Data	Comms Gateway Response
POLL	1AH	No data	Z1 - Zn

The POLL command is used by the VMC to obtain information from the Comms Gateway. This information may include setup information, activity requests, or error conditions. An ACK response indicates that no error states exist and either no information request is pending or pending information is not yet ready for transmission.

Petitioner Exhibit 1002-2897
CSC ServiceWorks – Ex. 1008
Page 173 of 270

In addition to an ACK, the VMC may receive the following POLL responses from the Comms Gateway.

Petitioner Exhibit 1002-2898
CSC ServiceWorks – Ex. 1008
Page 174 of 270

Z1 = 00 JUST RESET

Indicates the Comms Gateway has been reset internally or on command from the VMC.

Z1 = 01 COMMS GATEWAY CONFIGURATION

The Comms Gateway is responding to a SETUP command. This response includes the following data;

Z2 = Comms Gateway feature level

The feature level of the Comms Gateway. Currently the highest feature level is 03, with no requirement to support previous (obsolete) levels 1 and 2.)

Z3 - Z4 = Application maximum response time

The maximum length of time, in seconds, that an Comms Gateway may be unable to respond to any commands. This includes the time communicating over an external network. The VMC should continue POLLing the Comms Gateway during this time in an attempt to re-synchronize communications earlier. When the Comms Gateway is ready to communicate over the bus again, it should respond to the next POLL with COMPLETE (if communicating externally) or ACK. This time essentially replaces the standard MDB non-response time, as such it's default value is equal to the defined non-response time (5 seconds).

Z1 = 02 REQUEST TO TRANSMIT

The Comms Gateway is requesting permission to transmit data to an external collection device. This is done to control the bus power supply. The Comms Gateway should continue sending this response to each POLL until permission to transmit has been granted or the need to transmit goes away.

Z1 = 03 DATA TRANSMITTED

The Comms Gateway is finished transmitting to an external collect device.

Z1 = 04 ERROR

The Comms Gateway has developed some type of detectable error. The error codes will be sent continuously, or until the error is resolved.

Z2 – Zn = Error code

Petitioner Exhibit 1002-2899
CSC ServiceWorks – Ex. 1008
Page 175 of 270

The error codes are ASCII strings taken from the EVA DTS Communications fault list.

Petitioner Exhibit 1002-2000
CSC ServiceWorks – Ex. 1008
Page 176 of 270

Z1 = 05 DTS EVENT ACKNOWLEDGE

The Comms Gateway has recognized that a DTS Event has occurred and must act accordingly. The specific actions will be defined by the Comms Gateway operational specifications.

Z1 = 06H PERIPHERAL ID

Comms Gateway is sending peripheral ID information. This response includes the following data;

Z2 - Z4 = Manufacturer code

Identification code for the equipment supplier. Sent as ASCII characters. Blanks (20H) are acceptable.

Z5 - Z16 = Serial number

Factory assigned serial number sent as numeric ASCII characters. All bytes must be sent. Zeros (30H) and blanks (20H) are acceptable.

Z17 - Z28 = Model number ASCII.

Manufacturer assigned model number sent as ASCII characters. All bytes must be sent. Zeros (30H) and blanks (20H) are acceptable.

Z29 - Z30 = Software version

Current software version sent as packed BCD.

Z31 - Z34 = Optional Features

Each of the 32 bits indicate an optional features availability. If the bit is set the feature is available. Currently defined options are:

b0: File transport layer support
b1: Verbose mode: See REPORT command
b2 - b31: Future use, must be set to 0.

Petitioner Exhibit 1002-2001
CSC ServiceWorks – Ex. 1008
Page 177 of 270

Z1 = 07H RADIO SIGNAL STRENGTH

The Comms Gateway is reporting its signal strength from the network. This response includes the following data;

Z2 = Signal Strength

The level of radio signal strength detected by the Comms Gateway. This is a binary number from 00H to 64H (100%) representing the percentage of expected signal. This can be sent after every POLL, or as needed due to changes in the signal.

Note that all FTL responses below are defined in Section 2.6. For the Comms Gateway, the source address will always be the Comms Gateway (18H) as defined in Section 2.3.

Z1 = 1BH REQ TO RCV (File Transport Layer)

The Comms Gateway is requesting to receive data from a device or VMC.

Z2 = Destination address of response
Z3 = Source address of response (18H)
Z4 = File ID
Z5 = Maximum length
Z6 = Control

Z1 = 1CH RETRY/DENY (File Transport Layer)

The Comms Gateway is requesting a device or VMC to retry or deny the last FTL command.

Z2 = Destination address of response
Z3 = Source address of response (18H)
Z4 = Retry delay

Z1 = 1DH SEND BLOCK (File Transport Layer)

The Comms Gateway is sending a block of data (maximum of 31 bytes) to a device or VMC.

Z2 = Destination address of data
Z3 = Block #
Z4-Z34 = Data (maximum of 31 bytes)

Z1 = 1EH OK TO SEND (File Transport Layer)

Petitioner Exhibit 1002-2002
CSC ServiceWorks – Ex. 1008
Page 178 of 270

The Comms Gateway is indicating that it is OK for a device or VMC to send it data.

Z2 = Destination address of response
Z3 = Source address of response (18H)

Petitioner Exhibit 1002-2003
CSC ServiceWorks – Ex. 1008
Page 179 of 270

Z1 = 1F REQ TO SEND (File Transport Layer)

The Comms Gateway is requesting to send data to a device or VMC.

Z2 = Destination address of response
Z3 = Source address of response (18H)
Z4 = File ID
Z5 = Maximum length
Z6 = Control

Z1 = FFH DIAGNOSTICS

The Comms Gateway is responding to a EXPANSION/DIAGNOSTICS command. This response includes the following data;

Z2 - Zn User defined data

Device manufacturer specific responses after receiving manufacturing or test instructions. Z1 - Zn implies that any number of bytes may be used for the response data from the Comms Gateway.

VMC Command	Code/Sub-code	VMC Data	Comms Gateway Response
REPORT	1BH	Y1 – Ynn	No data

The REPORT command is used by the VMC to pass activity information to the Comms Gateway. If the "Verbose mode" is enabled via the EXPANSION / FEATURE ENABLE command, this command must be sent immediately following the completion of any activity it is describing. The activities may include; a transaction, a DTS defined event, an asset identification, currency identification, or product identification.

The intent of this command is to provide information so that the Comms Gateway can create a Data Transfer Standard file. All of the following fields show their corresponding DTS fields for reference, for further detail refer to the Data Transfer Standard.

If the "Verbose mode" is disabled, only the "DTS Event" report type records must be sent. This mode uses the FTL to transfer the complete DTS files and the DTS Event report types to alert the VMC of any alarm conditions.

Since reports data may vary, any field that is not relevant, or not known, should be populated with 00H's. All cash values are scaled and decimal adjusted using the data provided in the SETUP command.

Petitioner Exhibit 1002-2004
CSC ServiceWorks – Ex. 1008
Page 180 of 270

Y1 = Type: The type of activity that is being reported, includes one of the following:

01H	Transaction
02H	DTS Event
03H	Asset ID
04H	Currency ID
05H	Product ID

If Y1 = 01H then the following "Transaction" data fields have been identified to be included:

Y2 = Transaction Type

This field defines the type of transaction that the following data describes. The defined transaction types include;

01H	Paid Vend
02H	Token Vend
03H	Free Vend
04H	Test Vend
05H	Revalue
06H	Negative Vend
07H	Vendless*
08H	Manual / Service

* The end of a "Vendless" transaction is defined by the VMC manufacturer, for example an escrow request, a failed vend, etc.

Y3 – Y4 = Item Number

This is the binary field used to link REPORT type 01 to REPORT type 05. It is an item number, 0000H through FFFFH of the selected product involved in the most recent transaction. This number is defined by the manufacturer.

Y5 – Y6 = Price (PA102)

The established price of the product involved in the most recent transaction. The established price is the price before any adjustments i.e. discounts surcharges, etc.

Y7 – Y8 = Cash in, Coin Tubes (CA303/CA307 or CA1001/CA1002)

Petitioner Exhibit 1002-2005
CSC ServiceWorks – Ex. 1008
Page 181 of 270

The value of cash deposited into the coin tubes since the completion of the previous transaction.

Y9 – Y10 = Cash in, Cashbox (CA302/CA306)

The value of cash deposited into the cashbox since the completion of the previous transaction.

Y11 – Y12 = Cash in, Bills (CA304/CA308)

The value of cash deposited into the bill stacker since the completion of the previous transactions.

Y13 – Y14 = Value in, Cashless Device #1 (DA201/DA203)

The value removed from the media in cashless device #1 since the completion of the previous transaction.

Y15 – Y16 = Value in, Cashless Device #2 (DB201/DB203)

The value removed from the media in cashless device #2 since the completion of the previous transaction.

Y17 – Y18 = Revalue to Cashless Device #1 (DA401/DA402)

The value returned to the media in cashless device #1 since the completion of the previous transaction.

Y19 – Y20 = Revalue to Cashless Device #2 (DB401/DB402)

The value returned to the media in cashless device #2 since the completion of the previous transaction.

Y21 – Y22 = Cash out (CA401/CA403 or CA402/CA404)

The total value of the cash dispensed from the system since the completion of the previous transaction.

Y23 – Y24 = Discount Amount (CA701/CA702)

The value of any discounts awarded since the completion of the previous vend.

Y25 – Y26 = Surcharge Amount (CA705/CA706)

Petitioner Exhibit 1002-2006
CSC ServiceWorks – Ex. 1008
Page 182 of 270

The value of any surcharges collected since the completion of the previous vend.

Y27 = User Group # (DA701 or DB701)

The user group number that the transaction is associated with.

Y28 = Price List (LA101)

The price list that the transaction is associated with

Y29 – Y32 = Date (PA501)

The date of the transaction. This data is sent as BCD in the following sequence YYYY/MM/DD. For example, 17 March 2002 would be 20H 02H 03H 17H. If the date is not known these bytes are filled with 99Hs.

Y33 – Y34 = Time (PA502)

The time of the transaction. This data is sent as BCD , 24 hour format, in the following sequence HHMM. For example, 6:30 PM would be 18H 30H. If the time is not known these bytes are filled with 99Hs.

If Y1 = 02H then the following "DTS Event" data fields have been identified to be included:

Y2 – Y11 = DTS Event Code (EA101 or EA201 or EA701)

This is an alpha-numeric ASCII code defining the event being reported. The codes are list in the EVA DTS manual. In addition to the standard DTS event codes, an interrogation event is reported as "EA3" and a power outage event is reported as "EA7".

Y12 – Y15 = Date (EA102)

The date of the event. This data is sent as BCD in the following sequence YYYY/MM/DD. For example, 17 March 2002 would be 20H 02H 03H 17H. If the date is not known these bytes are filled with 99Hs.

Y16 – Y17 = Time (EA103)

Petitioner Exhibit 1002-2007
CSC ServiceWorks – Ex. 1008
Page 183 of 270

The time of the event. This data is sent as BCD in the following sequence HH/MM. For example, 6:30 PM would be 18H 30H. If the time is not known these bytes are filled with 99Hs.

Y18 – Y21 = Duration (EA206)

The duration of the event in total minutes. This data is sent as binary. For example, 4 hours and 15 minutes would be 00H 00H 00H FFH.

Y22 = Activity (EA205)

The current status of the events activity. This field is equal to 00H if the event is inactive (or not reset for "EA3") or 01H if the event is active (or reset for "EA3").

Z1 = 05 DTS EVENT ACKNOWLEDGE

The Comms Gateway has recognized that a possible alarm situation has occurred and must act accordingly. The specific actions will be defined by the Comms Gateway operational specifications.

If Y1 = 03H then the following "Asset ID" data fields have been identified to be included:

Y2 = Asset Type

The following code pairs have been defined to represent the type of equipment asset that is being communicated.

Code	Equipment type	DTS header (αα)
01H / 81H	Audit Module / Data Carrier (DC) Identification	AM1
02H / 82H	Bill Validator Identification	BA1
03H / 83H	Changer Identification	CA1
04H / 84H	Control Board Identification	CB1
05H / 85H	Cashless #1 Identification	DA1
06H / 86H	Cashless #2 Identification	DB1
07H / 87H	Machine Identification	ID1

If Y2 has the MSB = 0 (i.e. Y2 = 01H) then the following asset data fields have been identified to be included:

Y3 – Y5 = Manufacturer code (αα101, first 3 characters)

Petitioner Exhibit 1002-2008
CSC ServiceWorks – Ex. 1008
Page 184 of 270

Identification code for the equipment supplier. Sent as ASCII characters. Blanks (20H) are acceptable.

Y6 - Y17 = Serial number ($\alpha\alpha$101, 4th through 15th characters)

Factory assigned serial number sent as numeric ASCII characters. All bytes must be sent. Zeros (30H) and blanks (20H) are acceptable.

Y18 - Y29 = Model number ($\alpha\alpha$102)

Manufacturer assigned model number sent as ASCII characters. All bytes must be sent. Zeros (30H) and blanks (20H) are acceptable.

Y30 - Y31 = Software version (or Build Standard) ($\alpha\alpha$103)

Current software version sent as packed BCD.

If Y2 has the MSB = 1 (i.e. Y2 = 81H) then the following asset data fields have been identified to be included:

Y2 – Y21 = Asset Number ($\alpha\alpha$105 or $\alpha\alpha$106)

The asset number of the equipment. This is a reference number used for tracking purposes, separate from the serial number. It is usually programmed by the equipment operator.

If Y1 = 04H then the following "Currency ID" data fields have been identified to be included:

Y2 – Y3 = VMC's Country / Currency Code (ID402)

The packed BCD Country / Currency code of the VMC can be sent in two different forms depending on the value of the left most BCD digit.

If the left most digit is a 0, the International Telephone Code is used to indicate the country that the changer is set-up for. For example, the USA code is 00 01H (Z2 = 00 and Z3 = 01).

If the left most digit is a 1, the latest version of the ISO 4217 numeric currency code is used. For example, the code for the US dollar is 18 40H (Z2 = 18 and Z3 = 40) and for the Euro is 1978 (Z2 = 19 and Z3 = 78).

Petitioner Exhibit 1002-2009
CSC ServiceWorks – Ex. 1008
Page 185 of 270

All new designs after July, 2000 must use the ISO 4217 numeric currency codes.

Y4 = VMC's Coin Scaling Factor / Currency Description (ID403)

The multiplier used to scale all monetary values transferred between the VMC and the vending machines monetary system.

Y5 = VMC's Decimal Point (ID401)

The number of digits to the right of the decimal point. This field is used in countries whose currency requires a number of digits to the right of the decimal point other than 2.

If Y1 = 05H then the following "Product ID" data fields have been identified to be included:

Y2 – Y3 = Item Number

This is the binary field used to link REPORT type 01 to REPORT type 05. This number is defined by the manufacturer.

Y4 – Y9 = Product Number (PA101)

This is the ASCII representation of the Item Number that should be included in the DTS file. All bytes must be sent, leading blanks (20H) are acceptable.

Y10 – Y29 = Product Identification (PA103)

The ASCII product identification that should identify the product itself, as in a name (chips/crisps) or an ID number / bar code. All bytes must be sent, leading blanks (20H) are acceptable.

Y30 = Selection Presence Status (PA107)

This field is set to 00H if a vend mechanism (motor, solenoid, etc.) is present for this selection. This field is set to 01H if a vend mechanism is not present.

An example of a 01H being sent would be if the vend mechanism was present previously, and something occurred so that it is not being currently detected (i.e., removed, broken wire, etc.). It is **not** intended to indicate that a product is not available for vending (i.e., sold out).

Petitioner Exhibit 1002-2010
CSC ServiceWorks – Ex. 1008
Page 186 of 270

VMC Command	Code/Sub-code	VMC Data	Comms Gateway Response
CONTROL	1CH	Y1	No data

This command is the vehicle that the VMC uses to control the Comms Gateway's use of an external collection device. For example when it should, or should not, transmit through the external collection device. The information is identified by one of the following subcommands;

Y1 = 00 Disabled

No external transmissions will be granted and no REPORT commands will be sent.

Y1 = 01 Enabled

External transmissions may be requested and REPORT commands will be sent.

Y1 = 02 Transmit

Permission to transmit and / or receive data is granted, or a transmission session is requested. A DATA TRANSMITTED response to a POLL must be sent when the transmission session is complete.

VMC Command	Code/Sub-code	VMC Data	Comms Gateway Response
EXPANSION/ IDENTIFICATION	1FH/00H	Y1	Z1 - Z34

Y1 = 00H IDENTIFICATION subcommand

The VMC is requesting Comms Gateway identification information for asset tracking and optional feature purposes.

Z1 = 06H PERIPHERAL ID

Comms Gateway is sending peripheral ID information. This response includes the following data;

Z2 - Z4 = Manufacturer code

Identification code for the equipment supplier. Sent as ASCII characters. Blanks (20H) are acceptable.

Petitioner Exhibit 1002-2911
CSC ServiceWorks – Ex. 1008
Page 187 of 270

Z5 - Z16 = Serial number

Factory assigned serial number sent as numeric ASCII characters. All bytes must be sent. Zeros (30H) and blanks (20H) are acceptable.

Z17 - Z28 = Model number ASCII.

Manufacturer assigned model number sent as ASCII characters. All bytes must be sent. Zeros (30H) and blanks (20H) are acceptable.

Z29 - Z30 = Software version

Current software version sent as packed BCD.

Z31 - Z34 = Optional Features

Each of the 32 bits indicate an optional features availability. If the bit is set the feature is available. Currently defined options include:

b0:	File transport layer support.
b1:	Verbose mode: See REPORT command
b2 - b31:	Future use, must be set to 0.

VMC Command	Code/Sub-code	VMC Data	Comms Gateway Response
EXPANSION/ FEATURE ENABLE	1FH/01H	Y1 - Y5	No data

Y1 = 01H FEATURE ENABLE subcommand

This command is used to enable each of the optional features defined in Z32-Z35 of the PERIPHERAL ID response. The VMC should send the EXPANSION /IDENTIFICATION command, receive the PERIPHERAL ID response, perform a logical OR with the optional features it wants to enable, and return the resulting enabled features back to the Comms Gateway by setting a bit to 1 for each respective optional feature enabled. All optional features are disabled after reset.

Y2 - Y5 = Optional features enabled

Each of the 32 bits indicates an optional features state. If the bit is set the feature is enabled.

Petitioner Exhibit 1002-2012
CSC ServiceWorks – Ex. 1008
Page 188 of 270

VMC Command	Code/Sub-code	VMC Data	Comms Gateway Response
EXPANSION COMMAND	0FH FAH **FTL** REQ TO RCV	Y1-Y5	Z1 - Zn (immediate or POLLed)

The VMC is requesting to receive data from the Comms Gateway whose destination address will always be (18H). Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 = Destination address of command (18H)
Y2 = Source address of command
Y3 = File ID
Y4 = Maximum length
Y5 = Control

Z1 = 1DH which indicates SEND BLOCK
Z2 = Destination address of data
Z3 = Block #
Z4 - Z34 = Data (maximum of 31 bytes)

or

Z1 = 1CH which indicates RETRY / DENY
Z2 = Destination address of response
Z3 = Source address of response (18H)
Z4 = Retry delay

Petitioner Exhibit 1002-2918
CSC ServiceWorks – Ex. 1008
Page 189 of 270

VMC Command	Code/Sub-code	VMC Data	Comms Gateway Response
EXPANSION COMMAND	0FH FBH **FTL** RETRY / DENY	Y1-Y3	None

The VMC is retrying, denying, or aborting a data transfer to/from the Comms Gateway whose destination address will always be (18H). Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 = Destination address of command (18H)
Y2 = Source address of command
Y3 = Retry delay

VMC Command	Code/Sub-code	VMC Data	Comms Gateway Response
EXPANSION COMMAND	0FH FCH **FTL** SEND BLOCK	Y1-Y33	None

The VMC is sending data to the Comms Gateway whose destination address will always be (18H). Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 = Destination address of command & data (18H)
Y2 = Block #
Y3 - Y33 = Data (maximum of 31 bytes)

VMC Command	Code/Sub-code	VMC Data	Comms Gateway Response
EXPANSION COMMAND	0FH FDH **FTL** OK TO SEND	Y1-Y2	Z1-Z34 (immediate or POLLed)

The VMC is indicating that it is OK for the Comms Gateway to transfer data. The destination address will always be the Comms Gateway (18H). Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 = Destination address of command (18H)
Y2 = Source address of command

Z1 = 1DH which indicates SEND BLOCK
Z2 = Destination address of data
Z3 = Source address of data
Z4 - Z34 = Data (maximum of 31 bytes)

Petitioner Exhibit 1002-2014 – Ex. 1008
Page 190 of 270

VMC Command	Code/Sub-code	VMC Data	Comms Gateway Response
EXPANSION COMMAND	0FH FEH **FTL** REQ TO SEND	Y1-Y5	Z1 - Zn (immediate or POLLed)

The VMC is requesting to send data to the Comms Gateway whose destination address will always be (18H). Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 = Destination address of command (18H)
Y2 = Source address of command
Y3 = File ID
Y4 = Maximum length
Y5 = Control

Z1 = 1EH which indicates OK TO SEND
Z2 = Destination address of response
Z3 = Source address of response (18H)

or

Z1 = 1CH which indicates RETRY / DENY
Z2 = Destination address of response
Z3 = Source address of response (18H)
Z4 = Retry delay

VMC Command	Code/Sub-code	VMC Data	Comms Gateway Response
EXPANSION/ DIAGNOSTICS	1FH/FFH	Y1 - Yn	Z1 - Zn

Y1 = FFH DIAGNOSTICS subcommand

Device manufacturer specific instruction for implementing various manufacturing or test modes.

Y2 - Yn = User defined data

The data portion of this command is defined by the manufacturer and is not part of this document.

Z1 = FFH DIAGNOSTICS

The Comms Gateway is responding to a EXPANSION/DIAGNOSTICS command. This response includes the following data;

Z2 - Zn = User defined data

Petitioner Exhibit 1002-2015
CSC ServiceWorks – Ex. 1008
Page 191 of 270

Device manufacturer specific responses after receiving manufacturing or test instructions. Z1 - Zn implies that any number of bytes may be used for the response data from the Comms Gateway.

8.4 Communications Gateway Non-Response Time

The maximum non-response time for a Comms Gateway is 5 seconds. This is the maximum time for which a Comms Gateway will not respond to a command with ACK, NAK, or a data message.

8.5 Communications Gateway Power Requirements

The current draw for any Comms Gateway must fall within the following limits. All measurements are at the minimum VMC Voltage Output.

Idle mode = 300 mA. (avg.) continuous

Active mode = 1.8 A continuous and up to 2.5 A (max) for an accumulated maximum of 10 seconds. The active power mode must be initiated by the REQUEST TO TRANSMIT followed by the CONTROL/TRANSMIT. The active power mode must be closed by sending the DATA TRANSMITTED. During this time the VMC will make its own decisions about which other peripherals will be disabled or not. This may result in the entire machine being disabled for normal vending.

Petitioner Exhibit 1002-2016
CSC ServiceWorks – Ex. 1008
Page 192 of 270

8.6 Communications Gateway Examples

Event	Exchange
Power on Reset at VMC or JUST RESET received by VMC any other time	Reset sequence Enable sequence
Communications Gateway is triggered to send a file	Request sequence Transmit sequence
VMC is triggered to send a file	Dump sequence Transmit sequence
DTS Event situation occurs at VMC	DTS Event sequence Request sequence Transmit sequence
Error situation is detected at Comms Gateway	Error sequence
Every vend completion	Vend sequence

Reset sequence **VMC**		**Comms Gateway**	**Comments**
RESET (18)	→		Reset command
	←	ACK	
POLL (1A)	→		Must be sent once reset, internal or external
	←	JUST RESET (00)	
ACK	→		
SETUP (19…)	→		Establish operation configuration
	←	CONFIG. (01…)	
ACK	→		
EXPANSION/ID (1F/00…)	→		Send asset information
	←	PERIPHERAL ID (06…)	Get asset information
ACK	→		
EXPANSION/FEATURE ENABLE (1F/01…)	→		Enable additional feature if necessary
	←	ACK	
Enable sequence **VMC**		**Comms Gateway**	**Comments**
CONTROL/ENABLE (1C01)	→		Enable command
	←	ACK	
Disable sequence **VMC**		**Comms Gateway**	**Comments**
CONTROL/DISABLE (1C00)	→		Disable command
	←	ACK	

Petitioner Exhibit 1002-2917
CSC ServiceWorks – Ex. 1008
Page 193 of 270

Request sequence			
VMC		**Comms Gateway**	**Comments**
File transfer done		**using the MDB**	**file transport layer**

Dump sequence			
VMC		**Comms Gateway**	**Comments**
File transfer done		**using the MDB**	**file transport layer**

Transmit sequence			
VMC		**Comms Gateway**	**Comments**
POLL (1A)	→		
	←	Request to transmit (02)	
ACK	→		
CONTROL/ TRANSMIT (1C/02)	→		
	←	ACK	
POLL (1A)			
		ACK	
		.	Continue POLLing until …
		.	
POLL (1A)	→		
	←	Data transmitted (03)	
ACK	→		

DTS Event sequence			
VMC		**Comms Gateway**	**Comments**
REPORT (1B / 02…)	→		
	←	ACK	
		.	Repeat until recognized
		.	
REPORT (1B /02…)	→		
	←	DTS EVENT ACKNOWLEDGE (05)	

Error sequence			
VMC		**Comms Gateway**	**Comments**
POLL (1A)	→		Sent continuously, or until the error is resolved
	←	ERROR (06)	
ACK	→		

Activity sequence			
VMC		**Comms Gateway**	**Comments**
REPORT (1B…)	→		Sent every activity
	←	ACK	

Petitioner Exhibit 1002-2918
CSC ServiceWorks – Ex. 1008
Page 194 of 270

Section 9

Universal Satellite Device (USD)
VMC/Peripheral Communication Specifications

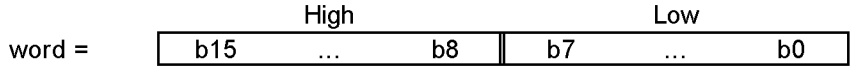
9.1 Introduction

An MDB Universal Satellite Device (USD) is a vending device which lacks customary credit acceptance peripherals. As such, a USD must rely on a host vending machine controller (VMC) to establish credit sufficient to perform a vend. The specification herein describes a protocol by which a USD and a VMC exchange messages and credit via the MDB bus.

9.1.1 Definitions

This section defines the non-response and application response time, base addresses, and the communication bytes sent by the MDB Universal Satellite Device (USD) and a Vending Machine Controller.

- The default maximum non-response time of the USD is 5 seconds.
- The default maximum application response time of the USD is 5 seconds.
- Three consecutive USD base addresses are defined to allow multiple USDs to operate simultaneously from a single VMC
- As defined in Section 2.3, the USD Base addresses are as follows: 01000xxxB (40H), 01001xxxB (48H), and 01010xxxB (50H).
- The specification defined herein assumes a USD base address of 40H in all examples. It should be understood that differing USD base addresses (48H and 50H) will follow the same command format.
- Multi-message responses to a single command are supported. Message length is subject to the 36 byte limit imposed by the MDB standard.
- Unless stated otherwise, all byte information contained herein is assumed to be in a binary format.
- Y_n represents bytes transmitted by the VMC, and Z_n are bytes transmitted by the USD.
- When words are referenced, they consist of two bytes with the higher order byte first.



9.2 USD Summary

This section is a summary of the USD command set and an overview of the modes of operation.

9.2.1 Command Summary

Petitioner Exhibit 1002-2019
CSC ServiceWorks – Ex. 1008
Page 195 of 270

Command	Hex Code	Description
RESET	40	Command for USD to self-reset.
SETUP	41	Command to configure USD to VMC requirements.
POLL	42	Command to request for USD activity status.
VEND	43	Command for vend approve / deny.
FUNDS	44	Command to send funds available or to set prices.
CONTROL	45	Command to enable/disable USD.
EXPANSION	47	Command to allow addition of features and enhancements.

9.2.2 Overview

The USD Command set described herein allows USDs' to be controlled under the following three modes of operation. The USD's mode of operation is determined by the USD's configuration byte [1] and the sequence of commands the VMC uses.

Mode One VMC is used to select items to be vended from the USD and the VMC contains all pricing information. The USD receives vend requests from the VMC and reports vend success or failure.

Mode Two The USD or the VMC may select items to be vended. The USD may have special requirements for price and/or selection ID display. In this case, the USD may issue a **FUNDS** request to retrieve this information. The USD must then issue a **VEND** request to gain approval from the VMC before a vend can take place.

Mode Three The USD selects items to be vended and has its own pricing information. The USD must issue an vend request to the VMC and gain approval before a vend can take place.

9.3 Command Protocol

This section contains the complete command set relating to the USD.

9.3.1 RESET

[1] Configuration byte refers to byte Z31 of the sequence Z31 through Z34 of the expansion 07 command. Please refer to page 9.12 for more information on how this byte influences the USD's mode of operation.

Petitioner Exhibit 1002-2020 CSC ServiceWorks – Ex. 1008
Page 196 of 270

Command	Code	VMC Data	USD Response data
RESET	40	No data bytes.	ACK

The **RESET** command is the vehicle that the VMC should use to instruct the USD to return to its default (power on) operating mode. The USD should respond to a reset command with an ACK to acknowledge receipt of the reset command. The USD must not accept any vend requests until the VMC issued setup command sequence has been completed.

The USD must also respond to the VMC issued "master reset" which resets all MDB peripheral devices. The VMC causes a master reset by transmitting a continuous break condition for a minimum of 100 milliseconds.

To ensure proper initialization, the USD should issue a "just reset" (see **POLL** response **00**) whenever it's pricing or configuration has changed.

9.3.2 SETUP

Command	Code	VMC Data	USD Response Data
SETUP	41	5 bytes: Y1-Y5	7 bytes: 04 + Z1 - Z6

The **SETUP** command is the vehicle that the VMC should use to configure the USD for feature level, credit scaling factor, display decimal place, and maximum vend approve/deny time. The USD responds to this command by returning it's feature level, highest vend price (divided by the scaling factor), selection configuration, and maximum application response time.

Alternatively, if the USD is not prepared to render a full response to the **SETUP** command, it may reply with an ACK. If this occurs, the USD must transmit it's setup data later, in response to a **POLL** command (see **POLL** command, response **04**). Until the **SETUP** command has been received by the USD, and the USD has correspondingly returned it's own setup data to the VMC, all vend requests will be disallowed.

Data sequence transmitted by the VMC to the USD during SETUP

VMC Data	Meaning or interpretation
Y1 =	VMC Feature level, Indicates current feature level of the VMC. Currently defined level is one.[2]
Y2 - Y3 =	Scaling factor 2 bytes (word). All transactions with the USD must be evenly divisible by this number.
Y4 =	Decimal place (02=US). Indicates the position of the decimal

[2] Feature level of the VMC is sent to allow the USD to arbitrate command compatibility with the VMC.

Petitioner Exhibit 1002-2021
CSC ServiceWorks – Ex. 1008
Page 197 of 270

	place on the USD's optional credit display
Y5 =	VMC maximum approve / deny time in seconds, FF = 255 seconds.

Data sequence transmitted by the USD to the VMC during SETUP

USD Response	Meaning or interpretation
04 + Z1 =	USD Feature level, indicates current feature level of the USD. Currently defined level is one.[3]
Z2 - Z3 =	Maximum price on USD in 2 bytes (word). Indicates the highest priced item on the USD.[4] USD should return FF FFh if it does not have internal pricing capability.
Z4 - Z5 =	Item number, defined by the manufacturer configuration (Binary).
Z6 =	USD maximum application response time in seconds, FF = 255 seconds.

[3] Feature level of the USD is sent to allow the VMC to arbitrate command compatibility with the USD. The USD may opt to send this data later in response to a POLL.
[4] The maximum price on the USD is returned to the VMC so this price can be used in the computation of maximum credit acceptance.

Petitioner Exhibit 1002-2022
CSC ServiceWorks – Ex. 1008
Page 198 of 270

9.3.3 POLL

Command	Code	USD response Data	USD Response Description
POLL	42	00	USD has just been reset, or wishes to be reset by the VMC.
		01 + 4 bytes Z1- Z4	Vend request, USD requests approval to vend a specified item from VMC.
		02	Vend or home success, requested vend or home was successful.
		03 + 4 bytes Z1 - Z4	Vend or home fail, requested vend or home has failed. Reason for failure is returned.
		04 + 6 bytes Z1 - Z6	USD configuration and setup data.
		05 + 2 bytes Z1 - Z2	USD item price request.
		06 + 2 bytes Z1 - Z2	USD Error codes.
		07 + 34 bytes Z1 - Z34	USD Peripheral ID string.
		08 + 4 bytes Z1 - Z4	USD Status response.
		09 + *n* bytes Z1 - *Zn*	USD multiple data block transfer response.
		0A + n bytes Z1 - Zn	USD single data block response
		1B + 5 bytes Z2 - Z6	FTL REQ TO RCV response
		1C + 3 bytes Z2 - Z4	FTL RETRY / DENY response
		1D + n bytes Z2 - Zn	FTL SEND BLOCK response
		1E + 2 bytes Z2 - Z3	FTL OK TO SEND response
		1F + 5 bytes Z2 - Z6	FTL REQ TO SEND response
		FF + Z1 - *Zn*	USD Diagnostic response.

The **POLL** command is used by the VMC to obtain status information from the USD. The same command is used by the USD to indicate a reset, request a vend, indicate vend success, indicate the reason for a vend failure, request the price of an item, send configuration and/or error data, return the USD's peripheral identification string, control the transmission and reception of data blocks, return a status and/or diagnostic response.

The USD responds to the **POLL** command with either an ACK, or a multi-byte response if there is more information to convey.

Petitioner Exhibit 1002-2028
CSC ServiceWorks – Ex. 1008
Page 199 of 270

Data sequence transmitted by the USD to the VMC after a *Reset Request*

USD Response	Meaning or interpretation
00	The 00 response indicates that the USD has just been reset or wishes to be reset[5].

Data sequence transmitted by the USD to the VMC for a V*end Request*

USD Response	Meaning or interpretation
01 + Z1 - Z2 =	Selection in 2 bytes. Indicates the product to be vended by item number, defined by the manufacturer, as part of a vend request.
Z3 - Z4 =	Scaled product price in 2 bytes (word). Indicates the price of the product to be vended divided by the scaling factor. A price of FFFF is transmitted if the USD does not contain price information.

Data sequence transmitted by the USD to the VMC after a V*end or Home success*

USD Response	Meaning or interpretation
02	Indicates that the requested vend or home was successful.

Data sequence transmitted by the USD to the VMC after a V*end or Home Fail*

USD Response	Meaning or interpretation
03 + Z1 - Z2 =	USD item number, defined by the manufacturer.
Z3 - Z4 =	Bits: b0 = Selection sold out. b1 = Selection motor / actuator jam. b2 = Non-existent motor / actuator. b3 = Invalid selection range[6]. b4 = Health safety error. b5 - b15 = Not defined.

[5] The VMC is expected to reconcile whether the USD is transmitting a 00 in confirmation of a VMC issued reset that has just occurred, or as an unsolicited request to be reset. The context of the VMC's prior communication activity should be used in making this assessment.

Petitioner Exhibit 1002-2024
CSC ServiceWorks – Ex. 1008
Page 200 of 270

Data sequence transmitted by the USD to the VMC if *SETUP response delayed*

USD Response	Meaning or interpretation
04 + Z1 =	USD Feature level, Indicates current feature level of the USD. The currently defined level is one.[7]
Z2 - Z3 =	Maximum price on USD 2 bytes (word). Indicates the highest priced item on the USD.[8] USD should return FF FFh if it does not have internal pricing capability.
Z4 - Z5 =	Item number, defined by the manufacturer.
Z6 =	USD maximum application response time in seconds, FF = 255 seconds.

Data sequence transmitted by the USD if the *USD needs pricing information*

USD Response	Meaning or interpretation
05 + Z1 - Z2 =	Item number, defined by the manufacturer.

Data sequence transmitted by the USD if the *USD has a failure to report to VMC*

USD Response	Meaning or Interpretation
06 + Z1 - Z2 =	Bits: b0 = Health Safety violation. b1 = Home or Chute sensor failure b2 = Keypad or Selection switch failure b3 - b15 = Not defined.

Data sequence transmitted by the USD for peripheral ID

[6] This error code is included to identify actuators that may not be present within the initially defined row and column configuration. See bytes Z4 and Z5 of the USD's setup response. This is typical in a snack machine implementation where some trays may not be populated with a full complement of motors and/or actuators.

[7] Feature level of the USD is sent to allow the VMC to arbitrate command compatibility with the USD. The USD may have elected to transmit this setup data in fulfillment of an earlier **SETUP** command.

[8] The maximum price on the USD is returned to the VMC so this price can be used in the computation of maximum credit acceptance.

Petitioner Exhibit 1002-2025
CSC ServiceWorks – Ex. 1008
Page 201 of 270

USD Response	Meaning or Interpretation
07 + Z1 - Z4 =	Manufacturer ID Code.
Z5 - Z16 =	USD Serial Number.
Z17 - Z28 =	USD Model Number.
Z29 - Z30 =	USD Software Version.
Z31 - Z34 =	Optional feature bits.

Data sequence transmitted by the USD to the VMC after a Status request

USD Response	Meaning or interpretation
08 + Z1 - Z2 =	Item number, defined by the manufacturer.
Z3 - Z4 =	Bits: b0 = Selection sold out. b1 = Selection motor / actuator jam. b2 = Non-existent motor / actuator. b3 = Invalid selection range. b4 = Health safety error. b5 - b15 = Not defined.

Data sequence transmitted by the USD to the VMC after a USD data transfer command

USD Response	Meaning or interpretation
09 + Z1 =	Z1 = 00 USD requests to receive data block Z2 from VMC Z1 = 01 USD requests to send Z2 data block(s) to VMC Z1 = 02 USD data block response where: Z2 = data block number Z3 - *Zn* = contents of data block
Z2 =	Z2 = Block number USD requests to receive if Z1 = 00 Z2 = Number of blocks the USD requests to send if Z1 = 01 Z2 = Block number the USD is sending if Z1 = 02.
Z3 - *Zn* =	Contents of data block sent by USD to VMC if Z1 = 02

Petitioner Exhibit 1002-2026
CSC ServiceWorks – Ex. 1008
Page 202 of 270

Data sequence transmitted by the USD to the VMC to send a single block of data

USD Response	Meaning or interpretation
0A + Z1 - Z*n*=	Z1 -Z*n* = Arbitrary data to be received by the VMC. The number "*n*" must be less than 35 per MDB standards

Data sequence transmitted by the USD to the VMC after an File Transport Layer (FTL) REQ TO RCV command

USD Response	Meaning or interpretation
Z1=1B + Z2 - Z6	The USD is requesting to receive data from a device or VMC Z2 = Destination address of response Z3 = Source address of response (40H, 48H, 50H) Z4 = File ID Z5 = Maximum length Z6 = Control

Data sequence transmitted by the USD to the VMC after an File Transport Layer (FTL) RETRY / DENY command

USD Response	Meaning or interpretation
Z1=1C + Z2 - Z4	The USD is requesting a device or VMC to retry or deny the last FTL command. Z2 = Destination address of response Z3 = Source address of response (40H, 48H, 50H) Z4 = Retry delay

Data sequence transmitted by the USD to the VMC after an File Transport Layer (FTL) SEND BLOCK command

USD Response	Meaning or interpretation
Z1=1D + Z2 - Z34	The USD is sending a block of data (maximum of 31 bytes) to a device or VMC. Z2 = Destination address of response Z3 = Block # Z4 - Z34 = Data (maximum of 31 bytes)

Petitioner Exhibit 1002-2027
CSC ServiceWorks – Ex. 1008
Page 203 of 270

Data sequence transmitted by the USD to the VMC after an File Transport Layer (FTL) OK TO SEND command

USD Response	Meaning or interpretation
Z1=1E + Z2 - Z3	The USD is indicating that it is OK for the device or VMC to send it data. Z2 = Destination address of response Z3 = Source address of response (40H, 48H, 50H)

Data sequence transmitted by the USD to the VMC after an File Transport Layer (FTL) REQ TO SEND command

USD Response	Meaning or interpretation
Z1=1F + Z2 - Z6	The USD is requesting to send data to a device or VMC. Z2 = Destination address of response Z3 = Source address of response (40H, 48H, 50H) Z4 = File ID Z5 = Maximum length Z6 = Control

Data sequence transmitted by the USD to the VMC after a diagnostic command

USD Response	Meaning or interpretation
FF + Z1 - Z*n* =	Diagnostic response.

9.3.4 VEND

Command	Code	Sub-Cmd	VMC Data	Response Data
VEND	43	00	none	none
	43	01	none	none
	43	02	2 bytes Y1-Y2	none
	43	03	2 bytes Y1-Y2	none
	43	04	2 bytes Y1-Y2	5 bytes: 08 + Z1 - Z4

Petitioner Exhibit 1002-2028
CSC ServiceWorks – Ex. 1008
Page 204 of 270

The **VEND** command is the vehicle that the VMC uses to signal vend approval or disapproval in response to a USD issued vend request (**POLL** response 01). The VEND command can also be used by the VMC to initiate a vend, home a selection, or query the status of a selection on the USD.

Sub Cmd:	Meaning or interpretation
00 =	Requested vend approved.
01 =	Requested vend disapproved.
02 =	Vend specified Item number, defined by the manufacturer.
03 =	Home specified Item number, defined by the manufacturer.
04 =	Request status of specified Item number, defined by the manufacturer.

Data sequence transmitted by the USD to the VMC after a Status request

USD Response	Meaning or interpretation
08 + Z1 - Z2 =	Item number, defined by the manufacturer.
Z3 - Z4 =	Bits: b0 = Selection sold out. b1 = Selection motor / actuator jam. b2 = Non-existent motor / actuator. b3 = Invalid selection range. b4 = Health safety error. b5 - b15 = Not defined.

9.3.5 FUNDS

Command	Code	Sub-Cmd	VMC Data	Response Data
FUNDS	44	00	2 bytes: Y1-Y2	none
	44	01	6 bytes: Y1-Y6	none

The **FUNDS** command is the vehicle the VMC should use to specify the funds available for vending. The **FUNDS** 00 command is issued by the VMC whenever the level of credit changes. Typically, the USD would display the credit information returned by a **FUNDS** 00 command on a credit display. The **FUNDS** 01 is issued by the VMC in response to an item price request (**POLL** response 05) by the USD.

Sub-Cmd	Meaning or interpretation

Petitioner Exhibit 1002-2020
CSC ServiceWorks – Ex. 1008
Page 205 of 270

00 + Y1 - Y2 =	Funds available in 2 bytes (word), scaled by the coin scaling factor.

Sub Cmd	Meaning or interpretation
01 + Y1 - Y2 =	Item number, defined by the manufacturer.
Y3 - Y4 =	Selection price in 2 bytes (word) scaled by coin scaling factor.
Y5 - Y6 =	Alphanumeric selection identifier 2 bytes (word), or FFFF if not available.[9]

9.3.6 CONTROL

Command	Code	Sub-Cmd	VMC Data	Response Data
CONTROL	45	00	none	none
	45	01	none	none

This command is the vehicle the VMC should use to enable or disable the USD.

Sub-Cmd	Meaning or interpretation
00	Disable USD.
01	Enable USD.

9.3.7 EXPANSION

Command	Code	Sub-Cmd	VMC Data	Response Data
EXPANSION	47	00	None	07 + Z1 - Z34 Peripheral ID string and feature bits.
	47	01	Y1 – Y4	none
	47	02	Y1	none
	47	03	Y1 - Y*n*	none
	47	04	Y1	09 + Z1 + Z2 - Z*n*
	47	05	Y1 - Y*n*	none
	47	FA	Y1 - Y5	1D + Z2 - Z34 or 1C + Z2 - Z4
	47	FB	Y1 - Y3	none

[9] Alpha-numeric selection identifier is provided to the USD for display purposes only.

Petitioner Exhibit 1002-2030
CSC ServiceWorks – Ex. 1008
Page 206 of 270

	47	FC	Y1 - Y33	none
	47	FD	Y1 - Y2	1D + Z2 - Z34
	47	FE	Y1 - Y5	1E + Z2 - Z3 or 1C + Z2 - Z4
	47	FF	Diagnostics	Diagnostic response.

Data sequence transmitted by the USD to the VMC after an expansion 00 sub-command

USD Response	Meaning or Interpretation
07 + Z1 - Z3 =	Manufacturer ID Code.
Z4 - Z15 =	USD Serial Number.
Z16 - Z27 =	USD Model Number.
Z28 - Z30 =	USD Software Version.
Z31 - Z34 =	Optional feature bits: b0 = USD is capable of storing and controlling pricing. b1 = USD is capable of selecting items to vend. b2 = USD is capable of supporting the File Transport Layer. This support is defined in Section 2.6. b3 - b31 = Available for future use.

Sub-Command used by the VMC to enable optional feature bits on the USD

Sub-Cmd	Meaning or interpretation
01 + Y1 - Y4	Enable optional feature bits defined in Z31-Z34 above. Feature is enabled if bit is set to 1, all features are disabled after a reset.

Sub-Command used by the VMC to identify the number of data blocks it wishes to send to the USD

Sub-Cmd	Meaning or interpretation
02 + Y1	Number of data blocks the VMC has to send to the USD (Binary)

Sub-Command used by the VMC to transmit a data block to the USD (Y2-Y*n*) and to identify the current block number being transmitted (Y1)

Sub-Cmd	Meaning or interpretation
03 + Y1	Block number the VMC is transmitting to the USD

Petitioner Exhibit 1002-2031
CSC ServiceWorks – Ex. 1008
Page 207 of 270

Y2 - Y*n*[10]	Data the VMC is transmitting to the USD

Sub-Command used by the VMC to request that the USD send or re-send data block number (Y1)

Sub-Cmd	Meaning or interpretation
04 + Y1	VMC requests USD to send block Y1

Sub-Command used by the VMC to send a single block of data to the USD

Sub-Cmd	Meaning or interpretation
05 + Y1 - Y*n*	VMC sends a single block of data consisting of Y1..Y*n*

Sub-Command used by the VMC for an FTL REQ TO RCV. The Z1- Zn response can be either immediate or delayed (POLLed).

Sub-Cmd	Meaning or interpretation
FA + Y1 - Y5	The VMC is requesting to receive data from the USD whose destination address will always be (40H, 48H, 50H). Note that all FTL Commands / Responses are defined in Section 2.6. Y1 = Destination address of command (40H,48H,50H) Y2 = Source address of command Y3 = File ID Y4 = Maximum length Y5 = Control
USD Response	**Meaning or interpretation**
Z1 - Z34 or Z1 - Z4	Z1 = 1DH which indicates SEND BLOCK Z2 = Destination address of data Z3 = Block # Z4 - Z34 = Data (maximum of 31 bytes) or Z1 = 1CH which indicates RETRY / DENY Z2 = Destination address of response Z3 = Source address of response (40H,48H,50H) Z4 = Retry delay

[10] The number "*n*" is limited by the MDB maximum message length of 36 bytes.

Petitioner Exhibit 1002-2032
CSC ServiceWorks – Ex. 1008
Page 208 of 270

Sub-Command used by the VMC for an FTL RETRY / DENY.

Sub-Cmd	Meaning or interpretation
FB + Y1 - Y3	The VMC is retrying, denying, or aborting a data transfer to/from the USD whose destination address will always be (40H, 48H, 50H). Note that all FTL Commands / Responses are defined in Section 2.6. Y1 = Destination address of command (40H,48H,50H) Y2 = Source address of command Y3 = Retry delay

Sub-Command used by the VMC for an FTL SEND BLOCK.

Sub-Cmd	Meaning or interpretation
FC + Y1 - Y33	The VMC is sending data to the USD whose destination address will always be (40H, 48H, 50H). Note that all FTL Commands / Responses are defined in Section 2.6. Y1 = Destination address of command (40H,48H,50H) Y2 = Block # Y3 - Y33 = Data (maximum of 31 bytes)

Sub-Command used by the VMC for an FTL OK TO SEND. The Z1 to Z33 response can be either immediate or delayed (POLLed).

Sub-Cmd	Meaning or interpretation
FD + Y1 - Y2	The VMC is requesting to receive data from the USD whose destination address will always be (40H, 48H, 50H). Note that all FTL Commands / Responses are defined in Section 2.6. Y1 = Destination address of command (40H,48H,50H) Y2 = Source address of command
USD Response Z1 - Z34	**Meaning or Interpretation** Z1 = 1DH which indicates SEND BLOCK Z2 = Destination address of data Z3 = Source address of data Z4 - Z34 = Data (maximum of 31 bytes)

Sub-Command used by the VMC for an FTL REQ TO SEND. The Z1 - Zn response can be either immediate or delayed (POLLed).

Sub-Cmd	Meaning or interpretation
FE + Y1 - Y5	The VMC is requesting to send data to the USD whose destination address will always be (40H, 48H, 50H). Note that all FTL Commands / Responses are defined in Section 2.6.

Petitioner Exhibit 1002-2038
CSC ServiceWorks – Ex. 1008
Page 209 of 270

	Y1 = Destination address of command (40H,48H,50H) Y2 = Source address of command Y3 = File ID Y4 = Maximum length Y5 = Control
USD Response Z1 - Z34 or Z1 - Z4	**Meaning or Interpretation** Z1 = 1EH which indicates OK TO SEND Z2 = Destination address of response Z3 = Source address of response (40H,48H,50H) or Z1 = 1CH which indicates RETRY / DENY Z2 = Destination address of response Z3 = Source address of response (40H,48H, 50H) Z4 = Retry delay

Data sequence transmitted by the USD to the VMC after a diagnostic command

USD Response	Meaning or interpretation
FF + Z1 - *Zn* =	Diagnostic response.

9.4 USD Power Requirements

This section defines the maximum power requirements for a USD.

USD peripherals may draw power from the MDB bus or from an integral power supply. In such cases where the USD will require power from the MDB bus, the current draw must remain within the following limits:

USD Mode	Current draw
Idle	200 mA (maximum continuous)
Vending/Homing	1.75 A (for up to 10 seconds)

Petitioner Exhibit 1002-2034
CSC ServiceWorks – Ex. 1008
Page 210 of 270

9.5 Examples – Mode 1 / 2 / 3 Sessions

This section contains three examples of USD sessions in which each of the three modes of USD operation are demonstrated operation respectively.

9.5.1 MODE ONE

In this example session the VMC selects the item to vend and knows the vend price. The USD receives the vend command, attempts the vend, and reports if the attempted vend failed or was successful.

VMC	MDB Data	Explanation	USD
⇒	**43+02+01+03**	VMC requests to vend item from the USD.	
	<ACK>	USD acks vend request.	⇐
⇒	**42**	VMC polls the USD.	
	<ACK>	USD acks receipt of poll.	⇐
⇒	**42**	VMC polls the USD again .	
	02	USD responds: vend complete	⇐
⇒	**<ACK>**	VMC acks vend outcome.	

Petitioner Exhibit 1002-2035
CSC ServiceWorks – Ex. 1008
Page 211 of 270

9.5.2 MODE TWO

In this example session the USD or the VMC can select items to vend but the USD may not be aware of the vend price of the item selected. If the USD needs the selected item price, it may request the item price from the VMC. The USD must then issue a **VEND** request, and wait for approval from the VMC before a vend is attempted. The VMC then approves or denies the requested vend and polls the USD for vend success or vend fail.

VMC	MDB Data	Explanation	USD
⇒	**42**	VMC polls the USD.	
	05+02+06	USD responds with pricing request for item in USD.	⇐
⇒	**<ACK>**	VMC acks the USD price request.	
⇒	**44+01+02+06+00+14 +FF+FF**	Using the Funds command the VMC sends a price of 20 coin factors for item in USD.	
	<ACK>	USD acks receipt of VMC price data.	⇐
⇒	**42**	VMC polls the USD.	
	01+02+06+FF+FF	USD responds with a request to vend item in USD at the VMC selected price.	⇐
⇒	**<ACK>**	VMC acks receipt of vend request.	
⇒	**43 + 00** or **01**	VMC approves or denies vend request.	
	<ACK>	USD acks receipt of approval or denial.	⇐
⇒	**42**	VMC polls the USD.	
	03+02+06+00+01	USD responds: vend fail, sold out.	⇐
⇒	**<ACK>**	VMC acks vend outcome.	

- The **FUNDS** command can be used by USD's which do not have internal prices but need pricing information for display purposes or for other reasons that are not required to complete a transaction.

Petitioner Exhibit 1002-2036
CSC ServiceWorks – Ex. 1008
Page 212 of 270

9.5.3 MODE THREE

In this example session the USD selects the item to vend and is aware of the vend price of the item. The USD must issue a vend request and the VMC then approves or denies the requested vend. The VMC then polls the USD for vend success or vend fail.

VMC	MDB Data	Explanation	USD
⇒	**42**	VMC polls the USD.	
	01+03+02+00+1E	USD requests vend for item at in USD with price of 30 coin factors.	⇐
⇒	**<ACK>**	VMC acks the USD vend request.	
⇒	**43+ 00** or **01**	VMC approves or denies vend request.	
	<ACK>	USD acks receipt of approval or denial.	⇐
⇒	**42**	VMC polls the USD.	
	02	USD responds: vend complete	⇐
⇒	**<ACK>**	VMC acks vend outcome.	

Petitioner Exhibit 1002-2037
CSC ServiceWorks – Ex. 1008
Page 213 of 270

9.6 Examples - Data Block Transfers

This section contains two examples in which data blocks are transferred between the VMC and the USD and vice versa.

9.6.1 Data Block Transfer from VMC to USD

In this example the VMC wishes to send two data blocks to the USD. To do this, the VMC uses the expansion 02 command to advise the USD of it's request to send data and also to identify the number of data blocks it wishes to send. In response, the USD uses a poll 09 to request the transmission of a data block with the block number enumerated as part of it's poll response. The VMC then uses a different expansion command (03) to send the data to the USD.

VMC	MDB Data	Explanation	USD
⇒	**47+02+02**	VMC issues a request to send two data blocks to the USD	
	<ACK>	USD acks receipt of the request	⇐
⇒	**42**	VMC polls the USD	
	09+00+01	USD responds with a request to receive data block number 01 from the VMC	⇐
⇒	**<ACK>**	VMC acks receipt of block number	
⇒	**47+03+01+21+22+23**	VMC transmits block number 01 containing data: 21, 22, and 23.	
	<ACK>	USD acks receipt of the data block	⇐
⇒	**42**	VMC polls the USD.	
	09+00+02	USD responds with a request to receive data block number 02 from the VMC.	⇐
⇒	**<ACK>**	VMC acks receipt of the block number.	
⇒	**47+03+02+24+25+26**	VMC transmits block number 02 containing data: 24, 25, and 26.	
	<ACK>	USD acks receipt of the data block	⇐

Petitioner Exhibit 1002-2038
CSC ServiceWorks – Ex. 1008
Page 214 of 270

9.6.2 Data Block Transfer from USD to VMC

In this example the USD wishes to send two data blocks to the VMC. To do this, the USD makes use of the Poll 09 command to inform the VMC of it's request to send data and also to identify the number of data blocks it wishes to send. In response, the VMC uses expansion 04 command to request the transmission of a data block by the individual block number. The USD then uses the poll 09 response to send the data blocks to the VMC.

VMC	MDB Data	Explanation	USD
⇒	**42**	VMC polls the USD	
	09+01+02	USD responds with a request to send 2 data blocks to the VMC	⇐
⇒	**<ACK>**	VMC acks request to send data	
⇒	**47+04+01**	VMC responds with a request to receive data block number 01 from the USD	
	<ACK>	USD acks receipt of block number request	⇐
⇒	**42**	VMC polls the USD	
	09+02+01+55+56+57	USD responds by transmitting block number 01 containing data 55, 56, and 57.	⇐
⇒	**<ACK>**	VMC acks receipt of data	
⇒	**47+04+02**	VMC responds with a request to receive data block number 02 from the USD	
	<ACK>	USD acks receipt of block number request	⇐
⇒	**42**	VMC polls the USD	
	09+02+02+58+59+60	USD responds by transmitting block number 02 containing data 58, 59, and 60.	⇐
⇒	**<ACK>**	VMC acks receipt of data	

Petitioner Exhibit 1002-2030
CSC ServiceWorks – Ex. 1008
Page 215 of 270

(this page intentionally left blank)

Petitioner Exhibit 1002-2040
CSC ServiceWorks – Ex. 1008
Page 216 of 270

Section 10

Coin Hopper or Tube - Dispenser
VMC/Peripheral Communication Specifications

10.1 Introduction

This section defines the communication bytes sent and received by a coin dispensing device, which may be in the form of a hopper or tube device. As defined in Section 2.3, the dispenser's address is 01011xxxB (58H).

Unless stated otherwise, all information is assumed to be in a binary format

10.2 VMC Commands

Command	Hex Code	Description
RESET	58H	Command for dispenser to self-reset
SETUP	59H	Request for dispenser setup.
DISPENSER STATUS	5AH	Request for dispenser tube / hopper status and coin count.
POLL	5BH	Request for dispenser activity status.
MANUAL DISPENSE	5CH	Signifies coin types allowable for coin dispensing. This command is followed by setup data. See command format section.
ENABLE		
DISPENSE *	5DH	Command to dispense coins. Followed by coin type or value to dispense. See command format section.
PAYOUT *	5EH	Command to determine value of coins dispensed. Followed by payout status or value poll. See command format section.
EXPANSION *	5FH	Command to allow addition of features, File Transport Layer, and future enhancements. See command format section.

Petitioner Exhibit 1002-2041
CSC ServiceWorks – Ex. 1008
Page 217 of 270

* **NOTE:** DISPENSE, PAYOUT, and EXPANSION commands are always followed by a "sub-command."

Petitioner Exhibit 1002-2042
CSC ServiceWorks – Ex. 1008
Page 218 of 270

10.3 VMC Command Format

VMC Command	Code	VMC Data
RESET	58H	No data bytes

This command is the vehicle that the VMC should use to tell the dispenser that it should return to its default operating mode and initialize internal hardware systems. With the exception of the ACK response, it should abort all communication until otherwise instructed by the VMC.

The following initialization sequence is recommended. It should be used after "power up" or after issuing the Bus Reset (pulling the transmit line "active" for a minimum of 100 mS).

RESET – 58h
POLL – 5Bh
To obtain "JUST RESET" response

SETUP – 59h
To obtain dispenser level and configuration information

EXPANSION IDENTIFICATION – 5F 00h
To obtain additional dispenser information and options

EXPANSION FEATURE ENABLE – 5F 01h
To enable desired options

DISPENSER STATUS – 5Ah (Note 1)
To obtain dispenser status / change information

MANUAL DISPENSE ENABLE – 5Ch
To enable and disable manual coin pay-out if desired

No power above idle current can be drawn until after the first POLL following the RESET command. Also, the JUST RESET response to the POLL command must be delayed until any high current usage has been completed.

The dispenser must hold its response of the DISPENSER status until a valid current reading from the sensor system is achieved.

Petitioner Exhibit 1002-2048
CSC ServiceWorks – Ex. 1008
Page 219 of 270

VMC Command	Code	Dispenser Response Data
SETUP	59H	26 bytes: Z1 - Z26

Z1 = Dispenser Feature Level - 1 byte

Indicates the feature level of the dispenser. This will distinguish the dispensers feature level to the VMC. Currently only level 1 is supported.

Z2 - Z3 = Country / Currency Code - 2 bytes

The packed BCD currency code of the dispenser is sent with the left most digit a 1. See Appendix A1 for the latest version of the ISO 4217 numeric currency code. For example, the code for the US dollar is 18 40H (Z2 = 18 and Z3 = 40) and for the Euro is 1978 (Z2 = 19 and Z3 = 78).

Z4 = Coin Scaling Factor - 1 byte

All dispensed coin values must be evenly divisible by this number. For example, this could be set to 05H for the USA nickel.

Z5 = Decimal Places - 1 byte

Indicates the number of decimal places on a credit display. For example, this could be set to 02H in the USA.

Z6 = Application Maximum Response Time (seconds) – 1 byte
The maximum length of time a dispenser will require to provide a response to any command from the VMC. The value reported here supercedes the dispenser's default NON-RESPONSE time defined in section 10.4 if the value reported here is greater.

Z7 – Z8 = Bit set, if coin disabled by dispenser (i.e. switch).

Z9 – Z10 = Bit set, if coin is self filling.

Z11 - Z26 = Coin Type Credit - 16 bytes

Indicates the value of coin types 0 to 15. Values must be sent in ascending order. This number is the coin's monetary value divided by the coin scaling factor. Unused coin types are sent as 00H. Unsent coin types are assumed to be zero. It is not necessary to send all coin types. Coin type credits sent as FFH are assumed to be vend tokens. That is, their value is assumed to be worth one vend.

Petitioner Exhibit 1002-2044
CSC ServiceWorks – Ex. 1008
Page 220 of 270

The byte position in the 16 byte string indicates the coin type(s). For example, the first byte sent would indicate the value of coin type 0, the second byte sent would indicate the value of coin type 1, and so on. For example, the USA coin types may be; Coin type 0 = nickel, Coin type 1 = dime, Coin type 2 = quarter, Coin type 3 = dollar.

Petitioner Exhibit 1002-2945
CSC ServiceWorks – Ex. 1008
Page 221 of 270

VMC Command	Code	Dispenser Response Data
DISPENSER STATUS	5AH	34 bytes: Z1 – Z34

Z1 - Z2 = Dispenser Full Status - 2 bytes

Indicates status of coin tube / hopper for coin types 0 to 15.

b15 b14 b13 b12 b11 b10 b9 b8 | b7 b6 b5 b4 b3 b2 b1 b0
Z1 Z2

A bit is set to indicate a full dispenser. For example, bit 7 = set would indicate the dispenser for coin type 7 is full.

Z3 – Z34 = Coin Count - 32 bytes

Indicates the greatest number of coins that the dispenser "knows" definitely are present in the coin tube / hopper. A word (2bytes) position in the 32 byte string indicates the number of coins in a tube / hopper for a particular coin type. For example, the first 2 bytes sent indicate the number of coins in a tube / hopper for coin type 0. Unsent bytes are assumed to be zero. For tube / hopper counts greater than 65535, counts should remain at 65535.

NOTE: If a dispenser can detect a tube or hopper jam, defective tube or hopper sensor, or other malfunction, it will indicate the tube / hopper is "bad" by sending a tube / hopper full status and a count of zero for the malfunctioning coin type.

VMC Command	Code	Dispenser Response Data
POLL	5BH	32 bytes: Z1 – Z32

Z1 - Z32 = Dispenser Activity - 32 bytes

Indicates the dispenser activity. If there is nothing to report, the dispenser should send only an ACK. Otherwise, the only valid responses are:

Coins Dispensed:

Z1 (10yzxxxx)

z	z=1 for manual dispense z=0 to report a non manual (automatic) dispense
y	y=1 For payout complete.
xxxx	The coin type dispensed (0 to 15)

Petitioner Exhibit 1002-2946
CSC ServiceWorks – Ex. 1008
Page 222 of 270

Z2 - Z3	The number of coins dispensed.
Z4 – Z5	The number of coins in the dispenser.

Petitioner Exhibit 1002-2947
CSC ServiceWorks – Ex. 1008
Page 223 of 270

Status:

(00000001) = Escrow request[1] - An escrow lever activation has been detected. If a button is present and activated.

(00000010) = Dispenser Payout Busy[2] - The dispenser is busy activating payout devices.

(00000011) = Not Used

(00000100) = Defective Dispenser Sensor[1] - The dispenser has detected one of the dispenser sensors behaving abnormally.

(00000101) = Not Used

(00000110) = Dispenser did not start[1].

(00000111) = Dispenser Jam[1] - A dispenser payout attempt has resulted in jammed condition.

(00001000) = ROM checksum error[1] - The dispensers internal checksum does not match the calculated checksum.

(00001001) = Not Used

(00001010) = Not Used

(00001011) = Dispenser was "Just Reset"[1] - The dispenser has detected a Reset condition and has returned to its power-on idle condition.

(00001100) = Not Used

(00001101) = Not Used

(00001110) = Not Used

(00001111) = Filled key pressed[1] – The VMC should request a new DISPENSER STATUS.

NOTES: The dispenser may send several of one type activity, up to 16 bytes total. This will permit zeroing counters such as inventory and status.

1 Sent once each occurrence.
2 Sent once each POLL

Petitioner Exhibit 1002-2048
CSC ServiceWorks – Ex. 1008
Page 224 of 270

File Transport Layer POLLed responses:

Note that all FTL responses are defined in Section 2.6. For the coin dispenser, the source address will always be the dispenser (58H) as defined in Section 2.3.

Z1

1B REQ TO RCV The coin dispenser is requesting to receive data from a device or VMC.

Z2 = Destination address of response
Z3 = Source address of response (58H)
Z4 = File ID
Z5 = Maximum length
Z6 = Control

1C RETRY/DENY The coin dispenser is requesting a device or VMC to retry or deny the last FTL command.

Z2 = Destination address of response
Z3 = Source address of response (58H)
Z4 = Retry delay

1D SEND BLOCK The coin dispenser is sending a block of data (maximum of 31 bytes) to a device or VMC.

Z2 = Destination address of data
Z3 = Block #
Z4-Z34 = Data (maximum of 31 bytes)

1E OK TO SEND The coin dispenser is indicating that it is OK for a device or VMC to send it data.

Z2 = Destination address of response
Z3 = Source address of response (58H)

1F REQ TO SEND The coin dispenser is requesting to send data to a device or VMC.

Z2 = Destination address of response
Z3 = Source address of response (58H)
Z4 = File ID
Z5 = Maximum length
Z6 = Control

Petitioner Exhibit 1002-2040
CSC ServiceWorks – Ex. 1008
Page 225 of 270

Petitioner Exhibit 1002-2950
CSC ServiceWorks – Ex. 1008
Page 226 of 270

VMC Command	Code	VMC Data
MANUAL DISPENSE ENABLE	5CH	2 bytes: Y1 – Y2

Y1 - Y2 = Manual Dispense Enable - 2 bytes

b15 b14 b13 b12 b11 b10 b9 b8 | b7 b6 b5 b4 b3 b2 b1 b0
Y1 Y2

A bit is set to indicate dispense enable. For example, bit 2 is set to enable dispensing of coin type 2. This command enables/disables manual dispensing using optional inventory switches. All manual dispensing switches are automatically disabled upon reset.

VMC Command	Code	Sub-command	VMC Data
DISPENSE COINS	5DH	00H	3 bytes: Y1 – Y3

b7 b6 b5 b4 b3 b2 b1 b0
Y1

Bits b3, b2, b1, b0 indicate coin type to be dispensed. Valid codes are 0H to FH to indicate coin types 0 to 15.

Bits b7, b6, b5, b4 = 0

Y2 - Y3 = Number of coins to be dispensed of coin type defined in Y1

There is no defined limit on how long the actual dispense takes since the command allows for up to 65535 coins to be paid out. The payout cycle begins when the dispenser ACKs the VMC's DISPENSE (5DH) command. This cycle typically lasts a minimum of 100 mS and ends when the dispenser stops dispensing the desired number of coins. VMCs should monitor the Dispenser Payout Busy and Dispenser Activity response to the POLL (5B) command to determine when the entire payout cycle is completed.

VMC Command	Code	Sub-command	VMC Data
DISPENSE VALUE	5DH	01H	2 bytes: Y1, Y2

Y1 – Y2 = Value of coins to be paid out.

Petitioner Exhibit 1002-2951
CSC ServiceWorks – Ex. 1008
Page 227 of 270

Y1 and Y2 are defined as the value of coins and this value is expressed as the number of coin scaling factors that would sum to the value. For example, in a USA system using a scaling factor of 05, if the change to be paid out is 75 cents, then Y1 will equal fifteen. That is, the sum of fifteen nickels equal 75 cents. The coin dispenser will determine which actual denominations of coins will be paid out. In the 75 cent example, the coins may be 3 quarters; or, 7 dimes & 1 nickel; or, 2 quarters & 2 dimes & 1 nickel, etc. The actual coins dispensed and if the dispense is finished can be acquired via the PAYOUT STATUS (5E, 00) and PAYOUT VALUE POLL (5E, 01).

Petitioner Exhibit 1002-2952
CSC ServiceWorks – Ex. 1008
Page 228 of 270

VMC Command	Code	Sub-command	VMC Data	Dispenser Response
PAYOUT STATUS	5E	00H	None	32 bytes: Z1-Z32

Z1 – Z32 = Number of each coin type paid out - 32 bytes (2 bytes per coin type).

This is the dispenser's response to the last VMC DISPENSE VALUE command (5DH sub command 01H). Bytes are sent in ascending order of coin types. A bytes position in the string indicates the coin type. That is, bytes one and two are the number of coins for coin type 1, bytes three and four are the number of coins for coin type two, and so on. Unsent bytes above the coin types dispensed are assumed to be zero.

The dispenser clears payout data after an ACK response from the VMC.

The VMC should compare the value of the coins paid out to the (5DH) DISPENSE VALUE command's Y2-Y3.

NOTES:

1) If the dispenser's payout is busy it will respond to the PAYOUT STATUS command with an ACK only.

2) If no coins have been paid out, at least one zero valued data byte must be sent.

3) There is no defined limit on how long the actual payout takes. See dispense command (5DH) for further details

VMC Command	Code	Sub-command	VMC Data	Dispenser Response Data
PAYOUT VALUE POLL	5EH	01H	None	2 bytes: Z1-Z2

Z1 – Z2 = Dispenser Payout Activity - 2 bytes

An interval value (scaled) which indicates the amount of paid out change since the previous PAYOUT VALUE POLL (or between the initial DISPENSE VALUE command (5DH sub command 01H) and the first PAYOUT VALUE POLL).

Petitioner Exhibit 1002-2958
CSC ServiceWorks – Ex. 1008
Page 229 of 270

A 00H response indicates no coins were paid out since the previous PAYOUT VALUE POLL (or the initial DISPENSE VALUE command (5DH sub command 01H)).

An ACK only indicates that the change payout is finished. This should be followed by the PAYOUT STATUS command (5EH-00H) to obtain the complete payout data.

NOTE: The initial intent of this command is to determine the amount of change paid out so that the credit display can be decremented as coins are dispensed.

Petitioner Exhibit 1002-2054
CSC ServiceWorks – Ex. 1008
Page 230 of 270

VMC Command	Code	Sub-Command	Dispenser Response Data
EXPANSION COMMAND	5FH	00H IDENTIFICATION	33 bytes: Z1 - Z33

Z1 - Z3 = Manufacturer Code - 3 bytes
Identification code for the equipment supplier. Sent as ASCII characters. Currently defined codes are listed in the **EVA** document entitled "***European Vending Association Data Transfer Standard***" (**EVA-DTS**), the Audit Data Lists section, sub-section 2, "Manufacturer Codes".

Z4 - Z15 = Serial Number - 12 bytes

Factory assigned serial number. All bytes must be sent as ASCII characters, zeros (30H) and blanks (20H) are acceptable.

Z16 - Z27 = Model Number - 12 bytes

Manufacturer assigned model number. All bytes must be sent as ASCII characters, zeros (30H) and blanks (20H) are acceptable.

Z28 - Z29 = Software Version - 2 bytes

Current software version. Must be sent in packed BCD.

Z30 - Z33 = Optional Features - 4 bytes

Each of the 32 bits indicate an optional features availability. If the bit is set the feature is available. Bits should be sent in descending order, i.e. bit 31 is sent first and bit 0 is sent last. Currently defined options are:

B0 - File Transport Layer (FTL) supported as defined in Section 2.6.

B1 - B31 Available for future use

VMC Command	Code	Sub-Command	VMC Data
EXPANSION COMMAND	5FH	01H FEATURE ENABLE	4 bytes: Y1 - Y4

Petitioner Exhibit 1002-2955
CSC ServiceWorks – Ex. 1008
Page 231 of 270

This command is used to enable each of the optional features defined in Z30-Z33 above. To enable a feature a bit is set to one. **All optional features are disabled after reset.**

Petitioner Exhibit 1002-2956
CSC ServiceWorks – Ex. 1008
Page 232 of 270

VMC Command	Code	Sub-command	VMC Data	Dispenser Response
EXPANSION COMMAND	5FH **FTL**	FAH REQ TO RCV	Y1-Y5	Z1 - Zn (immediate or POLLed)

The VMC is requesting to receive data from the dispenser whose destination address will always be (58H). Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 = Destination address of command (58H)
Y2 = Source address of command
Y3 = File ID
Y4 = Maximum length
Y5 = Control

Z1 = 1DH which indicates SEND BLOCK
Z2 = Destination address of data
Z3 = Block #
Z4 - Z34 = Data (maximum of 31 bytes)

or

Z1 = 1CH which indicates RETRY / DENY
Z2 = Destination address of response
Z3 = Source address of response (58H)
Z4 = Retry delay

VMC Command	Code	Sub-command	VMC Data	Dispenser Response
EXPANSION COMMAND	5FH **FTL**	FBH RETRY / DENY	Y1-Y3	None

The VMC is retrying, denying, or aborting a data transfer to/from the dispenser whose destination address will always be (58H). Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 = Destination address of command (58H)
Y2 = Source address of command
Y3 = Retry delay

Petitioner Exhibit 1002-2957
CSC ServiceWorks – Ex. 1008
Page 233 of 270

VMC Command	Code	Sub-command	VMC Data	Dispenser Response
EXPANSION COMMAND	5FH	FCH **FTL** SEND BLOCK	Y1-Y33	None

The VMC is sending data to the dispenser whose destination address will always be (58H). Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 = Destination address of command & data (58H)
Y2 = Block #
Y3 - Y33 = Data (maximum of 31 bytes)

VMC Command	Code	Sub-command	VMC Data	Dispenser Response
EXPANSION COMMAND	5FH	FDH **FTL** OK TO SEND	Y1-Y2	Z1-Z34 (immediate or POLLed)

The VMC is indicating that it is OK for the dispenser to transfer data. The destination address will always be the dispenser (58H). Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 = Destination address of command (58H)
Y2 = Source address of command

Z1 = 1DH which indicates SEND BLOCK
Z2 = Destination address of data
Z3 = Source address of data
Z4 - Z34 = Data (maximum of 31 bytes)

Petitioner Exhibit 1002-2058
CSC ServiceWorks – Ex. 1008
Page 234 of 270

VMC Command	Code	Sub-command	VMC Data	Dispenser Response
EXPANSION COMMAND	5FH	FEH **FTL** REQ TO SEND	Y1-Y5	Z1 (immediate or POLLed)

The VMC is requesting to send data to the dispenser whose destination address will always be (58H). Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 = Destination address of command (58H)
Y2 = Source address of command
Y3 = File ID
Y4 = Maximum length
Y5 = Control

Z1 = 1EH which indicates OK TO SEND
Z2 = Destination address of response
Z3 = Source address of response (58H)

or

Z1 = 1CH which indicates RETRY / DENY
Z2 = Destination address of response
Z3 = Source address of response (58H)
Z4 = Retry delay

VMC Command	Code	Sub-command	VMC Data	Dispenser Response
EXPANSION COMMAND	5FH	FFH DIAGNOSTICS	Y1-Yn	Z1-Zn

Y1 - Yn = Device manufacturer specific instruction for implementing various manufacturing or test modes. Y1 - Yn implies that any number of bytes can be used for the VMC data to the peripheral.

Z1 - Zn = Device manufacturer specific responses after receiving manufacturing or test instructions. Z1 - Zn implies that any number of bytes can be used for the Dispenser response data from the peripheral.

Petitioner Exhibit 1002-2959
CSC ServiceWorks – Ex. 1008
Page 235 of 270

10.4 Dispenser Non-Response Time

The default maximum non-response time for the dispenser is 5 seconds. This is the maximum time for which a dispenser will not respond to a command or a POLL with ACK, NAK or a message. The "Application Maximum Response Time" reported in byte Z6 of the SETUP (10.3) supersedes this default value if Z6 is greater.

10.5 Dispenser Power Requirements

The current draw for any dispenser must fall within the following limits. All measurements are at the minimum VMC voltage output.

Idle mode = 200 mA. (max.) continuous

Coin payout = 2.5 A. (max.) for up to 15 seconds per coin dispensed. This is the maximum for all dispensers operating simultaneously in this unit.

Petitioner Exhibit 1002-2060
CSC ServiceWorks – Ex. 1008
Page 236 of 270

Appendix 1

Currency Codes

A1.1 Information

The following **Tables of Codes for the Representation of Currencies and Funds** are provided by the Secretariat of ISO 4217 MA. It is provided here to be used for the MDB currency code information sent between the credit peripherals and the VMC.

Table A.1 Currency and Funds Code List (English alphabetical order by entity)

Table A.2 Funds Codes Registered with the Maintenance Agency

Table A.3 Codes for Historic Denominations of Currencies and Funds

A1.2 MDB/ICP Use

As stated in the individual credit device sections, the two byte, packed BCD country / currency code of the coin changer, bill validator, and card reader devices can be sent in two different forms depending on the value of the left most BCD digit .

If the left most digit is a 0, the International Telephone Code is used to indicate the country that the reader is set-up for.

For example, the USA telephone code is 001 which translates into the MDB code as **00 01**h (Zx = **00**h and Zy = **01**h).

If the left most digit is a 1, the latest version of the ISO 4217 numeric currency code is used as listed in this Appendix.

For example, the code for the US dollar is 840 which translates into the MDB code as **18 40**h (Zx = **18**h and Zy = **40**h).

The code for the Euro is 978 which translates into the MDB code as **1978**h (Zx = **19**h and Zy = **78**h).

FFFFh should be used if the country code in unknown (Zx = **FF**h and Zy = **FF**h).

Note that for level 3 cashless readers, it is mandatory to use the the ISO 4217 numeric currency code.

Petitioner Exhibit 1002-2961
CSC ServiceWorks – Ex. 1008
Page 237 of 270

Table A.1 Currency and Funds Code List (English alphabetical order by entity)

ENTITY	Currency	Code		Decimal Position
		Alphabetic	Numeric	
AFGHANISTAN	Afghani	AFA	004	2
ALBANIA	Lek	ALL	008	2
ALGERIA	Algerian Dinar	DZD	012	2
AMERICAN SAMOA	US Dollar	USD	840	2
ANDORRA	Spanish Peseta	ESP	724	0
	French Franc	FRF	250	2
	Andorran Peseta	ADP	020	0
ANGOLA	New Kwanza	AON	024	2
	Kwanza Reajustado	AOR	982	2
ANGUILLA	East Caribbean Dollar	XCD	951	2
ANTARCTICA	No universal currency			
ANTIGUA AND BARBUDA	East Caribbean Dollar	XCD	951	2
ARGENTINA	Argentine Peso	ARS	032	2
ARMENIA	Armenian Dram	AMD	051	2
ARUBA	Aruban Guilder	AWG	533	2
AUSTRALIA	Australian Dollar	AUD	036	2
AUSTRIA	Schilling	ATS	040	2
AZERBAIJAN	Azerbaijanian Manat	AZM	031	2
BAHAMAS	Bahamian Dollar	BSD	044	2
BAHRAIN	Bahraini Dinar	BHD	048	3
BANGLADESH	Taka	BDT	050	2
BARBADOS	Barbados Dollar	BBD	052	2
BELARUS	Belarussian Ruble	BYB	112	0
	Belarussian Ruble	BYR	974	0
BELGIUM	Belgian Franc	BEF	056	0
BELIZE	Belize Dollar	BZD	084	2
BENIN	CFA Franc BCEAO+	XOF	952	0
BERMUDA	Bermudian Dollar (customarily known as Bermuda Dollar)	BMD	060	2
BHUTAN	Indian Rupee	INR	356	2
	Ngultrum	BTN	064	2

+ CFA Franc BCEAO; Responsible authority: Banque Centrale des Etats de

Petitioner Exhibit 1002-2062
CSC ServiceWorks – Ex. 1008
Page 238 of 270

l'Afrique de l'Ouest.

Petitioner Exhibit 1002-2068
CSC ServiceWorks – Ex. 1008
Page 239 of 270

Table A.1 (Continued)

ENTITY	Currency	Code		Decimal
		Alphabetic	Numeric	Position
BOLIVIA	Boliviano	BOB	068	2
	Mvdol*	BOV	984	2
BOSNIA & HERZEGOVINA	Convertible Marks	BAM	977	2
BOTSWANA	Pula	BWP	072	2
BOUVET ISLAND	Norwegian Krone	NOK	578	2
BRAZIL	Brazilian Real	BRL	986	2
BRITISH INDIAN OCEAN TERRITORY	US Dollar	USD	840	2
BRUNEI DARUSSALAM	Brunei Dollar	BND	096	2
BULGARIA	Lev	BGL	100	2
	Bulgarian LEV	BGN	975	2
BURKINA FASO	CFA Franc BCEAO+	XOF	952	0
BURUNDI	Burundi Franc	BIF	108	0
CAMBODIA	Riel	KHR	116	2
CAMEROON	CFA Franc BEAC#	XAF	950	0
CANADA	Canadian Dollar	CAD	124	2
CAPE VERDE	Cape Verde Escudo	CVE	132	2
CAYMAN ISLANDS	Cayman Islands Dollar	KYD	136	2
CENTRAL AFRICAN REPUBLIC	CFA Franc BEAC#	XAF	950	0
CHAD	CFA Franc BEAC#	XAF	950	0
CHILE	Chilean Peso	CLP	152	0
	Unidades de fomento*	CLF	990	0
CHINA	Yuan Renminbi	CNY	156	2
CHRISTMAS ISLAND	Australian Dollar	AUD	036	2
COCOS (KEELING) ISLANDS	Australian Dollar	AUD	036	2
COLOMBIA	Colombian Peso	COP	170	2
COMOROS	Comoro Franc	KMF	174	0

+ CFA Franc BCEAO; Responsible authority: Banque Centrale des Etats de l'Afrique de l'Ouest.

CFA Franc BEAC; Responsible authority: Banque des Etats de l'Afrique Centrale.

- Funds code [See table A.2(E) for definitions of funds types].

Petitioner Exhibit 1002-2064 CSC ServiceWorks – Ex. 1008
Page 240 of 270

Table A.1 (Continued)

ENTITY Currency	Code	Decimal		
		Alphabetic	Numeric	Position
CONGO	CFA Franc BEAC#	XAF	950	0
CONGO, THE DEMOCRATIC REPUBLIC OF	Franc Congolais	CDF	976	2
COOK ISLANDS	New Zealand Dollar	NZD	554	2
COSTA RICA	Costa Rican Colon	CRC	188	2
COTE D'IVOIRE	CFA Franc BCEAO+	XOF	952	0
CROATIA	Kuna	HRK	191	2
CUBA	Cuban Peso	CUP	192	2
CYPRUS	Cyprus Pound	CYP	196	2
CZECH REPUBLIC	Czech Koruna	CZK	203	2
DENMARK	Danish Krone	DKK	208	2
DJIBOUTI	Djibouti Franc	DJF	262	0
DOMINICA	East Caribbean Dollar	XCD	951	2
DOMINICAN REPUBLIC	Dominican Peso	DOP	214	2
EAST TIMOR	Timor Escudo	TPE	626	0
	Rupiah	IDR	360	2
ECUADOR	US Dollar	ESD	840	2
EGYPT	Egyptian Pound	EGP	818	2
EL SALVADOR	El Salvador Colon	SVC	222	2
EQUATORIAL GUINEA	CFA Franc BEAC#	XAF	950	0
ESTONIA	Kroon	EEK	233	2
ERITREA	Nakfa	ERN	232	2
ETHIOPIA	Ethiopian Birr	ETB	230	2
FAEROE ISLANDS	Danish Krone	DKK	208	2
FALKLAND ISLANDS (MALVINAS)	Falkland Islands Pound	FKP	238	2

CFA Franc BEAC; Responsible authority: Banque des Etats de l'Afrique Centrale.

+ CFA Franc BCEAO; Responsible authority: Banque Centrale des Etats de l'Afrique de l'Ouest.

* Funds code [see Table A.2 (E) for definitions of funds types].

Petitioner Exhibit 1002-2065
CSC ServiceWorks – Ex. 1008
Page 241 of 270

Table A.1 (Continued)

ENTITY	Currency	Code	Decimal Position
		Alphabetic	Numeric	
FIJI	Fiji Dollar	FJD	242	2
FINLAND	Markka	FIM	246	2
FRANCE	French Franc	FRF	250	2
FRENCH GUIANA	French Franc	FRF	250	2
FRENCH POLYNESIA	CFP Franc	XPF	953	0
FRENCH SOUTHERN TERRITORIES	French Franc	FRF	250	2
GABON	CFA Franc BEAC#	XAF	950	0
GAMBIA	Dalasi	GMD	270	2
GEORGIA	Lari	GEL	981	2
GERMANY	Deutsche Mark	DEM	276	2
GHANA	Cedi	GHC	288	2
GIBRALTAR	Gibraltar Pound	GIP	292	2
GREECE	Drachma	GRD	300	2
GREENLAND	Danish Krone	DKK	208	2
GRENADA	East Caribbean Dollar	XCD	951	2
GUADELOUPE	French Franc	FRF	250	2
GUAM	US Dollar	USD	840	2
GUATEMALA	Quetzal	GTQ	320	2
GUINEA	Guinea Franc	GNF	324	0
GUINEA-BISSAU	Guinea-Bissau Peso	GWP	624	2
	CFA Franc BCEAO+	XOF	952	0
GUYANA	Guyana Dollar	GYD	328	2
HAITI	Gourde	HTG	332	2
	US Dollar	USD	840	2
HEARD AND MCDONALD ISLANDS	Australian Dollar	AUD	036	2
HONDURAS	Lempira	HNL	340	2

CFA Franc BEAC; Responsible authority: Banque des Etats de l'Afrique Centrale.

+ CFA Franc BCEAO; Responsible authority: Banque Centrale des Etats de l'Afrique de l'Ouest.

Petitioner Exhibit 1002-2066
CSC ServiceWorks – Ex. 1008
Page 242 of 270

Table A.1 (Continued)

ENTITY Currency	Code	Decimal		
		Alphabetic	Numeric	Point
HONG KONG	Hong Kong Dollar	HKD	344	2
HUNGARY	Forint	HUF	348	2
ICELAND	Iceland Krona	ISK	352	2
INDIA	Indian Rupee	INR	356	2
INDONESIA	Rupiah	IDR	360	2
INTERNATIONAL MONETARY FUND (IMF)**	SDR	XDR	960	N.A.
IRAN (ISLAMIC REPUBLIC OF)	Iranian Rial	IRR	364	2
IRAQ	Iraqi Dinar	IQD	368	3
IRELAND	Irish Pound	IEP	372	2
ISRAEL	New Israeli Sheqel*	ILS	376	2
ITALY	Italian Lira	ITL	380	0
JAMAICA	Jamaican Dollar	JMD	388	2
JAPAN	Yen	JPY	392	0
JORDAN	Jordanian Dinar	JOD	400	3
KAZAKHSTAN	Tenge	KZT	398	2
KENYA	Kenyan Shilling	KES	404	2
KIRIBATI	Australian Dollar	AUD	036	2
KOREA, DEMOCRATIC PEOPLE'S REPUBLIC OF	North Korean Won	KPW	408	2
KOREA, REPUBLIC OF	Won	KRW	410	0

* Currency name was effective 4th September 1985

** This entry is not derived fron ISO 3166, but is included here in alphabetic sequence for convenience.

Petitioner Exhibit 1002-2967
CSC ServiceWorks – Ex. 1008
Page 243 of 270

Table A.1 (Continued)

ENTITY	Currency	Code		Decimal Point
		Alphabetic	Numeric	
KUWAIT	Kuwaiti Dinar	KWD	414	3
KYRGYZSTAN	Som	KGS	417	2
LAO PEOPLE'S DEMOCRATIC REPUBLIC	Kip	LAK	418	2
LATVIA	Latvian Lats	LVL	428	2
LEBANON	Lebanese Pound	LBP	422	2
LESOTHO	Rand	ZAR	710	2
	(financial Rand)*	ZAL	991	2
	Loti	LSL	426	2
LIBERIA	Liberian Dollar	LRD	430	2
LIBYAN ARAB JAMAHIRIYA	Libyan Dinar	LYD	434	3
LIECHTENSTEIN	Swiss Franc	CHF	756	2
LITHUANIA	Lithuanian Litas	LTL	440	2
LUXEMBOURG	Luxembourg Franc	LUF	442	0
MACAU	Pataca	MOP	446	2
MACEDONIA, THE FORMER YUGOSLAV REPUBLIC OF	Denar	MKD	807	2
MADAGASCAR	Malagasy Franc	MGF	450	0
MALAWI	Kwacha	MWK	454	2
MALAYSIA	Malaysian Ringgit	MYR	458	2
MALDIVES	Rufiyaa	MVR	462	2
MALI	CFA Franc BCEAO+	XOF	952	0
MALTA	Maltese Lira	MTL	470	2
MARSHALL ISLANDS	US Dollar	USD	840	2
MARTINIQUE	French Franc	FRF	250	2
MAURITANIA	Ouguiya	MRO	478	2
MAURITIUS	Mauritius Rupee	MUR	480	2
MEXICO	Mexican Peso	MXN	484	2
	Mexican Unidad de Inversion (UDI)*	MXV	979	2
MICRONESIA	US Dollar	USD	840	2
MOLDOVA, REPUBLIC OF	Moldovan Leu	MDL	498	2
MONACO	French Franc	FRF	250	2

* Funds code [See table A.2(E) for definitions of funds types].

\+ CFA Franc BCEAO; Responsible authority: Banque Centrale des Etats de l'Afrique de l'Ouest.

Table A.1 (Continued)

Petitioner Exhibit 1002-2968
CSC ServiceWorks – Ex. 1008
Page 244 of 270

ENTITY	Currency	Code		Decimal Point
		Alphabetic	Numeric	
MONGOLIA	Tugrik	MNT	496	2
MONTSERRAT	East Caribbean Dollar	XCD	951	2
MOROCCO	Moroccan Dirham	MAD	504	2
MOZAMBIQUE	Metical	MZM	508	2
MYANMAR	Kyat	MMK	104	2
NAMIBIA	Rand	ZAR	710	2
	Namibia Dollar**	NAD	516	2
NAURU	Australian Dollar	AUD	036	2
NEPAL	Nepalese Rupee	NPR	524	2
NETHERLANDS	Netherlands Guilder	NLG	528	2
NETHERLANDS ANTILLES	Netherlands Antillian Guilder	ANG	532	2
NEW CALEDONIA	CFP Franc	XPF	953	0
NEW ZEALAND	New Zealand Dollar	NZD	554	2
NICARAGUA	Cordoba Oro	NIO	558	2
NIGER	CFA Franc BCEAO+	XOF	952	0
NIGERIA	Naira	NGN	566	2
NIUE	New Zealand Dollar	NZD	554	2
NORFOLK ISLAND	Australian Dollar	AUD	036	2
NORTHERN MARIANA ISLANDS	US Dollar	USD	840	2
NORWAY	Norwegian Krone	NOK	578	2
OMAN	Rial Omani	OMR	512	3
PAKISTAN	Pakistan Rupee	PKR	586	2
PALAU	US Dollar	USD	840	2

+ CFA Franc BCEAO; Responsible authority: Banque Centrale des Etats de l'Afrique de l'Ouest.

The lowest unit of recorded value for the Iraqi Dinar is the Dirham (1 Iraqi Dinar = 20 Dirhams).

** The Namibia Dollar becomes effective September 15th 1993

Table A.1 (Continued)

Petitioner Exhibit 1002-2060
CSC ServiceWorks – Ex. 1008
Page 245 of 270

ENTITY	Currency	Code Alphabetic	Code Numeric	Decimal Point
PANAMA	Balboa	PAB	590	2
	US Dollar	USD	840	2
PAPUA NEW GUINEA	Kina	PGK	598	2
PARAGUAY	Guarani	PYG	600	0
PERU	Nuevo Sol	PEN	604	2
PHILIPPINES	Philippine Peso	PHP	608	2
PITCAIRN	New Zealand Dollar	NZD	554	2
POLAND	Zloty	PLN	985	2
PORTUGAL	Portuguese Escudo	PTE	620	0
PUERTO RICO	US Dollar	USD	840	2
QATAR	Qatari Rial	QAR	634	2
REUNION	French Franc	FRF	250	2
ROMANIA	Leu	ROL	642	2
RUSSIAN FEDERATION	Russian Ruble	RUR	810	2
	Russian Ruble	RUB	643	2
RWANDA	Rwanda Franc	RWF	646	0
ST HELENA	St Helena Pound	SHP	654	2
ST KITTS - NEVIS	East Caribbean Dollar	XCD	951	2
SAINT LUCIA	East Caribbean Dollar	XCD	951	2
ST PIERRE AND MIQUELON	French Franc	FRF	250	2
SAINT VINCENT AND THE GRENADINES	East Caribbean Dollar	XCD	951	2
SAMOA	Tala	WST	882	2
SAN MARINO	Italian Lira	ITL	380	0
SAO TOME AND PRINCIPE	Dobra	STD	678	2
SAUDI ARABIA	Saudi Riyal	SAR	682	2

Petitioner Exhibit 1002-2970
CSC ServiceWorks – Ex. 1008
Page 246 of 270

Table A.1 (Continued)

ENTITY	Currency	Code		Decimal Point
		Alphabetic	Numeric	
SENEGAL	CFA Franc BCEAO+	XOF	952	0
SEYCHELLES	Seychelles Rupee	SCR	690	2
SIERRA LEONE	Leone	SLL	694	2
SINGAPORE	Singapore Dollar	SGD	702	2
SLOVAKIA	Slovak Koruna	SKK	703	2
SLOVENIA	Tolar	SIT	705	2
SOLOMON ISLANDS	Solomon Islands Dollar	SBD	090	2
SOMALIA	Somali Shilling	SOS	706	2
SOUTH AFRICA	Rand	ZAR	710	2
SPAIN	Spanish Peseta	ESP	724	0
SRI LANKA	Sri Lanka Rupee	LKR	144	2
SUDAN	Sudanese Dinar	SDD	736	2
SURINAME	Surinam Guilder	SRG	740	2
SVALBARD AND JAN MAYEN ISLANDS	Norwegian Krone	NOK	578	2
SWAZILAND	Lilangeni	SZL	748	2
SWEDEN	Swedish Krona	SEK	752	2
SWITZERLAND	Swiss Franc	CHF	756	2
SYRIAN ARAB REPUBLIC	Syrian Pound	SYP	760	2
TAIWAN, PROVINCE OF CHINA	New Taiwan Dollar	TWD	901	2
TAJIKISTAN	Tajik Ruble	TJR	762	0

+ CFA Franc BCEAO; Responsible authority: Banque Centrale des Etats de l'Afrique de l'Ouest.

Petitioner Exhibit 1002-2971
CSC ServiceWorks – Ex. 1008
Page 247 of 270

Table A.1 (Continued)

ENTITY	Currency	Code		Decimal
		Alphabetic	Numeric	Point
TANZANIA, UNITED REPUBLIC OF	Tanzanian Shilling	TZS	834	2
THAILAND	Baht	THB	764	2
TOGO	CFA Franc BCEAO+	XOF	952	0
TOKELAU	New Zealand Dollar	NZD	554	2
TONGA	Pa'anga	TOP	776	2
TRINIDAD AND TOBAGO	Trinidad and Tobago Dollar	TTD	780	2
TUNISIA	Tunisian Dinar	TND	788	3
TURKEY	Turkish Lira	TRL	792	0
TURKMENISTAN	Manat	TMM	795	2
TURKS AND CAICOS ISLANDS	US Dollar	USD	840	2
TUVALU	Australian Dollar	AUD	036	2
UGANDA	Uganda Shilling ++	UGX	800	0
UKRAINE	Hryvnia	UAH	980	2
UNITED ARAB EMIRATES	UAE Dirham	AED	784	2
UNITED KINGDOM	Pound Sterling	GBP	826	2
UNITED STATES	US Dollar	USD	840	2
	(Same day)*	USS	998	2
	(Next day)*	USN	997	2
UNITED STATES MINOR OUTLAYING ISLANDS	US Dollar	USD	840	2

+ CFA Franc BCEAO; Responsible authority: Banque Centrale des Etats de l'Afrique de l'Ouest.

++ The Uganda Shilling was denominated as from 18 May 1987.

* Funds code [See table A.2(E) for definitions of funds types].

Petitioner Exhibit 1002-2972
CSC ServiceWorks – Ex. 1008
Page 248 of 270

Table A.1 (Continued)

ENTITY	Currency	Code		Decimal
		Alphabetic	Numeric	Point
URUGUAY	Peso Uruguayo	UYU	858	2
UZBEKISTAN	Uzbekistan Sum	UZS	860	2
VANUATU	Vatu	VUV	548	0
VATICAN CITY STATE (HOLY SEE)	Italian Lira	ITL	380	0
VENEZUELA	Bolivar	VEB	862	2
VIETNAM	Dong	VND	704	2
VIRGIN ISLANDS (BRITISH)	US Dollar	USD	840	2
VIRGIN ISLANDS (U.S.)	US Dollar	USD	840	2
WALLIS AND FUTUNA ISLANDS	CFP Franc	XPF	953	0
WESTERN SAHARA	Moroccan Dirham	MAD	504	2
YEMEN	Yemeni Rial	YER	886	2
YUGOSLAVIA	New Dinar	YUM	891	2
ZAMBIA	Kwacha	ZMK	894	2
ZIMBABWE	Zimbabwe Dollar	ZWD	716	2

Petitioner Exhibit 1002-2978
CSC ServiceWorks – Ex. 1008
Page 249 of 270

Table A.1 (Continued)

ENTITYCurrency	Code	Decimal		
		Alphabetic	Numeric	Position
Entity not applicable	Gold	XAU	959	N.A.
	Bond Markets Units			
	European Composite Unit (EURCO)	XBA	955	N.A.
	European Monetary Unit (E.M.U.-6)***	XBB	956	N.A.
	European Unit of Account 9 (E.U.A.- 9)	XBC	957	N.A.
	European Unit of Account 17 (E.U.A.- 17)	XBD	958	N.A.
	Palladium	XPD	964	N.A.
	Platinum	XPT	962	N.A.
	Silver	XAG	961	N.A.

*** E.M.U.-6 is sometimes known as the European Currency Unit. This should not be confused with the settlement unit of the European Monetary Cooperation Fund (E.M.C.F.) which has the same name (see entry for 'European Monetary Cooperation Fund' in this table).

Petitioner Exhibit 1002-2074
CSC ServiceWorks – Ex. 1008
Page 250 of 270

Table A.1 (Continued)

ENTITY	Currency	Code		Decimal
		Alphabetic	Numeric	Position
Entity not applicable	Special settlement currencies			
	UIC-Franc	XFU	Nil	N.A.
	Gold-Franc	XFO	Nil	N.A.
	Codes specifically reserved for testing purposes	XTS	963	N.A.
	The codes assigned for transactions where no currency is involved are:	XXX	999	N.A.
	euro*	EUR*	978	2

* On 1 January 1999, the euro will become the currency of those Member States of the European Union which adopt the single currency in accordance with the Treaty establishing the European Community. This code has been issued now so that technical preparations can be started. The code element "EU" has been reserved by the ISO 3166 Maintenance Agency for use within ISO 4217 where "R" has been appended to make an acceptable mnemonic code.

Petitioner Exhibit 1002-2075
CSC ServiceWorks – Ex. 1008
Page 251 of 270

Table A.2 Funds Codes Registered with the Maintenance Agency

CURRENCY AUTHORITY	Currency	Fund Type	Code Alphabetic	Code Numeric	Decimal Position
BOLIVIA		Mvdol	BOV	984	2
CHILE		Unidades de Fomento	CLF	990	0
MEXICO		Mexican Unidad de Inversion (UDI)	MXV	979	2
UNITED STATES	US Dollar	Same day	USS	998	2
		Next day	USN	997	2

Definitions of the fund types listed above

BOV: For indexation purposes and denomination of certain finacial instruments (ex. treasury bills). The Mvdol is set daily by the Central Bank of Bolivia based upon the official USD/BOB rate.

CLF: This development unit has been approved by the Chilean government for use in insurance transactions (with effect from 10 April 1980).

ECV: A daily indexation mechanism set by the Ecuadorian Central Bank. The UVC is set according to the variation of the Consumer price Index (Urban), as compiled by the National Census and Statistics Institute (INEC).

MXV : The UDI is an inflation adjusted mechanism set by the Central Bank of Mexico according to the variation in the Mexican Consumer Price Index. The value of the UDI is expressed in terms of Mexican Pesos per UDI. It is used to denominate mortgage loans, some bank deposits with maturities of 3 month or more and Government bonds (UDIBONOS).

USN: "Next day" funds are immediately available for transfer in like funds, and subject to settlement, available the next business day for same day funds transfer or withdrawal in cash.

USS: "Same day" funds are immediately available for transfer today or for withdrawal in cash, subject to the settlement of the transaction through the payment mechanism used.

(USD designates the US Dollar, the currency designator when an accumlation of amounts contains more than one funds type.)

Petitioner Exhibit 1002-2976
CSC ServiceWorks – Ex. 1008
Page 252 of 270

Table A.3 Codes for Historic Denomination of Currencies and Funds

ENTITY	Historic Currencies	Code	Numeric	WD
ALBANIA	Old Lek	ALK *	-	12/89
ANGOLA	Kwanza	AOK	-	03/91
ARGENTINA	Peso Argentino	ARP	-	07/85
	Austral	ARA	-	01/92
	Peso	ARY*	-	
1989/1990				
BELGIUM	Convertible Franc	BEC	993	03/90
	Financial Franc	BEL	992	03/90
BOLIVIA	Peso	BOP	-	02/87
BOSNIA & HERZEGOVINA	Dinar	BAD	070	09/97
BRAZIL	Cruzeiro	BRB	-	03/86
	Cruzado	BRC	-	02/89
	New Cruzado	BRN	-	03/90
	Cruzeiro	BRE	076	08/93
	Cruzeiro Real	BRR	987	07/94
BULGARIA	Lev A/62	BGK*	-	
1989/1990				
	Lev A/52	BGJ*	-	
1989/1990				
BURMA#	N/A	BUK	-	02/90
CHINA	Peoples Bank Dollar	CNX*	-	12/89
CROATIA	Dinar	HRD	-	01/95
CZECHOSLOVAKIA	Krona A/53	CSJ*	-	1989/1990
	Koruna	CSK	200	03/93
ECUADOR	Sucre	ECS	218	9/00
	Unidad del Valor constante (UVC)*	ECV	983	9/00
EQUATORIAL GUINEA	Ekwele	GQE	226	06/86

Petitioner Exhibit 1002-2977
CSC ServiceWorks – Ex. 1008
Page 253 of 270

Ekwele	EQE*	-	12/89

* Non ISO code
Change in country name

Petitioner Exhibit 1002-2078
CSC ServiceWorks – Ex. 1008
Page 254 of 270

Table 3 (Continued)

ENTITY	Historic Currencies	Code	Numeric	WD
EUROPEAN MONETARY COOPERATION FUND (EMCF)**	European Currency Unit (E.C.U)	XEU	954	01/99
GERMAN DEMOCRATIC REPUBLIC	Mark der DDR	DDM	278	07/90 to 09/90
GEORGIA	Georgian Coupon	GEK	268	10/95
GUINEA	Syli	GNS	-	02/86
	Syli	GNE*	-	12/89
GUINEA BISSAU Between 1978-	Guinea Escudo	GWE	-	1981
ICELAND 1989/1990	Old Krona	ISJ*	-	
ISRAEL 1989/1990	Old Shekel	ILR*	-	
Between 1978-	Pound	ILP	-	1981
LESOTHO	Maloti	LSM	-	05/85
LAO	Kip Pot Pol	LAJ*	-	12/89
LATVIA	Latvian Ruble	LVR	-	12/94
LITHUANIA	Talonas	LTT	-	07/93
LUXEMBOURG	Convertible Franc	LUC	989	03/90
	Financial Franc	LUL	988	03/90
MALDIVES	Maldive Rupee	MVQ*	-	12/89
MALI	Mali Franc	MAF*	-	12/89
		MLF	446	11/84
MALTA	Maltese Pound	MTP	-	06/83
MEXICO	Mexican Peso	MXP	-	01/93

Petitioner Exhibit 1002-2979
CSC ServiceWorks – Ex. 1008
Page 255 of 270

* Non ISO code

Table 3 (Continued)

ENTITY	Historic Currencies	Code	Numeric	WD
MOZAMBIQUE Between 1978-1981	Mozambique Escudo	MZE	-	
NICARAGUA	Cordoba	NIC	-	10/90
PERU	Sol	PES	-	02/86
	Inti	PEI	-	07.91
1989/1990	Sol	PEH*	-	
POLAND	Zloty	PLZ	616	01/97
ROMANIA 1989/1990	Leu A/52	ROK*	-	
SOUTH AFRICA	Financial Rand	ZAL	991	03/95
SOUTHERN RHODESIA# Between 1978-1981	Rhodesian Dollar	RHD	-	
SPAIN Between 1981-1983	Spanish Peseta ("A" Account)	ESA	996	
	(convertible Peseta Accounts)	ESB	995	12/94
SUDAN	Sudanese Pound	SDP	-	06/98
UNION OF SOVIET SOCIALIST REPUBLICS#	Rouble	SUR	-	12/90
YEMEN, DEMOCRATIC OF	Yemeni Dinar	YDD	720	09/91
UGANDA	Uganda Shilling	UGS	-	05/87
1989/1990	Old Shilling	UGW*	-	

Petitioner Exhibit 1002-2080
CSC ServiceWorks – Ex. 1008
Page 256 of 270

UKRAINE	Karbovanet	UAK	804	09/96

* Non ISO code
Change in country name.

Petitioner Exhibit 1002-2081
CSC ServiceWorks – Ex. 1008
Page 257 of 270

Table 3 (Continued)

ENTITY	Historic Currencies	Code	Numeric	WD
URUGUAY	Old Uruguay Peso	UYN*	-	12/89
	Uruguayan Peso	UYP	-	03/93
VIETNAM 1989/1990	Old Dong	VNC*	-	
YUGOSLAVIA	New Yugoslavian Dinar	YUD	-	01/90
	Yugoslavian Dinar	YUN	890	11/95
ZAIRE	Zaire	ZRZ	-	02/94
	New Zaire	ZRN	180	06/99
ZIMBABWE	Rhodesian Dollar	ZWC*	-	12/89
ENTITY AND CURRENCY NOT APPLICABLE	RINET Funds Code	XRE	N/A	11/99

* Non ISO code

Petitioner Exhibit 1002-2082
CSC ServiceWorks – Ex. 1008
Page 258 of 270

ANNEX

INFORMATION TO BE PROVIDED BY THOSE MAKING APPLICATION FOR THE ISSUE OF NEW CODES, AMENDMENTS AND DELETIONS.

Applications for additions or changes to the code lists are acceptable from any source. However, on order to ensure rapid processing by the Secretaries, the information required from applicants has been laid down as follows:

(a) Name of entity

(b) Name of currency

(c) The institution responsible for the currency (name and place of operation).

(d) Requirements:

(1) Whether currency or funds code: if funds code, give definition and proposed use;

(2) If new code, make proposal;

(3) If revision, state existing code and make proposal;

(4) If deletion, indicate code to be deleted;

(e) Reason for application;

(f) Evidence of support (currency code only);

(g) Date of implementation (indicate if special conditions of urgency apply);

(h) Application submitted by (name, address, telephone, telex numbers, etc, of applicant);

(i) Date of application.

Applications should be addressed to

Miss A M Wadsworth Tel. (0181) 996 7466 National
Secretariat for ISO4217MA +44 181 996 7466 International
BSI
389 Chiswick High Road Fax (0181) 996 7466 National
London +44 181 996 7466 International
W4 4AL United Kingdom

Petitioner Exhibit 1002-2983
CSC ServiceWorks – Ex. 1008
Page 259 of 270

Appendix 2

Battery Operated Card Reader

A2.1 Special Application

The Battery Operated Card Reader described below is a special application of the MDB/ICP specification (non-standard) and is not sanctioned by NAMA. It is provided here to document an application that exists in use today.

A2.2 Extension to MDB/ICP – Card Reader Using Standby Feature

Some Vending machines use battery operated equipment. According to this feature, these machines and all devices used within these machines must provide a standby operating mode.

During standby operation - necessary for saving battery power while the machine is not in use - all devices shall consume a minimum standby current. Any device is equipped with some hardware wake-up mechanism. Both standby current and wake-up mechanism is to be defined in the device related hardware specification.

After wake-up, a device uses normal operating current, until a defined shutdown sequence is established and the device enters standby mode again.

The following specification shows the extensions and procedures for a normal MDB/ICP card reader and VMC-controller necessary to do wake-up and shut down sequences. The hardware specification related to wake-up is a separate BDTA-document. To understand the following details, it is necessary to know, that a separate bi-directional wake-up pin is applied to the card-reader. Pulling the wake-up line (from the card-reader while a card is inserted), both card-reader and VMC will be brought to normal operation mode.

Petitioner Exhibit 1002-2084
CSC ServiceWorks – Ex. 1008
Page 260 of 270

A2.3 Extension to MDB/ICP – SETUP Config Data

SETUP (11H)	Config Data (00H) Y1	VMC Feature Level Y2	Columns on Display Y3	Rows on Display Y4	Display Info Y5

Y1 : Configuration data.
VMC is sending its configuration data to reader.

Y2 : VMC Feature Level.
Indicates the feature level of the VMC. The available feature levels are:

01 - The VMC is not capable or will not perform the advanced features as specified in Table 1: COMMANDS & RESPONSES following Section 7.3.2. The reader will not provide advanced information to the VMC, but can do the advanced features internally (transparently to the VMC). The reader has no revaluation capability.

02 - The VMC is capable and willing to perform the advanced features as specified in Table 1: COMMANDS & RESPONSES following Section 7.3.2. The reader will provide advanced information to the VMC (if possible) and will not do the advanced features internally.

03 - The VMC is able to support level 02, but also supports some or all of the optional features listed in the EXPANSION ID command (i.e., file transfer, 32 bit credit, multi-currency / language features, negative vend, and / or data entry).

81H: VMC is Level 01, but battery operated.
82H: VMC is Level 02, but battery operated.
83H: VMC is Level 03, but battery operated.

Y3 : Columns on Display. The number of columns on the display. Set to 00H if the display is not available to the reader.

Y4 : Rows on Display.
The number of rows on the display.

Y5 : Display Information - xxxxxyyy
xxxxx = Unused
yyy = Display type
000 : Numbers, upper case letters, blank and decimal point.
001 : Full ASCII
010-111: Unassigned

Petitioner Exhibit 1002-2085
CSC ServiceWorks – Ex. 1008
Page 261 of 270

Reader Config Data (01H) Z1	Reader Feature Level Z2	Country / Currency Code High Z3	Country / Currency Code Low Z4	Scale Factor Z5	Decimal Places Z6	Application Maximum Response Time Z7	Miscellaneous Options Z8

Z1 : READER - Configuration data.
Indicates the payment media reader is responding to a SETUP - Configuration data request from the VMC.

Z2 : Reader Feature Level.
Indicates the feature level of the reader. Currently feature levels are:

01 - The reader is not capable or will not perform the advanced features as specified in Table 1: COMMANDS & RESPONSES following Section 7.3.2. The reader will not provide advanced information to the VMC, but can do the advanced features internally (transparently to the VMC). The reader has no revaluation capability.

02 - The reader is capable and willing to perform the advanced features as specified in Table 1: COMMANDS & RESPONSES following Section 7.3.2. The reader will provide advanced information to the VMC (if possible) and will not do the advanced features internally.

03 - The reader is able to support level 02, but also supports some or all of the optional features listed in the EXPANSION ID command (i.e., file transfer, 32 bit credit, multi-currency / language features, negative vend, and / or data entry).

80H: This bit is additionally set, if the reader is capable to work in battery operation mode and should be compared with the VMC against its own working mode. This is also done from the reader against the VMCs request in Y2.

Z3-Z4 : Country / Currency Code - packed BCD.
The packed BCD country / currency code of the changer can be sent in two different forms depending on the value of the left most BCD digit.

If the left most digit is a 0, the International Telephone Code is used to indicate the country that the changer is set-up for. For example, the USA code is 00 01H (Z3 = 00 and Z4 = 01).

If the left most digit is a 1, the latest version of the ISO 4217 numeric currency code is used (see Appendix A1). For example, the code for the US dollar is 18 40H (Z2 = 18 and Z3 = 40) and for the Euro is 1978 (Z3 = 19 and Z4 = 78). Use FFFFh if the country code in unknown.

Petitioner Exhibit 1002-2986
CSC ServiceWorks – Ex. 1008
Page 262 of 270

For level 3 cashless readers, it is mandatory to use the ISO 4217 numeric currency code (see Appendix A1).

Z5 : Scale Factor.
The multiplier used to scale all monetary values transferred between the VMC and the reader.

Z6 : Decimal Places.
The number of decimal places used to communicate monetary values between the VMC and the payment media reader.

All pricing information sent between the VMC and the payment media reader is scaled using the scale factor and decimal places. This corresponds to:

$$\text{ActualPrice} = P \cdot X \cdot 10^{-Y}$$

where P is the scaled value send in the price bytes, and X is the scale factor, and Y is the number of decimal places. For example if there are 2 decimal places and the scale factor is 5, then a scaled price of 7 will mean an actual of 0.35.

Z7 : Application Maximum Response Time - seconds.
The maximum length of time a reader will require to provide a response to any command from the VMC. The value reported here supercedes the payment reader's default NON-RESPONSE time defined in section 7.5 if the value reported here is greater.

Z8 : Miscellaneous Options - xxxxyyyy

xxxx:	Unused (must be set to 0)
yyyy:	Option bits
b0=0:	The payment media reader is NOT capable of restoring funds to the user's payment media or account. Do not request refunds.
b0=1:	The payment media reader is capable of restoring funds to the user's payment media or account. Refunds may be requested.
b1=0:	The payment media reader is NOT multivend capable. Terminate session after each vend.
b1=1:	The payment media reader is multivend capable. Multiple items may be purchased within a single session.
b2=0:	The payment media reader does NOT have a display.
b2=1:	The payment media reader does have its own display.
b3=0:	The payment media reader does NOT support the VEND/CASH SALE subcommand.
b3=1:	The payment media reader does support the VEND/CASH SALE subcommand.
b4-b7=0	Any future options must be covered by the EXPANSION COMMAND option bits.

Petitioner Exhibit 1002-2087
CSC ServiceWorks – Ex. 1008
Page 263 of 270

Note: The following changes are the only changes to upgrade to battery operated readers:

If a VMC is battery operated, it signals the card reader with the flag 80H to work in battery operation mode. Within byte Z2 the reader also sets the flag to 80H to signal standby feature capability.

If only one of both is in standby capability, this results in an configuration error and the manufacturers should deal with handling of this condition. Assume that at least one device will not enter standby mode and therefore battery lifetime is dramatically reduced!

A2.4 VMC-Reader Operation Sequences

The VMC and the Reader should operate during battery mode in the following way:

After wake-up, the VMC starts with the normal sequences:

Reset
Setup/Config
MAX/MIN-price
Identify
Enable
Poll

During these sequences, the VMC has two possibilities to signal the Card-Reader, not to enter standby-mode again:

Pulling the wake-up pin to low level
Running poll sequences in continuos timing.

If neither the wake-up pin is driven low, nor any command is further sent to the card reader, the reader enters standby state after its Application Maximum Response Time (normally defined to 5 sec in ICP, but sent in byte Z7 of status response)

During card operation, the sequences continue normally with

Begin Session

Petitioner Exhibit 1002-2088
CSC ServiceWorks – Ex. 1008
Page 264 of 270

Vend Request
Vend Accepted
Vend Success
Cancel Session/Session Complete

Whenever a cancel session or session complete command is received, the reader should stop all internal work after a defined timeout period (Application Maximum Response Time) is finished after the last command sequence and after the wake-up pin is not pulled low.

The VMC should stop polling after the cancel session or session complete command and additionally should no longer pull wake-up pin.

If even the reader or the VMC may wish any further communication (i.e. for additionally trailing display messages or multi vend purposes or etc.) the reader can use any non idle answer to the poll command (i.e. the display message) whereas the VMC can continue polling or pulling the wake-up pin.

Note that the wake-up pin may not be used from the reader to hold on operation, cause dynamic system consideration and of course holding more devices within the system in normal operation mode is not a good job.

The reader should be in a power saving mode after this timeout period where power consumption is less than 10 uA.

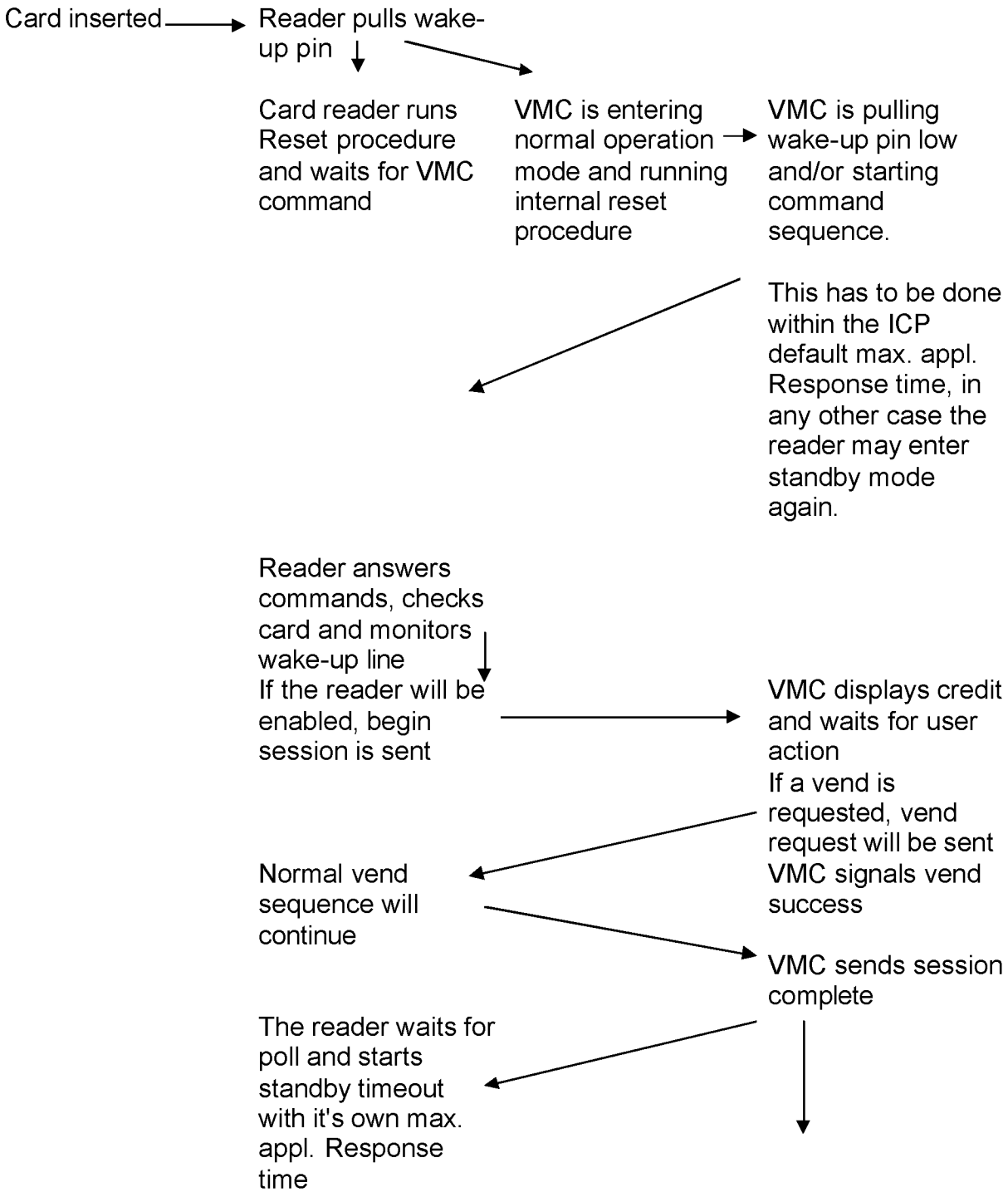
To allow the reader holding VMC operating, at least 5 poll have to be sent, after the cancel session or session complete. If any one of these polls is answered different with only a ACK, 5 polls have to be sent again. Note, that if a display message is sent, display time is added!

If the reader entered standby state, and a new card is inserted, the procedure starts a again.

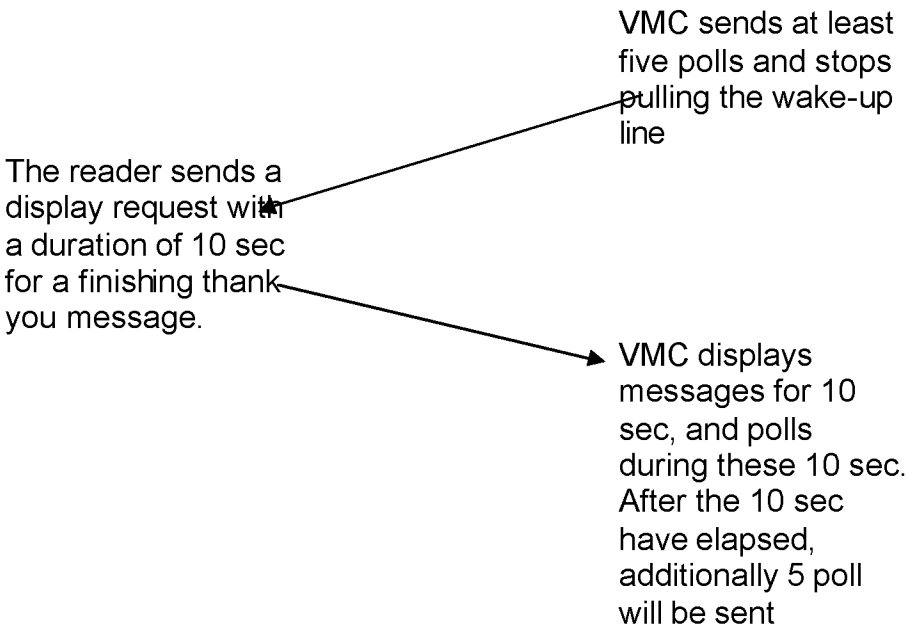
Whenever during this next session, the reader should avoid all unnecessary work, i.e. display messages like „reader xyz, Software version 99.4711“ or „checking RAM“ and so on should be avoided. While in battery operation, the user has inserted a card and is waiting for display of his fund, to continue with a vend and is not interested in service related messages.

Petitioner Exhibit 1002-2089
CSC ServiceWorks – Ex. 1008
Page 265 of 270

A2.5 Session Example



Petitioner Exhibit 1002-2990
CSC ServiceWorks – Ex. 1008
Page 266 of 270



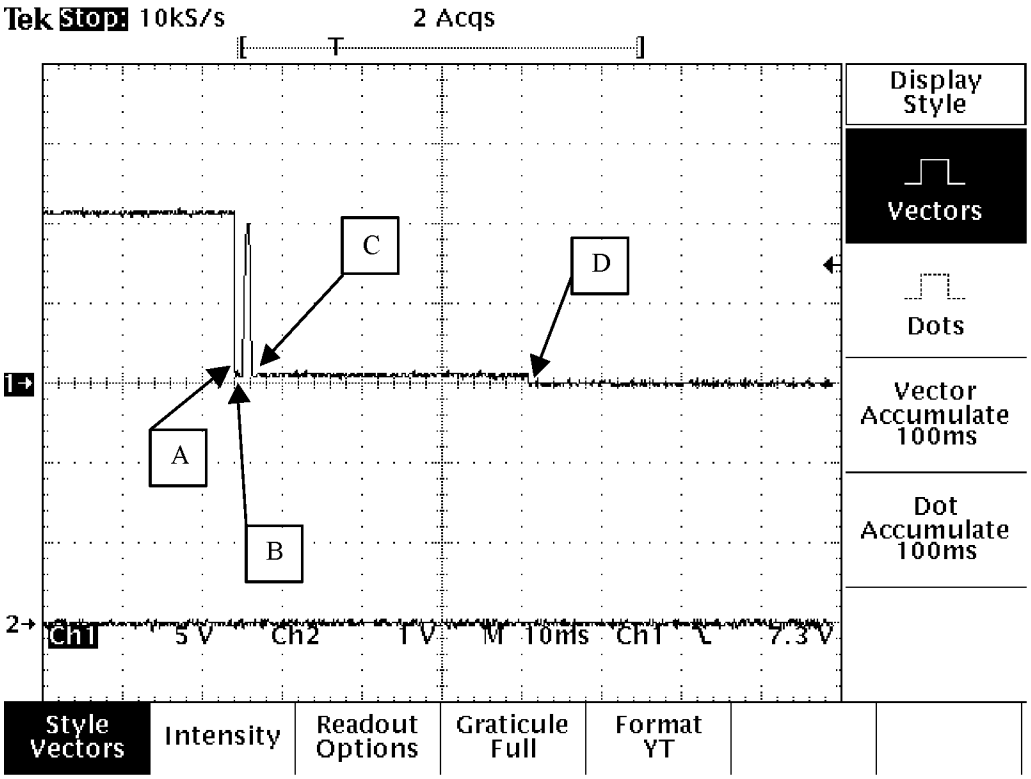
Petitioner Exhibit 1002-2091
CSC ServiceWorks – Ex. 1008
Page 267 of 270

A2.6 Hardware Considerations

Hardware Considerations

Within this special battery operation, the pin 3 of MDB/ICP connector is used as a wake-up signal. Refer to special BDTA-hardware specification.

To show an example of the timing for this pin, refer to the following diagram, which gives an example of all special timing problems related to more than one wake-up condition.



Position A: mechanical switch on VMC is pulling pin 3 low (i.e. door switch)
Position B: mechanical switch is released
Position C: card reader has finished reset routines and pulls pin 3 low
Position D: VMC has finished reset routines and pulls pin 3 low too.

If a card is inserted first, pin 3 may be pulled low first at position B.
If VMC is waked up via other means, maybe card reader is waked up at position D first.

In any case, this is a good example to clarify different waveform conditions on pin 3. Please note that any device may release pin 3 after a short duration (<1ms) cause pin 3 should work as dynamically wake-up. Holding pin 3 permanently low may prevent other

Petitioner Exhibit 1002-2992
CSC ServiceWorks – Ex. 1008
Page 268 of 270

devices from wake-up, i.e. after all devices ran into timeout and one is still holding pin 3, the other can no longer enter ready state (Note i.e. to door-switches etc.)

Petitioner Exhibit 1002-2993
CSC ServiceWorks – Ex. 1008
Page 269 of 270

(this page intentionally left blank)

Petitioner Exhibit 1002-2094
CSC ServiceWorks – Ex. 1008
Page 270 of 270

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/197,071	**12/06/2023 07:59:45 PM Z ET**	**104402-5075-US**

Title of Invention

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	9843	FILED BY	Jackeline De Ranieri
PATENT CENTER #	63518540	FILING DATE	05/14/2023
CUSTOMER #	24341	FIRST NAMED INVENTOR	Paresh K. Patel
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Douglas Crisman

Documents

TOTAL DOCUMENTS: 47

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
104402-5075-US Information Disclosure Statement 06DEC2023.pdf	4	Transmittal Letter	188 KB
104402-5075-US List of References Form 1449 06DEC2023.pdf	17	Information Disclosure Statement (IDS) Form (SB08)	289 KB
Warning: This is not a USPTO supplied IDS fillable form. Data in the form cannot be automatically loaded to other USPTO systems.			
WO2006020692A2.pdf	129	Foreign Reference	6153 KB
JP2010528716A.pdf	356	Foreign Reference	2504 KB

KR20130138637A.pdf	60	Foreign Reference	7091 KB
WO2016158748A1.pdf	92	Foreign Reference	11621 KB
CN106803175A.pdf	177	Foreign Reference	17248 KB
CN108352094A.pdf	40	Foreign Reference	2372 KB
JP2004310740A.pdf	32	Foreign Reference	6531 KB
JPH1125320A.pdf	89	Foreign Reference	19828 KB
JP4586607B2.pdf	39	Foreign Reference	8507 KB
CN1561508A.pdf	100	Foreign Reference	3669 KB
EP3901880A1.pdf	129	Foreign Reference	3952 KB
WO2017010936A1.pdf	50	Foreign Reference	3093 KB
Notice of Allowance US16681673 17AUG2022.pdf	22	Non Patent Literature	1698 KB
Notice of Allowance US17529111 22SEP2022.pdf	10	Non Patent Literature	1048 KB
Notice of Allowance US17654732 16SEP2022.pdf	9	Non Patent Literature	1009 KB
Non-Final Office Action US15893514 30SEP2022.pdf	8	Non Patent Literature	481 KB
Notice of Allownce US17147305 06OCT2022.pdf	9	Non Patent Literature	982 KB
Non-Final Office Action US17443802 23DEC2022.pdf	14	Non Patent Literature	1136 KB
Non-Final Office Action	11	Non Patent Literature	861 KB

US15956741 27FEB2023.pdf			
Notice of Allowance US15893514 10APR2023.pdf	13	Non Patent Literature	1193 KB
Heimerl et al. Community sourcing Engaging Local Crowds.pdf	10	Non Patent Literature	1390 KB
Notice of Allowance US17983311 28JUN2023.pdf	10	Non Patent Literature	1044 KB
EIC 3600 Search Report STIC Scientific and Technical Information Center.pdf	5	Non Patent Literature	547 KB
Notice of Allowance US15893514 12JUL2023.pdf	13	Non Patent Literature	1214 KB
Notice of Allowance US17973506 26JUL2023.pdf	13	Non Patent Literature	911 KB
Katy Jacob Are mobile payments the smart cards of the aughts.pdf	9	Non Patent Literature	568 KB
Notice of Allowance US17963170 04AUG2023.pdf	16	Non Patent Literature	1352 KB
USA Technologies Announces Cashless Solution to Be Offered by Blackboard Inc..pdf	6	Non Patent Literature	213 KB
Hossain_COMPREHENSIVE_STUDY_OF_BLUETOOTH_SIGNAL_PARAMETERS_FOR_LOCALIZATION.pdf	5	Non Patent Literature	950 KB
Hands-Free Profile	93	Non Patent Literature	6055 KB

Specification 1.5.pdf			
DEX and MDB - A Primer For Vendors.pdf	5	Non Patent Literature	3208 KB
MDB - Protocol V4.2.pdf	313	Non Patent Literature	2182 KB
Gruber The Commodity Vending Machine.pdf	11	Non Patent Literature	1931 KB
Kasavana Innovative VDI Standards.pdf	10	Non Patent Literature	1476 KB
SDFL Administrative Order 2021-33.pdf	5	Non Patent Literature	736 KB
Pogue In Arrival of 2 iPhones 3 Lessons.pdf	4	Non Patent Literature	2450 KB
Thompson How to use S Beam.pdf	5	Non Patent Literature	865 KB
iPhone User Guide for iOS 6.1.pdf	156	Non Patent Literature	4867 KB
Apple Reports Fourth Quarter Results.pdf	4	Non Patent Literature	1130 KB
Apple Announces iPhone 5s.pdf	5	Non Patent Literature	1598 KB
Reardon Motion sensing comes to mobile phones.pdf	4	Non Patent Literature	2574 KB
MDB- ICP Specification Version 3.0.pdf	270	Non Patent Literature	1501 KB
Weidong Kou Payment Technologies for E-Commerce.pdf	339	Non Patent Literature	22368 KB

Specification for RFID Air Interface V1.2.0.pdf	108	Non Patent Literature	1997 KB
Baier et al. Principles of Model Checking.pdf	994	Non Patent Literature	16062 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
104402-5075-US Information Disclosure Statement 06DEC2023.pdf	581C4DDC1D09BD45959E36EEB264DCDD533F7FFE9BA1D8E2B08C706EBDBFCD9D2EA7D83952B331603F71A013282998774135AD761482983C405C6E27C7BE5FF8
104402-5075-US List of References Form 1449 06DEC2023.pdf	1CC45ECACF44D4296BD243565F784AA802355023F00373B77FEA375D253FA14005F92262A6CF978E89EA5488A85581BC5D8DED6D5CEF6385B6790A2D8C9F9D1F
WO2006020692A2.pdf	F29F1F4ADA4DD505C27EB9A01851B76124A51875FACB35D070AE0CBDF3CC2014497F61E9499854834549 2E02BC006BF809D01A6A2E5E7BE5E9F68607400ECDF8
JP2010528716A.pdf	E4A239EF0CF1DAE6FD297DEFCB03D1682B26C7F003C719F4D74B674D596B554A3093E8518BF07E41C34FE991F8E9F16C09E1489B028884BF527EA43DAEBD2C88
KR20130138637A.pdf	2FE811D2ED1792947A341B154CE59C18D26E792C0683F39564F6E84D782833C34EB4E44552B1757FC59496CE7F7372EB7ED8C77AA003406FB18A84FB99033FA0
WO2016158748A1.pdf	73E84E0AF08F846A29DB69E8F8B3EBC8C69BFD2AB97DCB460DC4C156D8942EB28B02878DDBFF04FE9E60CB3FF0DE8A65B01DEC0CE5BCF5463E1BA7B755CEBE86
CN106803175A.pdf	518D61773C663BFB193DF4E7366FB8B2DB2F4A57F7873F536DA2632F82F491E428534946D9A725E854AF854C7272B937932C4BE3CCFF84F166A16A8B211CA15D

CN108352094A.pdf	59A8B728A6EFB7C6738DCAFB1D00077F362AD91A78228613C04D8B062FEEDA5ED9A2396907752098B1D642B19F11B9F9A138656C34477934292329BE4911F105
JP2004310740A.pdf	B321F974477D8E027C84F9FB2FB672004161526C864EDEA61CA59A55CF401E19BB5BBEAFF4D60DDA4480CD62EF28FE6A0B7E4F0772D35C8410E6B9F7525B682A
JPH1125320A.pdf	1128AF780E184DB399D506C87C3BEF6F336B4985DC15B730EA317C07FC38A04EE9EC5B86BD67AD3BA57FA10D466A6AF517AC3F1CF2E712F7E1DDE85D784EBA03
JP4586607B2.pdf	7C00C2436B987D864F09290884399F52D162199B593C72E67D2680498EC0D514022CA41EE64256B14D4250DDD1836DDE1CD91FEDE222525188E7F3E68266E7AE
CN1561508A.pdf	ECE5691C94A4EFD9D436D2DA2471B931936EDDEF8523651A3E2D944C936231E734EA2A774D034AD591D7A4CFD0BC60E2E13F23157A716BEEBF5EB0F307A99640
EP3901880A1.pdf	32DE6AD53678CB9FC86C5A0760921F04E9B3C1DF633D066B498DD8259B4DE02EFBA0E7240D9A0F8E44E164DC0B9468CE2DBDE893E66AF6A7FBCCAF6B769F0DF9
WO2017010936A1.pdf	F2E6C6794320F93E4CAED0608D6B8FBA913114772C2A69596A31B109565CAAF2982B6EF58E90E7E978144BC2B00ACE9456E75D0823C41B842B0CEFE7FD1E547D
Notice of Allowance US16681673 17AUG2022.pdf	45E8E3C446F2B7E821807073816053CD932B009EB383797774ECB44963AD1B54AA87836F9C5508C0C9F91546B03DB3B9E5D4AA25DBB1610FCD0AF86F438D7FA6
Notice of Allowance US17529111 22SEP2022.pdf	C4CCCE6396D89D8348CDAFAC8A91B5F49E9963B70DD3650DB014075E70445D0A968A754456DCB6972E73C2A9558465195F9109BA4B56536CBA51EABDDBC78CAF
Notice of Allowance US17654732 16SEP2022.pdf	28AF9F267CE26AB8C5E39A7652BA900476A1F0747A249588A92022697DA1BB134452B41D4B884B28BE8DB90C58343061687A4BF36960EFB5E58DC534AC2E992B

Non-Final Office Action US15893514 30SEP2022.pdf	427FCEFF197564828F17919E28E9E5518523992AE51D6238C3FD2367D2E584D684B8EE8468F32EFC6A4BA91A840492A4A456F58C0CBAAA70163CDB48C7B80ABE
Notice of Allownce US17147305 06OCT2022.pdf	BC42735D1713BA2205D9960AF87F47125BE36E49A52DD405C4972864DA328F655C2F577D12567C4C36C5ECD1C928A431861CDC281536A93546E204B92406C3BE
Non-Final Office Action US17443802 23DEC2022.pdf	4EFF76DF3FB79047C834D9FC6754994CE3BFA90D5CA6DBD729F770D2E2616805F7EA99A6D781FD66C1773554516A458ADA05DF3E61ADD445BDA6AE4BE27DADC7
Non-Final Office Action US15956741 27FEB2023.pdf	010D71B137FD34EC214325D9A1534B0ABBD9785F29CD26D41FE9155B504F717D93771663C320B0EC70E9450323FEE3FD0D5BC9D18E288AACA2F61F3001202BF2
Notice of Allowance US15893514 10APR2023.pdf	4B17D9C72F6C90C892A01572FBA6295B291FF82B597AB17F81479B1277699CEC23B4D8CBC9464A2F27C0F32BB3EDA7C2E4AAC993945F4D3B94B1C86F82F6C2BC
Heimerl et al. Communiy sourcing Engaging Local Crowds.pdf	FA3ABA76B282540FD587B83A0775FA3CDCE58B7D1488099BA3A0422A5F02BAC4078512283189278795FB08354B9DDCBCA4DAC1009ABA8652AE7640ACA9B9A7D6
Notice of Allowance US17983311 28JUN2023.pdf	B0089705740705BD5657CE769B0E77AE48F835154B6FDC23E04DECDF6CF70BCAB78FC850A34E86BE28AE1050B8CECD5D5A886FCE461458B95E0EAEF7B9DC4D23
EIC 3600 Search Report STIC Scientific and Technical Information Center.pdf	D9233E238654EE59866A6BB913419F981BA9129FE609676618FCFB8880BDE13EEE34DE19A3BC8E897F72F699E6F1EC9D0403039078EE7442A4FF33ABE6E7036E
Notice of Allowance US15893514 12JUL2023.pdf	EFD6E94D5949608CB6E5345387D258239874111179C80BA008973FFD435737BB8750343F266955615E1D292E1550EF953050F373FEDD1BE839697EDC9AF652E85
Notice of Allowance US17973506 26JUL2023.pdf	021FF1F29900F164587F74E0E5F0F29FE86D62358CD63C7B5EF1E10554428841A072AC29CBB8BE1D5A9B0A79EB8B162804F4B94679CFFBB2EA1C641C7312CC03

Katy Jacob Are mobile payments the smart cards of the aughts.pdf	BFEE3E3F4597168DA4179A8D823FA95F5C787727C04F2DA8A3881CBE0CBC21E6F49DFFF9441D55989D5A615E949408460A2B6E8CEF38CC2C3B7B44B1C0D57A5F
Notice of Allowance US17963170 04AUG2023.pdf	C8CBF6BCCB6CF53673BBB3DD390CF994AB8AAD19742F895ABF0F676EE304E4E71ECC60AEF6BB82F03C74E6F2546344B956DD06F481F05AE77E3842CF943ABA43
USA Technologies Announces Cashless Solution to Be Offered by Blackboard Inc..pdf	864ED9E0BF5041AFA6FE036FDE6F902D7BC5F3B50CD4A9C22B44672FC278EAFAD09C0A7D670300AD423F099ACB7AAF62B5B85B8F84927FFED6FA2C3382AC058B
Hossain_COMPREHENSIVE_STUDY_OF_BLUETOOTH_SIGNAL_PARAMETERS_FOR_LOCALIZATION.pdf	9A4A80BFC960220CF5577DE74611B800868A8AA0D41ADDC6F160C81BB3B0C7877522D5C02D2D64FC55610B107D4767AC9BF187C720B0352ABF6036933F2B96B8
Hands-Free Profile Specification 1.5.pdf	66FDF661543D2BF1278161789571AE5FEBA2AB479348BB2E1747673199 4D9B72E9ED8BD13F950C614B98E7C84179F2BE622C78BB2311F378CA803937204C7B4A
DEX and MDB - A Primer For Vendors.pdf	01C8AEF11E44308D0F6A258DB498429D918E1845B155D5A80CD6AE1E55D20BCCCD99F571FA07F6B5A22BB2F3AE300B09FE6F8B05B8DD87A29D35D6472E29D500
MDB - Protocol V4.2.pdf	A951C108FD41795AC8A8437F8306113D5F76DEF8A07D86F07A89A72A01E7BFAA3719878DD57141F9C844D56A0D0D001F096CCFEC5657667D976B3C7110718192
Gruber The Commodity Vending Machine.pdf	F4227F6F7C86D28A8F19C3A6DFBD76693277F197B53095E3AE2A7C2F1AFDF6EF0EE84326692264E0DDAE290988C3FD65AFC6414101866D6D6148D34FC0BD711B
Kasavana Innovative VDI Standards.pdf	F9E9704173098E10C6246A86277944D45A0F41C65E10FEF53BB4A31B0D060416D08BDD0317F17BC65C95E9DFE954CFFB82A6B64C76ECA4D2E880B64C123622BC
SDFL Administrative Order 2021-33.pdf	E2E12A2BE8EC67E87381AE6C303FADE76A1059A4F0E4D08393902B41865BB29C359ECD76E6D680FF649A55591113A8FA756DE056B3D2AFC4C838E8C398A3C4F4

Pogue In Arrival of 2 iPhones 3 Lessons.pdf	2B45F2E65A91AB0A9BE6AADF519486FA137E150018666A2BB865A637B88B7C6E63AE45BECC7FB3D8C1017F40F5109103B162FB4023ACE842DB96F93018AEBCE9
Thompson How to use S Beam.pdf	A075C837BFD9B96AF3F5F45B98FFCEBEA736040D32B0DA8CD7C20A369A302C80DA1E93CE10C0529292648563A4E6FF0A078A7C87F571330DDFDD2C202ED3EA2F
iPhone User Guide for iOS 6.1.pdf	D8C476A8D1262D2D8C94FC57EF6481591FDD0C9020F24AC4A11A32ADD34B5D8829851E5FE90DC7F9946B84960C079250BB9FA9564E31839FC0DDF97CDB62C5BA
Apple Reports Fourth Quarter Results.pdf	C4E6DE5ADB73E41ABD1A287E4E68F51255CEC8F4E12C2EAF93E720D1CF2F225AB93FB85A13A380FF1B05843197 8E6B5C8B35C4B6B9F01D59A000222D03CA3D87
Apple Announces iPhone 5s.pdf	1C3464D7D7C91FFD572FBCA517468363BC73E86649C5BD9E6F40F83153913D67CA9736BBCD289073FA00952D0993FDA7F5B27397C6ACC82B6C3D371328CED6B0
Reardon Motion sensing comes to mobile phones.pdf	A4BD2BD4C0382979B8989C2CDE799E9F6972FDFD8ECF921D8E8508D301416B0058A7937135D7A3F60CFDC0D2FB18710087F0C50622B0EADD66CD5E01524BA9DD
MDB- ICP Specification Version 3.0.pdf	D77E2EC8D571847FE9AA3D7F097F3BA79142F52FB86AB42799601A199DD8F3F48C8551815785022CD388462948 3E67B5C2E8D5C09039DEFAD89DA2A176145019
Weidong Kou Payment Technologies for E-Commerce.pdf	08291B2907C6383F20E72DF37B252E7B2A07B8E3502F809F924D7D419D2F09D36E5D98300DBCC208E1ED14811A9C36EAD2DB937E92935A021AE72E78DA6347C5
Specification for RFID Air Interface V1.2.0.pdf	488C2D4EB134EA04C7B81945443E56BF779F4A99D5B66D0292174FAABC0FDEAEF4063B5489CCFE95CED9F8F8A4257DDFB78B6EA0877856C6E4005AF5068D03C7
Baier et al. Principles of Model Checking.pdf	2891F123F400666F02165C1E0B2332C8085F5A17D4B41846DBB47701B860F55A17DB7335D99143A6932ADFCABEAD0B40EB37D0D8DF8877156B6A4459DD662BA1

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

MEDIA ALERT
October 28, 2013

Apple Reports Fourth Quarter Results

iPhone Sales Grow 26% to Establish New September Quarter Record

CUPERTINO, California—October 28, 2013—Apple® today announced financial results for its fiscal 2013 fourth quarter ended September 28, 2013. The Company posted quarterly revenue of $37.5 billion and quarterly net profit of $7.5 billion, or $8.26 per diluted share. These results compare to revenue of $36 billion and net profit of $8.2 billion, or $8.67 per diluted share, in the year-ago quarter. Gross margin was 37 percent compared to 40 percent in the year-ago quarter. International sales accounted for 60 percent of the quarter's revenue.

The Company sold 33.8 million iPhones, a record for the September quarter, compared to 26.9 million in the year-ago quarter. Apple also sold 14.1 million iPads during the quarter, compared to 14 million in the year-ago quarter. The Company sold 4.6 million Macs, compared to 4.9 million in the year-ago quarter.

Apple's Board of Directors has declared a cash dividend of $3.05 per share of the Company's common stock. The dividend is payable on November 14, 2013, to shareholders of record as of the close of business on November 11, 2013.

"We're pleased to report a strong finish to an amazing year with record fourth quarter revenue, including sales of almost 34 million iPhones," said Tim Cook, Apple's CEO. "We're excited to go into the holidays with our new iPhone 5c and iPhone 5s, iOS 7, the new iPad mini with Retina Display and the incredibly thin and light iPad Air, new MacBook Pros, the radical new Mac Pro, OS X Mavericks and the next generation iWork and iLife apps for OS X and iOS."

"We generated $9.9 billion in cash flow from operations and returned an additional $7.8 billion in cash to shareholders through dividends and share repurchases during the September quarter, bringing cumulative payments under our capital return program to $36 billion," said Peter Oppenheimer, Apple's CFO.

Apple is providing the following guidance for its fiscal 2014 first quarter:

- revenue between $55 billion and $58 billion
- gross margin between 36.5 percent and 37.5 percent
- operating expenses between $4.4 billion and $4.5 billion
- other income/(expense) of $200 million
- tax rate of 26.25 percent

Apple will provide live streaming of its Q4 2013 financial results conference call beginning at 2:00 p.m. PDT on October 28, 2013 at www.apple.com/quicktime/qtv/earningsq413. This webcast will also be available for replay for approximately two weeks thereafter.

This press release contains forward-looking statements including without limitation those about the Company's estimated revenue, gross margin, operating expenses, other income/(expense), and tax rate. These statements involve risks and uncertainties, and actual results may differ. Risks and uncertainties include without limitation the effect of competitive and economic factors, and the Company's reaction to those factors, on consumer and business buying decisions with respect to the Company's products; continued competitive pressures in the marketplace; the ability of the Company to deliver to the marketplace and stimulate customer demand for new programs, products, and technological innovations on a timely basis; the effect that product introductions and transitions, changes in product pricing or mix, and/or increases in component costs could have on the Company's gross margin; the inventory risk associated with the Company's need to order or commit to order product components in advance of customer orders; the continued availability on acceptable terms, or at all, of certain components and services essential to the Company's business currently obtained by the Company from sole or limited sources; the effect that the Company's dependency on manufacturing and logistics services provided by third parties may have on the quality, quantity or cost of products manufactured or services rendered; risks associated with the Company's international operations; the Company's reliance on third-party intellectual property and digital content; the potential impact of a finding that the Company has infringed on the intellectual property rights of others; the Company's dependency on the performance of distributors, carriers and other resellers of the Company's products; the effect that product and service quality problems could have on the Company's sales and operating profits; the continued service and availability of key executives and employees; war, terrorism, public health issues, natural

disasters, and other circumstances that could disrupt supply, delivery, or demand of products; and unfavorable results of other legal proceedings. More information on potential factors that could affect the Company's financial results is included from time to time in the "Risk Factors" and "Management's Discussion and Analysis of Financial Condition and Results of Operations" sections of the Company's public reports filed with the SEC, including the Company's Form 10-K for the fiscal year ended September 29, 2012, its Form 10-Q for the quarter ended December 29, 2012, its Form 10-Q for the quarter ended March 30, 2013, its Form 10-Q for the quarter ended June 29, 2013, and its Form 10-K for the year ended September 28, 2013 to be filed with the SEC. The Company assumes no obligation to update any forward-looking statements or information, which speak as of their respective dates.

Apple designs Macs, the best personal computers in the world, along with OS X, iLife, iWork and professional software. Apple leads the digital music revolution with its iPods and iTunes online store. Apple has reinvented the mobile phone with its revolutionary iPhone and App Store, and is defining the future of mobile media and computing devices with iPad.

Press Contact:
Steve Dowling
Apple
dowling@apple.com
(408) 974-1896

Investor Relations Contacts:
Nancy Paxton
Apple
paxton1@apple.com
(408) 974-5420

Joan Hoover
Apple
hoover1@apple.com
(408) 974-4570

Data Summary
View PDF

Apple, the Apple logo, Mac, Mac OS and Macintosh are trademarks of Apple. Other company and product names may be trademarks of their respective owners.

Newsroom

The latest news and updates, direct from Apple.

Read more >

Copyright © 2021 Apple Inc. All rights reserved.

Electronically filed December 6, 2023

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Paresh K. Patel	Confirmation No.:	9843
Serial No.:	18/197,071	Art Unit:	3698
Filed:	May 14, 2023	Examiner:	Frantzy POINVIL
For:	METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS	Attorney Docket No.:	104402-5075-US

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure provisions of 37 C.F.R. §1.56, there is hereby provided certain information which the Examiner may consider material to the examination of the subject U.S. patent application. It is requested that the Examiner make this information of record if it is deemed material to the examination of the application.

1. Enclosures accompanying this Information Disclosure Statement are:

1a. ☒ A list of all patents, publications, applications, or other information submitted for consideration by the office.

1b. A legible copy of:

☒ Each foreign patent;

☒ Each publication or that portion which caused it to be listed on the PTO-1449;

☐ For each cited pending U.S. application, the application specification including the claims, and any drawing of the application, or portion of the application which caused it to be listed on the PTO-1449 including any claims directed to that portion;

☒ all other information or portion which caused it to be listed on the PTO-1449.

1c. ☒ An English language copy of search report(s) from a counterpart foreign application or PCT International Search Report.

1d. ☐ Explanations of relevancy (ATTACHMENT 1(d), hereto) or English language abstracts of the non-English language publications.

Petitioner Exhibit 1002-3009

2. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(b):

☐ Within three months of the filing date of a national application other than a continued prosecution application under §1.53(d);

☐ Within three months of the date of entry of the national stage as set forth in §1.491 in an international application;

☐ Before the mailing of the first Office action on the merits;

☐ Before the mailing of a first Office action after the filing of a request for continued examination under §1.114.

3. ☒ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(c) after the period specified in 37 C.F.R. §1.97(b), but before the mailing date of any of a final action under 37 C.F.R. §1.113, a notice of allowance under 37 C.F.R. §1.311 or an action that otherwise closes prosecution in the application.

(Check either Item 3a, 3b, 3c or 3d)

3a. ☐ The Certification Statement in Item 5 below is applicable. Accordingly, no fee is required.

3b. ☐ The $260 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

3c. ☒ The $104 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 104402-5075-US).

3d. ☐ The $52 (micro entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

(Items 3b or 3c to be checked if any reference known for more than 3 months)

4. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(d) after the period specified in 37 C.F.R. §1.97(c), but on or before the date of payment of the issue fee.

(Check Item 4a, and 4b, 4c or 4d)

4a. ☐ The Certification Statement in Item 5 below is applicable.

4b. ☐ The $260 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

4c. ☐ The $104 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

4d. ☐ The $52 (micro entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

Petitioner Exhibit 1002-3010

5. ☐ Certification Statement (applicable if Item 3a or Item 4a is checked)

(Check either Item 5a, 5b, 5c or 5d)

5a. ☐ In accordance with 37 C.F.R. §1.97(e)(1), it is certified that each item of information contained in this information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Information Disclosure Statement.

5b. ☐ In accordance with 37 C.F.R. §1.97(e)(2), it is certified that no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 C.F.R. §1.56(c) more than three months prior to the filing of this information disclosure statement.

5c. ☐ Each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

5d. ☐ Pursuant to 37 C.F.R. §1.704(d), each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

6. ☒ Copies of each cited U.S. patent and each U.S. patent application publication are not enclosed pursuant to the USPTO OG Notice dated 05 August 2003 waiving the requirement under 37 C.F.R. 1.98(a)(2)(i) for U.S. patent applications filed after June 30, 2003.

7. ☒ This application is a continuation application under 37 C.F.R. §1.53(b) or (d).

(Check appropriate Items 7a, 7b and/or 7c)

7a. ☐ A Petition to Withdraw from issue under 37 C.F.R. §1.313(b)(5) is concurrently filed herewith.

7b. ☒ Copies of publications listed on Form PTO-1449 from prior application Serial No. 17/973,507, filed on October 25, 2022, from prior application Serial No. 17/654,732, filed on March 14, 2022, from prior application Serial No. 17/147,305, filed on January 12, 2021, from prior application Serial No. 15/603,400, filed on May 23, 2017, from prior application Serial No. 14/458,199, filed on August 12, 2014, from prior application Serial No. 14/456,683, filed on August 11, 2014, from prior application Serial No. 14/335,762, filed on July 18, 2014, from prior application Serial No. 14/214,644, filed on March 14, 2014, of which this application claims priority under 35 U.S.C. §120, are not being submitted pursuant to 37 C.F.R. §1.98(d).

7c. ☒ Copies of the publications listed on the attached Form PTO-1449 that were not previously cited in prior application Serial No. 17/973,507, filed on October 25, 2022, from prior application Serial No. 17/654,732, filed on March 14, 2022, from prior application Serial No. 17/147,305, filed on January 12, 2021, from prior application Serial No. 15/603,400, filed on May 23, 2017, from prior application Serial No. 14/458,199, filed on August 12, 2014, from prior application Serial No. 14/456,683, filed on August 11, 2014, from prior application Serial No. 14/335,762, filed on July 18, 2014, from prior application Serial No. 14/214,644, filed on March 14, 2014, are provided herewith.

8. ☐ This is a Supplemental Information Disclosure Statement. (Check Item 8a)

8a. ☐ This Supplemental Information Disclosure Statement under 37 C.F.R. §1.97(f) supplements the Information Disclosure Statement filed on . A bona fide attempt was made to comply with 37 C.F.R. §1.98, but inadvertent omissions were made. These omissions have been corrected herein. Accordingly, additional time is requested so that this Supplemental Information Disclosure Statement can be considered as if properly filed on .

9. ☐ In accordance with 37 C.F.R. §1.98, a concise explanation of what is presently understood to be the relevance of each non-English language publication is:

(Check Item 9a, 9b, or 9c)

9a. ☐ satisfied because all non-English language publications were cited on the enclosed English language copy of the PCT International Search Report or the search report from a counterpart foreign application indicating the degree of relevance found by the foreign office.

9b. ☐ set forth in the application.

9c. ☐ enclosed as an attachment hereto.

10. ☒ The Commissioner is authorized to charge any additional fee required or credit any overpayment for this Information Disclosure Statement and/or Petition to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 104402-5075-US).

11. ☒ No admission is made that the information cited in this Statement is, or is considered to be, material to patentability nor a representation that a search has been made (other than a search report of a foreign counterpart application or PCT International Search Report if submitted herewith). 37 C.F.R. §§1.97(g) and (h).

Respectfully submitted,

Date: December 6, 2023

/Douglas J. Crisman/ 39,951
Douglas J. Crisman (Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP
1400 Page Mill Road
Palo Alto, CA 94304
(650) 843-4000

Petitioner Exhibit 1002-3012

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

24341 7590 07/26/2023
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER
HAMILTON, MATTHEW L

ART UNIT	PAPER NUMBER
3682	

DATE MAILED: 07/26/2023

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/973,506	10/25/2022	Paresh K. Patel	104402-5072-US	5383

TITLE OF INVENTION: Method and System for Asynchronous Mobile Payments for Multiple In-Person Transactions Conducted in Parallel

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	10/26/2023

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 40% the amount of undiscounted fees, and micro entity fees are 20% the amount of undiscounted fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

Petitioner Exhibit 1002-3013

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

24341 7590 07/26/2023
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/973,506	10/25/2022	Paresh K. Patel	104402-5072-US	5383

TITLE OF INVENTION: Method and System for Asynchronous Mobile Payments for Multiple In-Person Transactions Conducted in Parallel

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	10/26/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS
HAMILTON, MATTHEW L	3682	705-071000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑ Issue Fee ❑ Publication Fee (if required)

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via Patent Center or EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

❑ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

❑ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

Petitioner Exhibit 1002-3014

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/973,506	10/25/2022	Paresh K. Patel	104402-5072-US	5383

24341 7590 07/26/2023

Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER	
HAMILTON, MATTHEW L	
ART UNIT	**PAPER NUMBER**
3682	

DATE MAILED: 07/26/2023

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Petitioner Exhibit 1002-3015

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Petitioner Exhibit 1002-3016

Notice of Allowability	Application No. 17/973,506	Applicant(s) Patel et al.	
	Examiner MATTHEW L HAMILTON	Art Unit 3682	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to October 25, 2022.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are 1-20 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some* c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☑ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☑ Interview Summary (PTO-413), Paper No./Mail Date. 20230707.
5. ☐ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/MATTHEW L HAMILTON/
Primary Examiner, Art Unit 3682

Petitioner Exhibit 1002-3017

DETAILED ACTION

This action is in response to the initial filing filed on October 25, 2022. Claim 1 was originally filed. A preliminary amendment was filed on July 12, 2023. Claim 1 was amended. Claims 2-20 were added. Claims 1-20 have been examined and is currently pending.

Notice of Pre-AIA or AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Inventorship

This application currently names joint inventors. In considering patentability of the claims the examiner presumes that the subject matter of the various claims was commonly owned as of the effective filing date of the claimed invention(s) absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and effective filing dates of each claim that was not commonly owned as of the effective filing date of the later invention in order for the examiner to consider the applicability of 35 U.S.C. 102(b)(2)(C) for any potential 35 U.S.C. 102(a)(2) prior art against the later invention.

Allowable Subject Matter

Claim 1-20 is allowed.

The applicant's invention discloses a mobile consumer device with a display, processor(s), and memory: identifies a merchant device in proximity to the consumer device based on broadcasted information transmitted by the first merchant device, the broadcasted information including a first identifier corresponding to the first merchant device; transmits the first identifier to a server and receives from the server an electronic communication including identification and transaction information associated with the merchant; displays the identification information, receives user selection of the merchant identification information; and in response, displays the merchant transaction information, receives supplemental user information, and transmits the supplemental transaction information to the server for completion of the transaction.

Claim 1 is allowed because no prior art in combination, fails to teach or suggest or otherwise make obvious, all the limitations comprising:

and first merchant transaction information identifying a proposed in-person transaction between the consumer device and the first merchant, wherein the first merchant transaction information includes a merchant-specified transaction amount;

displaying the first merchant transaction information;

receiving from the user of the consumer device first supplemental transaction information, wherein the first supplemental transaction information is a selection of the merchant-specified transaction amount;

Independent claim 8 and 14 are allowed based on a similar rationale. Dependent claims 2-7, 9-13, and 15-20 are allowable based on the same rationale as the claims from which they depend.

The Examiner notes the applicant's invention is directed to patentable eligible subject matter under 35 U.S.C. 101. The applicant's invention provides an improvement over past systems, the applicant's specification discloses, "Traditional electronic payment systems for in-person transactions are one-to-one such that there is one merchant and one consumer conducting one transaction at a time. The process requires a captive, exclusive interaction between the merchant and consumer, and typically neither party may disengage from the process until the payment has completed or has been cancelled." (paragraph 0008), "Additionally, other consumers who want to make a payment to the same merchant must wait until the current transaction has completed processing. Consumers interact with the merchant sequentially and wait their turn." (paragraph 0009), "This system is acceptable in traditional retail situations where one consumer is purchasing a good or service and needs the merchant to perform "check out" tasks. In such electronic payment systems, the payment transaction is first initiated by the merchant (e.g., requesting a consumer pay a certain amount). These electronic payment systems do not work well when there are multiple consumers needing to pay a single merchant at approximately the same time, or when the merchant is not able to initiate the payment process." (paragraph 0010), "Implementations described herein provide methods and systems for enabling electronic payments via a mobile device such that multiple consumers can initiate overlapping in-person payments to a single merchant at the same time, or substantially the same time. Moreover, in some implementations, the consumer has the option to send payment to a merchant without the merchant having to request payment first." (paragraph 0012), "There are numerous use cases for such a system, some of which are currently only handled by cash payments (since existing electronic payment systems do not address the need to have multiple parties sending payments to a single merchant). One example use case involves payments to a street performer, who would traditionally put out a box, hat, or an open guitar case (collectively referred to as collection box) for audience payments. As he or she is performing, any number of audience members can drop cash into

the collection box to pay the performer." (paragraph 0013) and "Notably, the performer (or in different contexts, a merchant) is not required to initiate the payment with each consumer and does not need to stop doing what he or she is doing. A plurality of consumers can also pay the performer/merchant without needing to wait for each transaction to finish. The transaction is asynchronous as the performer/merchant need not acknowledge the transaction before the next payment and may not acknowledge the payment at all. Methods and systems described herein allow this and similar in-person payment scenarios to be handled via electronic payments managed via mobile electronic devices associated with a merchant/performer and one or more customers." (paragraph 0014).

Jacob, K. (2007). Are mobile payments the smart cards of the aughts? Chicago Fed Letter

The article discloses the potential future of mobile payments in consumers' lives.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Laracey et al. US Publication 20180005220 A1 Localized Identifier Broadcasts to Alert Users of Available Processes and Retrieve Online Server Data

Laracey discloses provided systems and methods for localized identifier broadcasts to alert users of available processes and retrieve online server data. A user may visit a merchant location and engage in a transaction to purchase items from a merchant at the merchant location. The merchant may wish to alert the user of various payment methods, include payments through a payment application of the user's device using a received identifier for retrieval of an online invoice with a service provider. The merchant may utilize a merchant device to broadcast a location awareness identifier to alert the user of availability of payment processes with the service provider. Additionally, once the online invoice is

generated for a transaction, the merchant device may broad cast a payment terminal request identifier that allows the user to retrieve the online invoice using data associated with the identifier and a location for the merchant.

Grassadonia US Patent 10410194 B1 Customized Tipping Flow

Grassadonia discloses a technology for customizing the flow of a payment transaction at a payer's mobile device, based on parameters associated with a merchant payee to which the payer is making the payment. The payee can be a business entity that conducts transactions involving tips (e.g., restaurant, professional service, etc.). The transaction flow technology involves communication between a mobile application installed on the mobile device and a remote payment service system (PSS). A list of potential payees can be displayed for selection by the payer at the mobile application. The payees can be nearby payees identified by using, e.g., BLE, Bluetooth®, Wi-Fi®, geofence, etc. Upon selection of a particular payee by the payer, the PSS identifies one or more parameters of that payee, e.g., payee type, and generates a transaction flow that includes a tipping flow corresponding to the parameters of the merchant payee.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW L HAMILTON whose telephone number is (571)270-1837. The examiner can normally be reached Monday-Thursday 9:30-5:30 pm EST.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Waseem Ashraf can be reached on (571)270-3948. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MATTHEW L HAMILTON/
Primary Examiner, Art Unit 3682

Examiner-Initiated Interview Summary	**Application No.** 17/973,506	**Applicant(s)** Patel et al.		
	Examiner MATTHEW L HAMILTON	**Art Unit** 3682	**AIA (First Inventor to File) Status** Yes	**Page** 1 of 1

All Participants (applicant, applicants representative, PTO personnel)	**Title**	**Type**
MATTHEW L HAMILTON	Primary Examiner	Telephonic
Benjamin Pezzner	Attorney of Record	

Date of Interview: 12 July 2023

Issues Discussed:

Proposed Amendment(s)

The applicant's representative, Mr. Benjamin Pezzner filed an amended set of claims. The additional set of claims are directed to other aspects of the invention that were not claimed in the original set of claims.

Non-statutory Double Patenting

The examiner requested the applicant file a terminal disclaimer in light of the related patented application 16/681,673. The terminal disclaimer was filed.

/MATTHEW L HAMILTON/ Primary Examiner, Art Unit 3682	

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

Petitioner Exhibit 1002-3024

Notice of References Cited	Application/Control No. 17/973,506	Applicant(s)/Patent Under Reexamination Patel et al.	
	Examiner MATTHEW L HAMILTON	Art Unit 3682	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-10410194-B1	09-2019	Grassadonia; Brian	G06Q20/327	1/1
*	B	US-20180005220-A1	01-2018	Laracey; Kevin	G06Q20/3278	1/1
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Jacob, K., Are mobile payments the smart cards of the aughts?, July 2007, Chicago Fed Letter, Federal Reserve of Chicago (Year: 2007)
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Petitioner Exhibit 1002-3025

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

24341 7590 08/04/2023

Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER
HAMILTON, MATTHEW L

ART UNIT	PAPER NUMBER
3682	

DATE MAILED: 08/04/2023

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/963,170	10/10/2022	Paresh K. Patel	104402-5071-US	9471

TITLE OF INVENTION: METHOD AND SYSTEM FOR PROVIDING OFFERS FOR AUTOMATED RETAIL MACHINES VIA MOBILE DEVICES

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	11/06/2023

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 40% the amount of undiscounted fees, and micro entity fees are 20% the amount of undiscounted fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

Petitioner Exhibit 1002-3026

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

24341 7590 08/04/2023
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/963,170	10/10/2022	Paresh K. Patel	104402-5071-US	9471

TITLE OF INVENTION: METHOD AND SYSTEM FOR PROVIDING OFFERS FOR AUTOMATED RETAIL MACHINES VIA MOBILE DEVICES

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	11/06/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS
HAMILTON, MATTHEW L	3682	705-014370

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑ Issue Fee ❑ Publication Fee (if required)

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via Patent Center or EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

❑ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

❑ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

Petitioner Exhibit 1002-3027

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/963,170	10/10/2022	Paresh K. Patel	104402-5071-US	9471

24341 7590 08/04/2023

Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER	
HAMILTON, MATTHEW L	
ART UNIT	PAPER NUMBER
3682	

DATE MAILED: 08/04/2023

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Petitioner Exhibit 1002-3028

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Petitioner Exhibit 1002-3029

Notice of Allowability	Application No. 17/963,170	Applicant(s) Patel, Paresh K.	
	Examiner MATTHEW L HAMILTON	Art Unit 3682	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to July 12, 2023.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are 2-21 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some* c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☑ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☑ Interview Summary (PTO-413), Paper No./Mail Date. 20230711.
5. ☑ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/MATTHEW L HAMILTON/
Primary Examiner, Art Unit 3682

Petitioner Exhibit 1002-3030

DETAILED ACTION

This action is in response to the initial filing filed on October 10, 2022. Claim 1 was filed. A preliminary amendment was filed on July 12, 2023. Claim 1 was cancelled. Claims 2-21 were added. Claims 2-21 have been examined and are currently pending.

Notice of Pre-AIA or AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Allowable Subject Matter

Claims 2-21 are allowed subject to the examiner's amendment described below.

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Benjamin Pezzner, Reg. 70,711 on July 24, 2023.

EXAMINER'S AMENDMENT

The application has been amended as follows: Please amend claims 2-3, 7, 16, and 20-21 have been amended.

2. (Currently Amended) A method, comprising:

at a mobile device including a display, one or more processors, a communications unit, and memory:

transmitting via the communications unit of the mobile device an identifier corresponding to a retail machine to a server and receiving from the server an electronic communication including one or more promotional offers;

displaying on the display of the mobile device the one or more promotional offers;

detecting selection of a respective promotional offer of the one or more promotional offers;

receiving, via the communications unit, notification information from the retail machine associated with provision of a product ~~or service~~ by the retail machine for a user of the mobile device;

in response to receiving the notification information:

capturing, with a camera or scanner of the mobile device, an image or scan associated with the product ~~or service~~ provided by the retail machine, the image or scan including a code; and

transmitting to the server via the communications unit of the mobile device the code and the notification information; and

in response to transmitting the code and the notification information to the server:

receiving, via the communications unit, promotion validation information from the server indicating the respective promotional offer has been applied; and

displaying on the display a confirmation that the respective promotional offer has been applied.

3. (Currently Amended) The method of claim 2, wherein the product ~~or service~~ that was provided is part of a transaction associated with the user of the mobile device, and further wherein the promotion validation information includes promotion validation information with respect to the transaction.

7. (Currently Amended) The method of claim 2, further comprising, before detecting selection of a respective promotional offer, receiving the one or more promotional offers based at least in part on particular products ~~or services~~ offered by the retail machine.

16. (Currently Amended) The method of claim 2, further comprising, in response to receiving the notification information:

providing a prompt instructing the user of the mobile device to confirm that the product ~~or service~~ was provided; and

capturing the image or scan in response to the prompt.

20. (Currently Amended) A mobile device, comprising:

a display;

a communications unit;

one or more processors; and

memory storing one or more programs to be executed by the one or more processors, the one or more programs comprising instructions for:

transmitting via the communications unit of the mobile device an identifier corresponding to a retail machine to a server and receiving from the server an electronic communication including one or more promotional offers;

displaying on the display of the mobile device the one or more promotional offers;

detecting selection of a respective promotional offer of the one or more promotional offers;

receiving, via the communications unit, notification information from the retail machine associated with provision of a product ~~or service~~ by the retail machine for a user of the mobile device;

in response to receiving the notification information:

capturing, with a camera or scanner of the mobile device, an image or scan associated with the product ~~or service~~ provided by the retail machine, the image or scan including a code; and

transmitting to the server via the communications unit of the mobile device the code and the notification information; and

in response to transmitting the code and the notification information to the server:

receiving, via the communications unit, promotion validation information from the server indicating the respective promotional offer has been applied; and

displaying on the display a confirmation that the respective promotional offer has been applied.

21. (Currently Amended) A non-transitory computer readable storage medium storing one or more programs, the one or more programs comprising instructions, which, when executed by a mobile device with a display, a communications unit, and one or more processors, cause the mobile device to perform ~~the~~ functions of:

transmitting via the communications unit of the mobile device an identifier corresponding to a retail machine to a server and receiving from the server an electronic communication including one or more promotional offers;

displaying on the display of the mobile device the one or more promotional offers;

detecting selection of a respective promotional offer of the one or more promotional offers;

receiving, via the communications unit, notification information from the retail machine associated with provision of a product ~~or service~~ by the retail machine for a user of the mobile device;

in response to receiving the notification information:

capturing, with a camera or scanner of the mobile device, an image or scan associated with the product ~~or service~~ provided by the retail machine, the image or scan including a code; and

transmitting to the server via the communications unit of the mobile device the code and the notification information; and

in response to transmitting the code and the notification information to the server:

receiving, via the communications unit, promotion validation information from the server indicating the respective promotional offer has been applied; and

displaying on the display a confirmation that the respective promotional offer has been applied.

The applicant's invention discloses a mobile device with a display, processor(s), and memory: identifies a retail machine configured for wireless communications based on broadcasted information transmitted by the retail machine and including an identifier corresponding to the retail machine; transmits the identifier to a server and receives from the server an electronic communication including a promotional offer for products or services offered by the retail machine; displays the promotional offer; detects selection of a promotional offer; receives a notification from the retail machine that a product or service was provided by the retail machine for a user of the mobile device; transmits confirmation information associated with the notification to the server, receives promotion validation information from the server indicating validation of the promotional offer; and based on the promotion validation information, displays information confirming application of the promotional offer.

Claim 2 is allowed no prior art alone or in combination fails to teach or suggest or otherwise make obvious, all the limitations comprising:

in response to receiving the notification information:

capturing, with a camera or scanner of the mobile device, an image or scan associated with the product provided by the retail machine, the image or scan including a code; and

transmitting to the server via the communications unit of the mobile device the code and the notification information; and

in response to transmitting the code and the notification information to the server:

receiving, via the communications unit, promotion validation information from the server indicating the respective promotional offer has been applied; and

displaying on the display a confirmation that the respective promotional offer has been applied.

Independent claims 20-21 are allowable based on a similar rationale. Dependent claims 3-19 are allowable based on the same rationale as the claims they depend.

The Examiner notes the applicant's invention is directed to patent eligible subject matter under 35 U.S.C. 101. The additional limitations that when considered as an ordered combination demonstrates a technologically rooted solution to a network-centric problem and amounts to 'significantly more' than an abstract idea. Additionally, the claims do not recite the performance of some business practice known from the pre-Internet world with the requirement to perform in on the Internet. The applicant has incorporated the features of a communications unit, mobile device, retail machine, server, processors, scanner, and camera demonstrate the invention is rooted in computer technology. Furthermore, the applicant's specification discloses the following advantages of the invention: "The payment processing system 100 harnesses the connectivity of the mobile device 104 to

communicate with the payment module 124, which has neither a dedicated communication connection nor a long-range communication transceiver. As such, the mobile device 124 acts as a relay between the payment module 124 and the server system 108. Furthermore, leveraging the connectivity of the mobile device 104 helps to keep costs down from the point of view of the operator of the automatic retail machine 122." (paragraph 0035) and "After obtaining the product code, the mobile device transmits (1226) the product code to the server. In response to transmitting the product code, the mobile device: receives promotion validation information from the server; and displays the promotion validation information on the display, where the promotion validation information indicates whether the respective promotion offer was validated. In some implementations, the mobile device 104 or a component thereof (e.g., the product code processing module 242, Figure 2) either validates the obtained product code or sends the obtained product code to the server 108 for validation. In some implementations, the mobile device 104 or a component thereof (e.g., the information relaying module 244, Figure 2) sends the transaction completion notification or a portion thereof to the server 108 regardless of whether the user follows the prompt and the mobile device 104 ultimately obtains the product code. In some implementations, the server 108 determines whether conditions for the respective promotional offer have been based on the transaction and the product code. For example, the server 108 determines whether the proper product code was obtained for the respective promotional offer, whether the respective promotional offer has expired, whether the user has fulfilled a buy N items get one free condition, whether the user has fulfilled cross-promotion condition, and/or the like. In some implementations, the offer is validated and applied by the server 108 to the user's account." (paragraph 0136).

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

USA Technologies Announces Cashless Solution to be Offered by Blackboard Inc., July 18, 2007, Business Wire

The article is about permitting college students to use cashless payments at campus vending machines. Additionally, the vending machines allow students to use a variety of payments options.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW L HAMILTON whose telephone number is (571)270-1837. The examiner can normally be reached Monday-Thursday 9:30-5:30 pm EST.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Waseem Ashraf can be reached on (571)270-3948. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MATTHEW L HAMILTON/
Primary Examiner, Art Unit 3682

Examiner-Initiated Interview Summary	**Application No.** 17/963,170	**Applicant(s)** Patel, Paresh K.		
	Examiner MATTHEW L HAMILTON	**Art Unit** 3682	**AIA (First Inventor to File) Status** Yes	**Page** 1 of 1

All Participants (applicant, applicants representative, PTO personnel)	**Title**	**Type**
MATTHEW L HAMILTON	Primary Examiner	Telephonic
Benjamin Pezzner	Attorney of Record	

Date of Interview: 24 July 2023

Issues Discussed:

Proposed Amendment(s)

The examiner received authorization from the applicant's representative, Mr. Benjamin Pezzner to enter and amend claims via Examiner's Amendment. The claims are allowed.

/MATTHEW L HAMILTON/ Primary Examiner, Art Unit 3682	

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

Petitioner Exhibit 1002-3040

Notice of References Cited	Application/Control No. 17/963,170	Applicant(s)/Patent Under Reexamination Patel, Paresh K.	
	Examiner MATTHEW L HAMILTON	Art Unit 3682	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
	A					
	B					
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	USA Technologies Announces Cashless Solution to be Offered by Blackboard Inc., July 18, 2007, Business Wire (Year: 2007)
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Petitioner Exhibit 1002-3041

Espacenet

Bibliographic data: JPH1125320 (A) — 1999-01-29

AUTOMATIC TELLER MACHINE

Inventor(s): SHIODA TAKUJI; FUKAI MIDORI; ASAWA TAKEO; IWASAKI AKIHIRO; SUGIYAMA MUTSUKO ± (SHIODA TAKUJI, ; FUKAI MIDORI, ; ASAWA TAKEO, ; IWASAKI AKIHIRO, ; SUGIYAMA MUTSUKO)

Applicant(s): FUJITSU LTD ± (FUJITSU LTD)

Classification: **- international:** ***G06F3/048; G06F3/14; G06Q20/18; G06Q40/00; G06Q40/02; G07D9/00; G07F19/00;*** (IPC1-7): G06F19/00; G06F3/14; G07D9/00

- cooperative: **G06Q20/1085 (EP, US); G07F19/20 (EP, US); G07F19/201 (EP, US)**

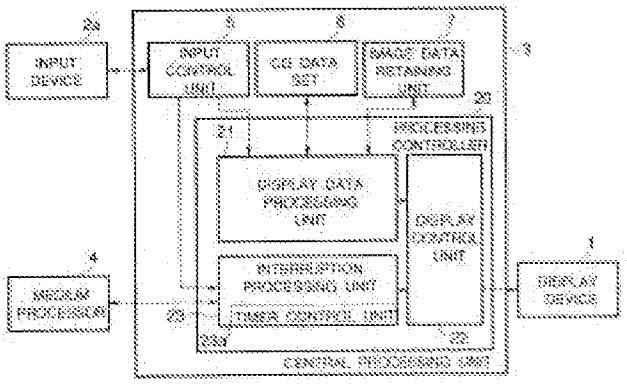
Application number: JP19970182881 19970708

Priority number(s): JP19970182881 19970708

Also published as: JP3856910 (B2) US6073120 (A)

Abstract of JPH1125320 (A)

PROBLEM TO BE SOLVED: To improve operability independently of the skillness of user's operation by displaying a procedure formed by arranging plural input item columns in input order, and at the time of inputting plural information in the input order, displaying operation pictures corresponding to respective information in a state superposed to the display of the procedure. SOLUTION: A processing controller 20 controls the information display of a display device 1 and executes transaction processing based on information inputted from an input device 2a consisting of a transparent touch panel superposed on the display surface of the device 1. The controller 20 displays a procedure display formed by arranging plural input item columns respectively indicating plural information items inputted from the input device 2a in the input order on the



Petitioner Exhibit 1002-3042

device 1. In the case of inputting plural information from the device 2a in the input order, operation pictures corresponding to respective information data are respectively displayed in a state superposed to the surface of the procedure display.

Petitioner Exhibit 1002-3043

Patent Translate
Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

DESCRIPTION JPH1125320A

[0001]

13 BACKGROUND OF THE INVENTION 1. Field of the Invention The present invention relates to an automatic teller's machine (ATM), an automatic teller's machine (CD: cash dispenser), an automatic teller machine, a transfer-only device, or a securities issuing device. It relates to an automatic transaction device called.

[0002]

20 2. Description of the Related Art In recent years, financial institutions such as banks have put into practical use automatic teller machines that enable transactions without the intervention of bank employees.

23 In such an automated teller machine, a desired transaction is performed by a customer interactively performing operations such as inputting information while looking at the screen display of the machine.

[0003]

29 That is, the display device of the automated teller machine displays a start screen displaying all items that can be traded as an initial screen.

31 Then, when the customer selects a desired transaction item on the start screen, processing by the automated teller machine is started. The display has a touch panel, and the customer presses buttons displayed on the display device to operate the automated teller machine and input data.

[0004]

38 When an arbitrary transaction is selected on the start screen (an arbitrary transaction type button displayed on the display device is pressed), the automated teller machine executes processing corresponding to the transaction.

41 That is, the automated teller machine sequentially displays a plurality of transaction screens showing the operation details of the automated teller machine on the display device in accordance with a predetermined operation procedure so that the transaction can be conducted with the customer. On the other hand, when the customer presses a button set in each transaction screen according to the display contents of the transaction screen, the operation procedure is advanced and the next transaction screen is displayed on the display device. When all operating procedures are completed, transaction processing by the automatic transaction device is completed, and the transaction is treated as having been executed between the customer and the financial institution.

[0005]

53 Transactions with financial institutions are indispensable in daily life, and according to certain data, about 80% of customers who visit financial institutions such as banks use automated teller machines to conduct transactions.

56 It can be said that the automated teller machines used by the majority of people are highly public devices.

[0006]

61 However, conventional automated teller machines have the following problems.

62 That is, the users of automatic teller machines span a wide range of age groups, from the young to the elderly. In addition, the knowledge of how to operate automatic teller machines, knowledge of transactions with financial institutions, etc., varies widely from one user to another. In other words, the degree of proficiency in operating an automated teller machine varies greatly depending on the user. In order to cope with this, it is desired that automatic transaction machines are configured to provide an equal operating environment to all users regardless of their proficiency level.

[0007]

72 However, in the conventional automatic transaction machine, the operation of the automatic transaction machine is performed according to the instructions displayed on each transaction screen, but each transaction screen only shows the operation contents at that time.

75 Each transaction screen was completely switched to the next transaction screen each time the operation procedure progressed (see FIGS. 32 and 33). Therefore, the user can grasp the operation that has already been performed, the content of the data that has already been input, the content of the operation to be performed from now on, or the overall flow of the operation procedure from the display content of the transaction screen that is currently

displayed on the display. I couldn't. As a result, the user cannot grasp the current operation and the progress of the operation procedure, and there are cases where the user erroneously inputs data or erroneously operates the device.

[0008]

86 In addition, in the conventional automatic transaction machine, only one operation procedure is set for each of a plurality of transactions that can be executed using the automatic transaction machine, and a plurality of transaction screens according to this operation procedure are sequentially displayed on the display. It was only displayed (see FIGS. 31, 32, and 33).

91 For this reason, the users of the automated teller machine have had to operate the automated teller machine according to the same operating procedures regardless of their level of proficiency. Here, the operation procedure of the automated teller machine has been set according to users having an average degree of proficiency in operation, in order to accommodate as wide a range of users as possible.

[0009]

99 Therefore, the operation procedure is simple for users with low proficiency, and redundant for users with high proficiency.

101 Therefore, a user with a low proficiency may not grasp or predict the sequence of operation procedures or the operation method of the automatic teller machine, and may perform an erroneous operation. On the other hand, users with a high level of proficiency find it troublesome to operate automatic teller machines according to redundant operating procedures. Incorrect data entry or incorrect operation may occur.

[0010]

109 SUMMARY OF THE INVENTION An object of the present invention is to provide an automated teller machine capable of improving operability regardless of the user's proficiency in operation.

[0011]

115 SUMMARY OF THE INVENTION The present invention employs the following configurations to solve the above-described problems.

117 That is, the invention of claim 1 comprises a display device for displaying information, an input device for inputting information relating to transactions, and a display device for controlling the display of information on the display device and controlling the information displayed on the display device according to the information displayed on the display device. and a control unit that performs transaction processing based on information input from an

input device.

123 In this automatic teller machine, the control unit displays, on the display device, a procedure display formed by arranging a plurality of input item fields each showing a plurality of information items to be input from the input device in order of input. Further, when each of the plurality of information is input from the input device according to the input order, an operation screen corresponding to each information is displayed in a state superimposed on the procedure display.

[0012]

132 According to the first aspect of the invention, the control unit causes the display device to display the procedure display.

134 Then, when each of a plurality of pieces of information is input, the control unit causes the operation screen corresponding to each piece of information to be displayed in a state of being superimposed on the procedure display. Therefore, the user of the automated teller machine can understand information such as multiple input items, the number of input items, the order of input, etc. from the procedure display, and operate using the operation screen displayed superimposed on the procedure screen. becomes possible.

[0013]

143 The invention of claim 2 specifies that the procedure display of claim 1 is always displayed on the display device.

145 The invention according to claim 3 comprises a display device for displaying information, an input device for inputting information related to transactions, and the input device for controlling information display of the display device and according to the information displayed on the display device. and a control unit that performs transaction processing based on information input from. In this automated teller machine, a specific area is set on the screen of the display device, and the control section displays a plurality of information items input from the input device on the display device. Displaying a procedure display formed by arranging a plurality of input item fields in order of input, and moving the procedure display in a direction substantially perpendicular to the longitudinal direction of each of the input item fields according to the progress of the operation procedure of the transaction. to display an input item column corresponding to an operation currently being performed among the plurality of input item columns in the specific area.

[0014]

160 According to the invention of claim 4, the operation screen is arranged below the specific area of claim 2, an explanation display showing explanation of the operation screen is arranged above the specific area, and the explanation display is above the explanation display. It is specified by arranging a transaction type display field in which the transaction

type is indicated in the .

[0015]

168 In the invention of claim 5, each of the input item fields of claim 2 is formed with an input information display area in which information corresponding to the input item is displayed, and the control unit receives input from the input device. In response to a request from a user, the content displayed on the display device is returned to the state at the time when the information held in the holding means was input, and the corresponding information is read out from the holding means. is specified by displaying it in the input information display area.

[0016]

178 According to the invention of claim 6, the control unit of claim 5 excludes at least the operation screen in the range overlapping with the procedure display from the display contents of the display in response to a request from the user, and the information held in the holding means is specified by displaying in the input information display area of the corresponding input item column.

[0017]

186 The invention of claim 7 is specified by the control unit of claim 1 changing the change speed of the display content of the display device according to a request from the user.

188 According to an eighth aspect of the invention, the control unit according to claim 1 has information presenting means for displaying operation information related to the input of information on the display device when information is input from the input device, and the information is displayed on the display device. This is specified by changing the number of times the operation information is displayed on the display device by the presentation means according to a request from the user.

[0018]

197 According to the ninth aspect of the invention, when the control unit according to the second aspect displays the procedure display on the display device, the number of input item columns constituting the procedure display and the procedure display are fixed or not. When the number of input item fields is less than the fixed threshold, the procedure display is fixed and displayed on the display device, thereby specifying the is.

[0019]

205 According to the invention of claim 10, the control unit of claim 3 enlarges and displays the

input information display area of the input item column displayed in the specific area and the information displayed in this input information display area. It is specified.

[0020]

211 The invention of claim 11 is specified by displaying a part of the operation screen of claim 1 translucently.

213 The invention of claim 12 is specified by providing the transaction type display column of claim 4 with a cancel button for forcibly terminating the processing related to the transaction.

[0021]

219 According to the invention of claim 13, the input information display area in each of the plurality of input item fields of claim 5 is provided with a button for correcting the information displayed in the input information display area. It is specified.

[0022]

225 In the invention of claim 14, when all the information in the transaction is input, the control unit of claim 5 displays the procedure display on the display as a confirmation screen for each input information, and displays all the information. Each piece of information is specified by displaying it in the corresponding input information display area.

[0023]

232 According to the invention of claim 15, the plurality of input item fields of claim 3 are classified into a plurality of operation sets according to the attributes of the information input from the input device, and each set is displayed in a different color. It is specified by the presence of

[0024]

239 The invention of claim 16 specifies that the plurality of input item fields constituting the operation set of claim 15 are color-coded in a state of drawing a gradation according to the order of information input.

[0025]

245 The invention of claim 17 is specified by changing the basic color of the background of the screen forming the display content of the display device of claim 15 according to the color of the input item column displayed in the specific area. is.

[0026]

251 According to the invention of claim 18, the control unit of claim 1 detects the input time that is the time required for the user to input specific information, and determines the detected input time and the user's operation proficiency. If the input time is less than the proficiency threshold, the change speed of the display content of the display device is increased to specify the input time.

[0027]

259 According to a nineteenth aspect of the invention, the control unit according to the eighteenth aspect of the invention has information presenting means for causing the display device to display operation information related to the input of information when information is input from the input device, When the time is less than the proficiency level threshold, it is specified by reducing the number of times the operation information is displayed on the display device by the information presenting means.

[0028]

268 The invention according to claim 20 comprises a display device for displaying information, an input device for inputting information related to transactions, and a display device for controlling information display on the display device and controlling the information displayed on the display device according to the information displayed on the display device. and a control unit that performs transaction processing based on information input from.

273 In this automated teller machine, the control unit selects either one of a procedure consisting of a plurality of operations and a plurality of procedures corresponding to the plurality of operations included in the one procedure in accordance with a user's request. characterized by providing

[0029]

280 According to the invention of claim 21, when the control unit of claim 1 or 20 does not input information from the input device for a predetermined time, the display device displays a caution display for prompting the input of information, It is specified.

[0030]

286 The invention of claim 22 is specified by causing the control unit of claim 1 or 20 to display information input operation guidance on the display device when there is no information input from the input device for a predetermined time. be.

[0031]

292 23. The invention according to claim 1 or 20, wherein the screen displayed on the display when information is input from the input device is generated by synthesizing a plurality of image data by the control unit. , the image corresponding to each image data is specified by being displayed in a predetermined area set on the screen of the display device.

[0032]

299 In the twenty-fourth aspect of the present invention, the control unit of the fourth aspect possesses a plurality of types of image data for the explanation display and image data for the operation screen, and generates image data for the procedure display according to the type of transaction. Identify any of a plurality of input item fields that form a procedure display according to the order of inputting information, obtain image data of the explanation display and image data of the operation screen corresponding to the items in the identified input item field, and obtain the obtained procedure. This is specified by generating image data to be displayed on the display device using display image data, operation screen image data, and created procedure display image data.

[0033]

311 The invention of claim 25 is characterized in that the automated teller machine of claim 1 or 20 further comprises voice output means for outputting a voice when the control unit becomes capable of receiving information from the input device. It is what I did.

[0034]

317 According to the invention of claim 26, the automated teller machine of claim 3 comprises voice output means for outputting a voice when said control unit moves said procedure display in a direction substantially perpendicular to the longitudinal direction of each of said input item fields. It is specified by further comprising

[0035]

324 A twenty-seventh aspect of the invention is characterized in that the input device according to the first aspect or the twenty-first aspect is a touch panel, and position detecting means for detecting position information of an object in contact with the touch panel; determining means for determining whether or not the object changes its position while in contact with the touch panel; and outputting a warning sound when the determining means determines that the object changes its position while in contact with the touch panel. It is specified by having an audio output means.

[0036]

334 BEST MODE FOR CARRYING OUT THE INVENTION Embodiments of the present invention will now be described with reference to the drawings.

336 [Embodiment 1] First, Embodiment 1 according to the present invention will be described.

337 [Construction of Automatic Transaction Machine] FIG. 1 is a block diagram showing the main construction of an automatic teller machine (hereinafter referred to as "ATM", corresponding to an automatic transaction machine) according to the first embodiment.

340 In FIG. 1, the ATM comprises a display device 1, an input device 2a, a central processing section 3 and a media processing device 4. FIG.

[0037]

345 The display device 1 uses, for example, a CRT display or a liquid crystal display panel to display ATM operation information and the like.

347 The input device 2 a is a transparent plate-shaped switch (touch panel) superimposed on the display surface of the display device 1 .

349 The input device 2a detects the position where the user touches the touch panel, and inputs information corresponding to this position to the central processing unit 3. FIG.

351 The media processing device 4 handles media including magnetic cards, passbooks, slips, cash, and the like.

[0038]

356 The central processing unit 3 includes an input control unit 5 , a CG (Character Generator) unit 6 , an image data holding unit 7 and a processing control device 20 .

358 The input control unit 5 controls the input device 2a.

359 The CG section 6 has a character generator consisting of data sets for storing character patterns (character codes, font data) required for display, for example, and generates character data constituting display information such as messages displayed on the display device 1. Generate.

363 Image data holding unit 7 stores in advance a plurality of image data for forming a display screen to be displayed on display device 1 .

365 Each of the plurality of image data is read out from the image data holding unit 7 and used for display as required.

367 Further, each image data is synthesized with a character pattern generated by the CG section 6 as necessary and used for display.

[0039]

372 The image data stored in the image data holding unit 7 may be drawing data of an ATM, for example, and is image data obtained by taking an image of an actual ATM with an imaging

device such as a video camera and extracting only a necessary portion. It can be.

[0040]

378 The processing control device 20 has a display data processing section 21 , a display control section 22 and an interrupt control section 23 .

380 The processing control device 20 controls information display by the display device 1 and performs transaction processing based on information input from the input device 2 a via the input control section 5 .

383 The processing control device 20 is a device that performs main processing control by functioning, for example, software-led control of the central processing unit 3, and is configured by, for example, a microprocessor unit.

[0041]

389 The display data processing unit 21 controls the display based on information such as input information, display character data, image data, and interrupts obtained from the input control unit 5, the CG unit 6, the image data holding unit 7, and the interrupt processing unit 23. Display data to be displayed on the device 1 is generated and supplied to the display control unit 22 .

[0042]

397 The display control unit 22 controls the display device 1 based on the display data received from the display data processing unit 21 to perform screen display according to this display data.

400 The interrupt processing unit 23 has a timer control unit 23 a for timer interrupt, and performs interrupt control for the display data processing unit 21 according to information from the input control unit 5 and the media processing device 4 .

[0043]

406 FIG. 2 is a perspective view showing the external configuration of an ATM in which the configuration shown in FIG. 3 is incorporated.

408 FIG. 2 shows an ATM housing, a display input unit 31 consisting of the display device 1 and the input device 2a shown in FIG. A card insertion/extraction opening 33 for withdrawal, a coin insertion/extraction opening 34 for inserting/extracting coins, and a bill insertion/extraction opening 35 for inserting/extracting bills are shown.

[0044]

415 FIG. 3 is a block diagram showing a specific internal configuration of ATM.

416 In FIG. 3, the ATM has a certificate output/card reading/writing unit DOC, a banknote recycling unit BRU, a coin recycling unit CRU, a customer operation unit UOP, a management operation unit MOP, a control unit CPU, and a power supply unit PSU. ing.

[0045]

422 The control unit CPU corresponds to the central processing unit 3 described above (see FIG. 1).

424 The control unit CPU is connected to a host computer in the center via a transmission line such as a communication line.

426 Alternatively, the control unit CPU is connected to a terminal controller (a plurality of terminal devices such as ATMs are connected to the terminal controller) from a transmission line such as a communication line, and is coupled to the host computer of the center via this terminal controller. ing.

430 The ATM communicates with the center to proceed with the transaction while updating the center's ledger, ie, the file in which the individual's balance, transaction history, etc. are stored.

[0046]

436 In addition, the control unit CPU includes a remote monitoring unit RSU for remotely monitoring the status of ATMs installed in branch offices and unmanned stores (stores where only ATM devices are installed). are coupled via transmission lines.

439 The remote monitoring unit RSU monitors a plurality of ATMs and performs failure prevention, failure detection, failure countermeasures, maintenance, or the like.

[0047]

444 The certificate output/card read/write unit DOC, bill recycling unit BRU, and coin recycling unit CRU correspond to the above-described medium processing device 4 (see FIG. 1).

446 The certificate output/card reading/writing unit DOC comprises a card reading/writing/image reading/printer unit CIP and a passbook printer unit PPR.

448 The card reading/writing/image reading/printing section CIP comprises a card reader/writer section 41, a card embossing reading section 42, a printer section 43, and a transfer card issuing section 44. FIG.

[0048]

454 The card reader/writer unit 41 reads information such as an account number, a branch number, etc., from the magnetic stripe of the card inserted into the card insertion/extraction port 33 for conducting transactions, and writes to the magnetic stripe as necessary. .

457 The card emboss reading unit 42 reads the name of the embossed portion of the card inserted

into the card insertion/extraction port 33, the account number, and the like.

459 The printer unit 43 prints the account number, transaction amount, etc. read from the card on a receipt (statement slip) and outputs it from the card insertion/extraction port 33, and stores the same data printed on the receipt as a copy of the printed information, i.e., a journal. Leave as

463 The transfer card issuing unit 44 writes the transfer information such as the transfer destination on the magnetic stripe on the back side of the transfer card used for the transfer transaction, prints necessary information on the blank portion on the front side, and issues the transfer card.

467 This transfer card is also output from the card insertion/extraction port 33 .

[0049]

471 The passbook printer PPR has a passbook magnetic stripe reader/writer section 45 and a passbook printer section 46 .

473 The passbook magnetic stripe reader/writer unit 45 reads and writes the magnetic stripe of the passbook inserted into the passbook insertion/extraction port 32, for example.

475 The passbook printer unit 46 prints the transaction history on the passbook.

476 The banknote recycle unit BRU has, for example, three stackers 47, 48, 49 and an attendant safe 50, and handles banknotes.

[0050]

481 The three stackers 47 to 49 are, for example, one stacker 47 for storing 1,000 yen bills and two stackers 48 and 49 for storing 10,000 yen bills.

483 When a payment transaction is performed, only the designated amount is paid out from the respective stackers 47 to 49 to the banknote insertion/extraction port 35, and when a deposit transaction is performed, the banknotes inserted in the banknote insertion/removal port 35 are sorted by denomination. are stored in respective stackers 47-49.

487 Note that the 5,000-yen bills are stored in a collection-only stacker (not shown).

488 Furthermore, the three stackers 47 to 49 exchange bills with a detachable attendant safe 50 as necessary.

490 That is, when the number of banknotes in any of the three stackers 47 to 49 decreases as a result of continuous withdrawal transactions, the stacker whose banknotes have decreased is replenished with banknotes from the attendant safe 50, and deposit transactions continue. is done.

494 On the other hand, when any one of the stackers 47 to 49 is full of banknotes, the banknotes are collected from the full stacker and transported to the clerk's safe 50 .

[0051]

499 The coin recycling unit CRU consists of stackers 51, 52, 53, 54, 55, 56 for each coin, an

overflow stacker 57, and a coin cassette 58, and handles coins.

501 When it becomes necessary to pay out coins due to a transaction such as a payment transaction or a transfer transaction that requires change, the required number of coins and the required amount of coins are delivered from the stackers 51 to 56 to the coin insertion/extraction port. 34 pays out. Also, when coins are inserted into the coin insertion/extraction opening 34, the inserted coins are stored in the respective stackers 51 to 56 by denomination. Furthermore, when coins are continuously dispensed and the coins in the stackers 51-56 run short, coins are replenished from the coin cassette 58 to the stackers 51-56. Furthermore, coins overflowing from the stackers 51 to 56 are stored in the overflow stacker 57 as the coins are continuously stored. The overflow stacker 57 and the coin cassette 58 are detachable and used for refilling and taking out coins.

[0052]

514 The customer operation unit UOP has a color display device 59 as the display device 1 and a touch keyboard 60 composed of a touch panel as the input device 2a overlaid on the display screen.

517 That is, the display surface of color display device 59 and touch keyboard 60 constitute display input section 31 shown in FIG.

[0053]

522 The management operation unit MOP has a liquid crystal display 61 and a keyboard 62, and, like the remote monitoring unit RSU, grasps the internal state of the ATM and enables necessary maintenance operations.

[0054]

528 The audio output unit 60 is composed of an audio processor, an amplifier circuit, a speaker, and the like.

530 This audio output unit 60 outputs audio to the outside according to a command from the control unit CPU.

532 [Processing by ATM] Next, processing for the customer operation unit UOP by the control unit CPU will be described as processing by the above-mentioned ATM. In FIG. 1, when the power supply unit PSU shown in FIG. The program is loaded into the RAM 9, the control program loaded into the RAM 9 is executed, and screen display processing for the display device 1 is started.

[0055]

540 FIG. 4 is a flow chart showing screen display processing for the display device 1 .

541 In FIG. 4, when the process starts, the display data processing unit 21 determines whether

position information has been transferred from the touch panel, which is the input device 2a, via the input control unit 5 (step S01). At this time, if the display data processing unit 21 determines that the position information has not been received, the process proceeds to step S04. On the other hand, when the display data processing unit 21 determines that the position information has arrived, it acquires the position information (step S02).

[0056]

550 Subsequently, based on the acquired position information, the display data processing unit 21 determines whether or not the user has pressed an ATM operation button such as "cancel" or "correction" displayed on the display device 1. .

553 At this time, if the display data processing unit 21 determines that the operation button has been pressed (step S03; YES), the process proceeds to step S05. On the other hand, when the display data processing unit 21 determines that the operation button has not been pressed (step S03; NO), it is assumed that the data input key has been pressed, and the process proceeds to step S04.

[0057]

561 When the process proceeds to step S04, the display data processing unit 21 outputs character data corresponding to the position information acquired in step S02 (character data corresponding to the pressed key (button)) from the CG unit 6. After reading, the process proceeds to step S05.

[0058]

568 When the process proceeds to step S05, the display data processing section 21 reads character data from the CG section 6 and reads image data (texture data) from the image data holding section 7 according to the control program.

571 Subsequently, the display data processing unit 21 generates screen data by synthesizing the character data and the image data on its own VRAM (Video RAM) (not shown) (step S06).

573 Subsequently, the display data processing unit 21 transfers the storage contents of the VRAM (not shown) to the display control unit 22 (step S07).

[0059]

578 Then, the display control unit 22 converts the storage contents of the VRAM (not shown) into a video signal (step S08) and transfers it to the display device 1 (step S09).

580 As a result, the ATM transaction screen 70 (see FIG. 5) is displayed on the display device 1, and the information input from the input device 2a is also displayed. In addition, when the process of step S09 ends, the process returns to step S01. [Contents displayed on the display device] Next, the contents displayed on the display device 1 will be described. <Transaction

Screen> FIG. 5 is an explanatory view of a transaction screen 70 displayed on the display device 1. As shown in FIG. A user of the ATM operates the ATM according to the display contents of the transaction screen 70 displayed on the display device 1 to carry out transactions. A plurality of transaction screens 70 are displayed on the display device 1 according to the operation procedure preset in the ATM. At this time, even if the transaction screen 70 is switched to another transaction screen 70, the transaction screen 70 is configured as follows so that the user can properly grasp the display contents of the transaction screen 70.

[0060]

595 5, the transaction screen 70 is set in a rectangular shape, and consists of a transaction type display area 71, an operation explanation area 72, an input object display area 73, an input data display area 74, and an operation area 75.

[0061]

601 The transaction type display area 71 is a belt-like area set at the top of the transaction screen 70, and displays the transaction type (for example, "transfer", "withdrawal", "deposit", etc.).

603 The operation explanation area 72 is a band-shaped area set immediately below the transaction type display area 71, and displays a character string indicating an ATM operation explanation for the user.

[0062]

609 The input object display area 73 and the input data display area 74 are belt-shaped areas set immediately below the operation explanation area 72 .

611 The input object display area 73 is arranged on the left side of the transaction screen 70 , and the input data display area 74 is arranged on the right side of the transaction screen 70 .

613 The input object display area 73 displays a character string indicating an input object (for example, "client name", "deposit amount", "account number", etc.). The input data display area 74 displays a character string indicating data input by the user of the ATM via the input device 2a.

[0063]

620 The operation area 75 is a rectangular area set at the bottom of the transaction screen 70 .

621 In this operation area 75, keys for the user to input data to the ATM and operation buttons of the ATM are displayed.

[0064]

626 The positions of the regions 72 to 75 described above are fixed regardless of changes in the display content of the display device 1 .

628 Therefore, the user of the ATM can grasp or predict which information will be displayed at which position while proceeding with the operation of the ATM. Therefore, even when the transaction screen 70 is switched to another transaction screen 70, the user can properly grasp the contents displayed on the transaction screen 70, so that the user can smoothly operate the ATM and carry out transactions. can. <Screen Elements of Transaction Screen> FIG. FIG. 6 shows screen elements of the transaction screen 70 in the case of "transfer". As shown in FIG. 6, the transaction screen 70 is configured by superimposing each screen element of a background 81, a procedure display 82, an input panel display 83, and an explanation display 84 according to the ATM operation procedure. These screen elements are stored as texture data in the image data holding unit 7 shown in FIG. The image data holding unit 7 also has color palette data corresponding to these texture data. Then, the transaction screen 70 is displayed on the display device 1 by performing the above-described screen display processing (see FIG. 4). <Background> In FIG. 6, the background 81 is set in a rectangular shape and arranged over the entire transaction screen 70 . A strip-shaped transaction type display field 81a is provided above the background 81, and is arranged in the transaction type display area 71 shown in FIG. A character string indicating the transaction type is displayed in the transaction type display field 81a (in FIG. 6, the character string "transfer" is shown as an example). <Procedure display> The procedure display 82 is superimposed on the background 81 and displayed. This procedure display 81 is arranged over the operation explanation area 72, the input object display area 73, the input data display area 74, and the operation area 75 shown in FIG. This procedure display 82 shows the operation procedure to be performed by the ATM user at the time of transaction. That is, the procedure display 72 consists of a plurality of strip-shaped input data fields 87 (input data fields 87a to 87g are shown as examples in FIG. 6). Each input data column 87 is a column for displaying data or the like to be input to the ATM according to the operating procedure of the ATM. there is

[0065]

657 On the leftmost side of each of the plurality of input data fields 87, a number indicating the procedure number, which is the order of the operation procedure, is displayed, and on the right side, an input object name (operation item name) is displayed.

660 A character string indicating the data input via the input device 2a is displayed on the right side of the input object name.

[0066]

665 FIG. 7 is a diagram showing a screen display example of a transaction screen 70 in which a procedure display 82 is superimposed on a background 81. As shown in FIG.

667 In the example shown in FIG. 7, in each of the input data fields 87a to 87g, a number

indicating the procedure number is displayed on the leftmost side thereof, and on the right side thereof, as input object names, "payee financial institution", "payee Item names such as branch name, account number, recipient name, transfer amount, client name, and telephone number are displayed. Input data corresponding to each input object name is displayed on the right side of each input object name.

[0067]

676 By the way, an operation procedure is composed of a plurality of operation sets consisting of procedures that can be associated.

678 Correspondingly, in each input data field 87, a plurality of input data fields 87 constituting an operation set are arranged in a lump, and the input data fields 87 constituting mutually different operation sets are arranged at intervals. It is

[0068]

684 For example, in the example shown in FIG. 7, the operation procedure for "transfer" consists of an operation set related to the payee, an operation set related to the amount, and an operation set related to the client.

687 According to the configuration of such operation sets, the input data fields 87a to 87d corresponding to the operation set related to the payee and the input data fields 87f and 87g corresponding to the operation set related to the client each form one block. It is arranged in a state of eggplant. A space (blank) is provided between the input data column 87d and the input data column 87e, and between the input data column 87e and the input data column 87f.

[0069]

696 Therefore, by looking at the procedure display 82, the user of the ATM can easily grasp the number of operation procedures, the number of operation sets, the order of the operation procedures, and the input objects.

699 <Background Color of Procedure Number> Although not shown in FIG. 7, the background color of each procedure number is displayed in a different color depending on the operation set. Specifically, the background color of each procedure number in the input data fields 87a to 87d is set in red gradation according to the numerical order, and the background color of the procedure number in the input data field 87e is set in green. The background color of the procedure number in the input data fields 87f and 87g is set with a blue gradation in numerical order.

[0070]

709 This allows the ATM user to grasp the operation set without understanding the meaning of

the operation set.

711 Further, as the operation procedure progresses, the background color of the procedure number changes from the long wavelength color to the short wavelength color, so that the user can grasp or predict the progress of the operation procedure from the background color of the procedure number.

[0071]

718 Also, the basic color of the background 81 of the transaction screen 70 changes according to the background color of the procedure number.

720 For example, if the background color of the procedure number corresponding to the operation procedure currently being performed is red, the base color of the background 81 is red. This allows the user to easily grasp which operation set the operation currently being performed belongs to. <Attention Area> In FIG. 7, a band-shaped range from about three-tenths to about four-tenths from the upper edge of the transaction screen 70 is set as an attention area 80 . This gaze area 80 is a range where information can be received with high accuracy in ergonomics. The input target display area 73 and the input data display area 74 described above are arranged in this gaze area 80 . In this manner, the oblong gaze area 80 is set, the operation explanation area 72 is set above the gaze area 80, and the operation area 75 is set below the gaze area 80, thereby suppressing unnecessary movement of the line of sight. be done. Therefore, the visibility of the transaction screen 70 can be improved, and the difficulty of understanding the transaction screen 70 and the difficulty of operation can be improved.

[0072]

736 Each of the plurality of input data fields 87 described above is displayed in the gaze area 80 (the input object display area 73 and the input data display area 74) according to the operation procedure.

739 For example, as shown in FIG. 7, if the transaction is "transfer", first, an input data column 87 (input data column 87a) displaying the procedure number "1" is displayed in the attention area 80. FIG. After that, when the data input is completed and the operation procedure proceeds to the next step, as shown in FIG. A column 87 b) is displayed in the gaze area 80 .

[0073]

746 That is, the procedure display 82 is scrolled to the upper side of the screen each time the operation procedure progresses, and an input data field 87 displaying the next procedure number is displayed in the gaze area 80 .

749 Among the data displayed in the input data field 87 in the gaze area 80, the procedure number and the input object name are displayed in the input object display area 73 in the gaze area 80, and the character string indicating the input data is displayed in the gaze area.

80 is displayed in the input data display area 74 .

[0074]

756 In this manner, an input data field 87 indicating the operating procedure currently in progress is displayed in the gaze area 80. FIG.

758 Therefore, if the user of the ATM is looking at the attention area 80, which is the most visible part of the transaction screen 70, he/she can read the procedure number displayed in the attention area 80 and the character string indicating the input object. It is possible to easily grasp the operating procedure that is currently being performed and the progress of the operating procedure. In addition, by scrolling the procedure display 82, the user can intuitively understand that the operation procedure is progressing.

[0075]

767 Also, when the procedure display 82 is scrolled, the ATM emits a signal sound.

768 This function is such that when the process of scrolling the procedure display 82 is being performed, an operation command is given from the control unit CPU to the audio output unit 60 (see FIG. 3), and the audio output unit 60 outputs a signal sound. can be realized by With this signal sound, the user can be made to pay attention to the transaction screen 70, and the user can appropriately understand that the operation procedure has progressed. Therefore, it is possible to eliminate the time loss that occurs when the user does not notice the progress of the operation procedure, and to shorten the operation time of the ATM.

[0076]

778 As in the example shown in FIG. 7, when the number of transaction operation procedures is small, all of the plurality of input data fields 87 forming the procedure display 82 are displayed on the display device 1 at the start of the transaction.

781 On the other hand, when the number of operation procedures in a transaction is large and all of the plurality of input data fields 87 cannot be displayed on the display device 1 at the start of the transaction, the screen display example shown in FIG. , only the displayable input data field 87 is displayed on the display device 1 .

[0077]

788 The functions described above are realized, for example, as follows.

789 That is, the display data processing unit 21 shown in FIG. 1 has the number (threshold value) of the input data fields 87 that can be displayed on the display device 1 at one time. At the start of the transaction, the display data processing unit 21 receives the data of the corresponding procedure display 82 from the image data holding unit 7, and compares the number of input data columns 87 forming the procedure display 82 with the above

threshold. At this time, if the number of input data columns 87 is less than the threshold, the display data processing unit 21 causes the display device 1 to display all of the input data columns 87 forming the procedure display 82 . On the other hand, when the number of input data columns 87 is below the threshold, the display data processing section 21 causes the display device 1 to display a part of the input data columns 87 forming the procedure display 82 .

[0078]

803 As shown in the screen display example of FIG. 9(b), each time one operation procedure is completed and the procedure display 82 is scrolled to the upper side of the screen, any of the input data fields 87 that could not be displayed at the start of the transaction are displayed. is displayed on the screen.

807 At this time, when the procedure display 82 is scrolled to the upper side of the screen so that a part of the procedure display 82 overlaps the transaction type display column 81a, the procedure in the range overlapping the transaction type display column 71a is displayed. Display 82 disappears from trading screen 70 .

[0079]

814 By the way, if the number of operating steps for a transaction is small (for example, if the operating procedure is completed by entering the "PIN" and "Refund Amount", as in a "refund" transaction), the operating procedure is as follows. The procedure display 82 does not scroll even if it advances.

818 In this case, as shown in FIG. 16, the explanation display 83 and the input panel display 84 are arranged in the lower part of the transaction screen 70 in contact with each other.

[0080]

823 This function can be realized by configuring the processing control device 20 shown in FIG. 1 as follows.

825 That is, as described above, the display data processing unit 21 compares the number of input data columns 87 of the procedure display 82 to be displayed with the threshold, and if the number of input data columns 87 exceeds the threshold, the operation is performed. When the procedure proceeds to the next step, the procedure display 82 is scrolled, and if the number of input data fields 87 is less than the threshold value, the transaction screen 70 shown in FIG. The scrolling process of the procedure display 82 is not performed even if the process proceeds to the next step. <Description Display and Input Panel Display> Returning to FIG. 6, the description display 83 is set in a strip shape, and displays a character string indicating an operation explanation in each operation procedure (in FIG. Please press confirm" string). This explanation display 83 is arranged in the operation explanation area 72 shown in FIG.

[0081]

839 The input panel display 84 is set in a rectangular shape, and displays keys and buttons for inputting the input objects displayed in the input object display area 73 in each operation procedure.

842 This input panel display 84 is arranged in the operation area 75 shown in FIG.

[0082]

846 10 to 12 are explanatory diagrams showing screen display examples of the explanation display 83 and the input panel display 84. FIG.

848 As shown in FIGS. 10 to 12, a plurality of types of explanation display 83 and input panel display 84 are prepared according to the input target of the user. For example, an explanation display 83a and an input panel display 84a (see FIG. 10) for entering an account number, an explanation display 83b and an input panel 84b (see FIG. 11) for entering an amount, and an explanation display for entering characters. 83c and an input panel display 84c (see FIG. 12) are prepared.

[0083]

857 As shown in FIG. 10, the input panel display 84a is provided with a numeric keypad 91 for inputting an account number and a first confirmation button 92 for temporarily confirming the input account number.

860 Further, as shown in FIG. 11, the input panel display 84b has a numeric keypad 91 for inputting an amount, a digit button 93 for inputting a digit (10,000,000), and a A first confirmation button (circular button) 92 and the like are provided. Further, as shown in FIG. 12, the input panel display 84c includes a Japanese syllabary key group 94 for inputting characters, and word keys for inputting specific words (corporation, limited company, sales office, branch). A group 95, a first confirmation button 92, etc. are provided.

[0084]

869 In this way, since the input panel display 84 arranged in the operation area 75 is a separate screen element from the procedure display 82, the input panel display 84 (operation area 75) can occupy a large proportion of the transaction screen 70. .

872 Therefore, it is possible to optimize the size of the keys and buttons displayed on the input panel display 83, their arrangement, and the like. Therefore, it is possible to reduce the possibility of erroneous input and erroneous operation due to erroneous pressing of keys or buttons. This is particularly effective for users with low proficiency in operating ATMs, or for users with diminished visual or manual dexterity.

[0085]

880 Note that icons may be provided instead of the keys and buttons displayed on the input panel display 84 .

882 <Switching of Transaction Screens> Incidentally, the background 81 and the procedure display 82 described above are displayed on the display device 1 from the start of the operation of the ATM by the user until the end of the operation. Therefore, the user can grasp the overall picture of the input operation to be performed from now on, and understand the relationship between the preceding and succeeding items. Therefore, it is possible to mentally prepare for each input object (each operation procedure) in advance. In addition, in each operation procedure, the user does not feel uneasiness or frustration due to not being able to grasp the entire operation procedure. Furthermore, it is possible to avoid the danger of erroneously interpreting the content of the input request and making an erroneous input.

[0086]

895 On the other hand, the explanation display 83 and the input panel display 84 are displayed on the display device 1 at the start of each operation procedure, depending on the operation procedure.

898 In the ATM according to Embodiment 1, the transaction screen 70 is switched by switching the explanation display 83 and the input panel display 84 according to the operation procedure. When each operation procedure is started, as shown in the screen display example of FIG. 13, an explanation display 83 appears from the lower edge of the screen and moves toward the upper edge of the screen until it fits within the operation explanation area 72 described above. Moving. Simultaneously with the appearance of the explanation display 83 or following the appearance of the explanation display 83, the input panel display 84 appears from the lower edge of the screen and moves toward the upper edge of the screen until it fits within the operation area 75 described above. .

[0087]

910 Then, when the explanation display 83 fits in the operation explanation area 72 and the input panel display 84 fits in the operation area 75 , the part of the procedure display 82 that exists in the operation explanation area 72 and the part that exists in the operation area 75 (explanation display) 83 or the portion overlapping with the input panel display 84) is hidden by the explanation display 83 or the input panel display 84 .

915 As a result, the ATM user can see only the input object name displayed in the gaze area 80 among the input object names shown in the procedure display 72 . Therefore, the user can clearly grasp the operating procedure currently being performed.

[0088]

921 However, the explanation display 83 and the input panel display 84 are set so as not to overlap the numbers indicating each procedure number in the procedure display 82 .

923 Therefore, the user of the ATM can grasp the number of operation procedures even while data is being input, and can grasp how far the current operation procedure has progressed.

[0089]

928 Thereafter, data is entered using the input panel display 84, and when the operating procedure is completed, the explanation display 83 and the input panel display 84 move toward the lower edge of the screen and disappear from the display device 1. FIG.

931 Then, when the operation procedure proceeds to the next step, the explanation display 83 and the input panel display 84 corresponding to the operation procedure appear in the display device 1 by the method described above. Also, the procedure display 82 scrolls to the upper side of the screen, and an input data field 87 showing the next procedure number is displayed in the gaze area 80 .

[0090]

939 Hereinafter, the switching between the explanation display 83 and the input panel display 84 and the scrolling of the procedure display 82 performed when the operation procedure proceeds will be collectively referred to as "screen transition".

942 <Enlarged display in gaze area> As shown in FIGS. 10 to 12, when each input data column 87 is displayed in the gaze area 80, the range in the input data display area 74 is enlarged and displayed. At the same time, the characters representing the input data are displayed larger than the characters representing the input data in the other input data column 87 . This is because the display data processing unit 21 shown in FIG. This is achieved by performing processing for enlarging the font.

[0091]

951 By enlarging and displaying the input data in this manner, the ATM user with poor eyesight can easily read the input data, and the user's visual burden can be reduced.

953 Therefore, it is possible to reduce the possibility of erroneous data input and erroneous operation of the ATM. In addition, since the burden on the eyesight is reduced, it becomes possible to add elderly people or people with mild visual impairments such as amblyopia as users of ATMs, thereby expanding the range of users of ATMs.

[0092]

960 Also, since the characters displayed in the input data display area 74 of the gaze area 80 are displayed larger than the characters of the input data in the other input data fields 87, they

are emphasized more than the other input data.

963 Therefore, it is possible to easily distinguish between the characters in the other input data area 87, thereby improving the information recognition accuracy of the user. <Correction Button> As shown in FIG. 6, a correction button 101 is provided on the rightmost side of each of the plurality of input data fields 87, respectively. Each correction button 101 is a button for correcting data when an ATM user makes a mistake in data input. When any of the correction buttons 101 is pressed, characters indicating already-input data in the input data column 87 to which the correction button 101 belongs are cleared, and the user can enter new data.

[0093]

974 In this way, the correction button 101 is provided for each input data, and the correction button 101 is arranged next to the input data, so that the user can properly grasp the meaning of the correction button 101, When a user makes a mistake in data input, the correction button 101 can be found without hesitation.

978 In addition, it is possible to prevent data that does not require correction from disappearing due to the user pressing another correction button by mistake. In addition, it is possible to prevent the user from mistakenly recognizing the correction button 101 and pressing the cancel button 81b. Therefore, it is possible to improve the accuracy and speed of ATM operation by the user. <Confirmation Button> As shown in FIGS. 10 to 12, a first confirmation button 92 is provided at the lower right corner of each input panel display 84 (for example, 84a to 84c). When the first confirmation button 92 is pushed, a confirmation signal is given from the input device 2a to the interrupt processing section 23, and the interrupt processing section 23 gives a confirmation processing command to the display data processing section 21. FIG.

[0094]

991 Then, the display data processing unit 21 performs confirmation processing and changes the contents stored in the VRAM.

993 As a result, as shown in FIG. 14, the explanation display 83 and the input panel display 84 disappear from the transaction screen 70, and the procedure display 82 scrolls to the bottom of the screen to display the data that has been input so far. Become. By pressing one of the correction buttons 101 provided in each input data area 87, the user can correct the corresponding input data.

[0095]

1001 Furthermore, a rectangular confirmation display 104 is displayed below the procedure display 82 .

1003 The confirmation display 104 displays an instruction prompting confirmation of the input

data on its left side, and displays a second confirmation button 105 on its right side. Then, when the user of the ATM presses the second confirmation button 105, the operation procedure proceeds to the next assuming that the operation procedure has been completed.

[0096]

1010 In this way, since the procedure display 82 is used as a screen for confirming the input data, the ATM user can collectively confirm and correct the data that has been input up to now. Can understand relationships between input data.

1013 <Cancel Button> As shown in FIG. 6, a cancel button 81b is provided on the right side of the transaction type display field 81a. This cancel button 81b is a button for canceling the transaction (forcibly terminating the operation of the ATM). When the cancel button 81b is pushed, a reset signal is given to the interrupt processing section 23 from the input device 2a. Then, the interrupt processing section 23 gives a forced termination command to the display data processing section 21 based on the reset signal. As a result, the display data processing unit 21 forcibly terminates the transaction. After that, the display data processing unit 21 causes the display device 1 to display a transaction type selection screen (not shown).

[0097]

1025 In this way, the transaction type name and the cancel button 81b are arranged in the same column, so that the ATM user can properly understand the meaning of the characters "Cancel" displayed on the cancel button 81b. can.

1028 Therefore, it is possible to prevent the ATM user from accidentally pressing the cancel button 81b and wasting the operation that has been performed up to that point. <Return Button> In the conventional automated teller machine, the user could not see the data that had already been input before all the data to be input was input. In addition, even if the user wants to correct part of the data that has already been input, the conventional automated teller machine does not have a function to respond to the request. Therefore, if the user wants to repeat the operation procedure that has already been performed, the user has no choice but to press the "Cancel" button.

[0098]

1039 However, when the user presses the "Cancel" button, the operation procedure returns to the very beginning and the data that has already been input is erased.

1041 For this reason, the user had to redo the operation from the beginning. That is, for example, when the user notices an error in the data that has already been input, the user has no choice but to press the "cancel" button and redo the operation. I could be wrong.

[0099]

1047 In view of this problem, the ATM according to Embodiment 1 is provided with a return button 102 on the input panel display 84 as shown in FIGS.

1049 When the return button 102 is pushed, the ATM operating procedure returns to the previous operating procedure. For example, as shown in FIG. 15A, assume that the return button 102 is pressed when the operation procedure has progressed to procedure number "2" and the input data field 87b is displayed in the gaze area 80. FIG.

[0100]

1056 Then, the procedure display 82 scrolls to the lower side of the screen, and as shown in FIG. is displayed.

1058 At this time, the already input data is displayed in the input data display area 74 of the input data column 87a.

[0101]

1063 The functions described above are realized as follows.

1064 That is, data input in each operation procedure is held in a storage device (not shown) of the processing control device 20 shown in FIG. When the return button 102 is pressed, an interrupt signal is input to the interrupt processing section 23 from the input device 2a. The interrupt processing unit 23 gives the display data processing unit 21 a command (procedure return command) to return the operation procedure to the previous one according to the interrupt signal. The display data processing unit 21 returns the contents of the transaction screen 70 to the operation procedure one step before according to the procedure return command, reads the corresponding input data from the storage device (not shown), and causes the display device 1 to display it. The user's input data held in the storage device (not shown) is erased when the transaction (ATM operation) is completed.

[0102]

1077 Also, when the return button 102 is pressed, the explanation display 83 and the input panel display 84 are changed to those corresponding to the previous operation procedure.

1079 At this time, if the user presses the correction button 101, the already input data can be corrected using the changed input panel display 84. FIG. Further, when the return button 102 provided on the changed input panel display 84 is pressed, the operation procedure is further returned to the previous one. Therefore, the user can return the operation procedure to any of the operation procedures already performed.

[0103]

1087 Thus, according to the ATM of Embodiment 1, by providing the return button 102, the

operation procedure can be returned to the operation procedure that has already been performed.

1090 Also, when the operation procedure is returned, the already input data is displayed in the gaze area 80 . Therefore, it is possible to confirm and redo the operation procedure that has already been performed for each operation procedure. Therefore, it is possible to improve the operability of the ATM for the user, thereby avoiding erroneous operation and erroneous input by the user. In that data input can be redone, a sense of security can be given especially to users with low proficiency.

[0104]

1099 Also, the return button 102 is provided at the same position (upper right corner of the input panel display 84) regardless of the type of the input panel display 84. FIG.

1101 Therefore, the ATM user can memorize the position of the return button 102 without being particularly conscious of it. Therefore, the user can appropriately press the return button 102 when he/she wants to return the operation procedure to the procedure that has already been performed. <Help Display> FIG. 16 is an explanatory diagram of a help display (commentary screen) 106 displayed on the transaction screen 70. As shown in FIG. As shown in FIG. 16, the help display 106 indicates operations to be performed by the ATM user, and is superimposed on the input panel display 84 . The help display 106 is displayed on the display device 1 by the same process as the screen elements of the transaction screen 70 .

[0105]

1113 In FIG. 16, as an example of the help display 106, an image explaining the card slot is displayed.

1115 This help display 106 is displayed for a predetermined period of time when screen transition is completed, and disappears from the transaction screen 70 after the predetermined period of time has elapsed. Although not shown, the help display 106 is also provided with a character string. <Fast display button and polite explanation button> As shown in FIGS. 10 to 12 and 16, at the lower left corner of the input panel display 84, a quick display button 107 and a polite explanation button 108 are provided. When the fast display button 107 is pressed, each operation procedure is changed from the normal mode to the fast mode. That is, the number of times the help display 106 is displayed in each operation procedure is reduced, and screen transitions are performed at high speed. Note that the change to the high-speed mode is performed by turning ON the expert flag held in the control unit CPU.

[0106]

1128 On the other hand, when the polite explanation button 108 is pressed, each operation procedure is changed from the normal mode to the detailed mode.

1130 That is, the screen transitions are displayed at a lower speed than in the normal mode, and the number and types of help displays 106 displayed in each operation procedure increase. Further, a character string of detailed explanation about the operation is appropriately displayed on the transaction screen 70 .

[0107]

1137 If the fast display button 107 is pressed in the fast mode, the fast mode returns to the normal mode.

1139 Further, when the high speed display button 107 is pressed in the detailed mode, the detailed mode is changed to the high speed mode. On the other hand, when the detailed display button 108 is pressed in the detailed mode, the detailed mode returns to the normal mode. Further, when the polite display button 108 is pressed in the high speed mode, the high speed mode is changed to the detailed mode.

[0108]

1147 Since the quick display button 107 and the polite explanation button 108 are provided in this way, the user can operate the ATM by selecting a mode according to the user's level of proficiency.

1150 The operation time can be shortened by operating in the high speed mode. Further, by performing operations in the detailed mode, operations can be performed reliably and accurately, and the occurrence of operation errors and data input errors can be avoided. [ATM Operation Procedure] FIG. 17 is a conceptual diagram of the above-described ATM operation procedure, and FIG. 18 is a diagram showing an example of the ATM operation procedure. As shown in FIG. 17, the ATM according to Embodiment 1 has a multi-layered operation procedure for each transaction. Specifically, the operating procedure consists of a main procedure layer (shortest sequence), a selection procedure layer (subsequence), and a detailed procedure layer (subsequence).

[0109]

1162 The main procedure layer consists of the shortest procedures (the minimum necessary procedures).

1164 The selection procedure layer consists of procedures that are added to the operating procedures by user selection. The detailed procedure layer consists of a plurality of procedures that further detail each procedure in the selection procedure layer, and is added to the operation procedure by user's selection. In this way, the operating procedures are multi-layered, and it is up to the user to decide whether or not to add the procedures belonging to the selected procedure layer and the detailed procedure layer to the operating procedures. ATM operations (transactions) can be performed according to appropriate procedures.

[0110]

1175 FIG. 18 shows the operating procedure for a "transfer" transaction.

1176 This operation procedure is provided to the user by causing the display 1 to display the transaction screen 70 generated by the screen generation process by the control unit CPU. In FIG. 18, if the user has a bank transfer card, the procedure for "input of transfer destination" (see FIG. 18) can be omitted because the contents of the bank transfer card are recorded.

[0111]

1184 This procedure of "entering the payee" consists of three procedures of "selecting a financial institution", "entering a branch name", and "entering an account number" of the payee.

1186 By the way, the procedure of "entering the transfer destination" can be processed as one procedure by a user accustomed to the transaction of "transfer".

[0112]

1191 Therefore, on the transaction screen 70 of the display device 1, the omitted procedures ("select financial institution", "input branch name" and "input account number") are displayed by the control unit CPU, and once As a procedure that can be processed, the procedure of "input of transfer destination" is displayed.

1195 Further, it is displayed that one of the procedure to be omitted and the procedure of "input bank transfer" is to be selected.

[0113]

1200 Here, if the procedure of "input bank transfer" is selected, after the user performs the operation in the "input bank transfer" procedure, the operation procedure should proceed to the next step "input transfer money". becomes.

1203 On the other hand, if the skipped procedure is selected, the user must go through the steps of "selecting a financial institution", "entering a branch name" and "entering an account number" (see Figure 18). , the operation procedure will proceed to the next "transfer money input".

[0114]

1210 Also, when the procedure of "Select financial institution" is completed, the next procedure will be instructed to select whether to perform the next procedure by the procedure of "Enter branch name" or "Enter initials of branch name" and "Select branch name". It is displayed on the display device 1 by the processing of the control unit CPU.

1214 On the other hand, the user selects one of them and proceeds with the operation procedure.

[0115]

1218 In this way, a complicated procedure consisting of multiple operations can be processed as multiple simple procedures.

1220 Therefore, it is possible to provide users with high proficiency with the shortest procedure, and users with low proficiency with detailed procedures to operate the ATM.

[0116]

1225 In addition, a help display 106 (see FIG. 18) of "explanation" indicating the meaning of operations and input objects in the procedure is prepared in association with each procedure. It is displayed on the display device 1 together with a procedure selection instruction.

1229 This allows the user to select procedures carefully and properly.

[0117]

1233 As described above, according to the ATM according to the first embodiment, the user of the ATM can operate the ATM according to the operation procedure according to his or her level of proficiency in operation, thereby improving the operability of the ATM.

1236 [Embodiment 2] Next, an automatic teller machine (ATM) according to Embodiment 2 will be described. However, since the ATM according to the second embodiment is substantially the same as the ATM according to the first embodiment, only different points will be explained.

[0118]

1243 FIG. 19 is an explanatory diagram showing part of a transaction screen 70 displayed on the ATM display device 1 according to the second embodiment.

1245 In addition, the same code|symbol is attached|subjected about the component same as the component in Embodiment 1. FIG. In FIG. 19, explanation display 183 and input panel display 184 are displayed above background 81 and procedure display 82 . The explanation display 183 is translucent except for the character string indicating the operation explanation. The input panel display 84 is translucent except for the Japanese syllabary key group 94 .

[0119]

1254 Therefore, the ATM user can see the display contents of the procedure display 82 behind them through the translucent explanation display 183 and the input panel display 184 .

1256 Therefore, it is possible to confirm the input result already displayed in each input data column 87 and to recognize the whole image of the input object to be input.

[0120]

1261 According to the second embodiment, the ATM user can see the display contents of the procedure display 82 through the explanation display 183 and the input panel display 184 .

1264 Therefore, the user can more properly grasp the display contents of the procedure display 82 as compared with the first embodiment. Further, by making the explanation display 183 and the input panel display 184 translucent, it becomes possible to display information that could not fit on one screen in the past, on one screen. It can be displayed on one screen. Therefore, the operating procedure can be shortened.

[0121]

1272 In the second embodiment, the description display 183 and the input panel display 184 are configured to be translucent. good.

1274 [Embodiment 3] Next, an ATM according to Embodiment 3 will be described. Since the ATM according to Embodiment 3 is substantially the same as the ATM according to Embodiment 1, the description of the common points will be omitted and the differences will be described.

[0122]

1281 FIG. 20 is a block diagram showing the configuration of an ATM according to Embodiment 3;

1282 However, the same reference numerals are given to the same components as in the first embodiment, and the description thereof is omitted. The control unit CPU has a timer A and a timer B for measuring time in addition to the configuration described in the first embodiment. The control unit CPU performs a process of determining a user's level of proficiency in ATM operation (familiarity level determination process).

[0123]

1290 The proficiency level determination process is performed by measuring the speed of data input by the user.

1292 For example, when a user inputs numbers (personal identification number, account number, etc.), the proficiency level is determined based on the time required for the user to input a four-digit number. Alternatively, the degree of proficiency is determined based on the time from the input of an arbitrary number to the pressing of a correction key for correcting the input of the number (proficiency level determination processing based on input of numbers).

[0124]

1301 In the case of inputting Japanese syllabary characters (recipient, client, etc.), the proficiency level is determined based on the character input time interval.

1303 Alternatively, the proficiency level is determined based on the time from the input of an arbitrary character until the correction key for correcting the character input is pressed (proficiency level determination processing by character input).

[0125]

1309 Also, the proficiency level determination process is performed by measuring the user's level of knowledge of financial terms.

1311 For example, the proficiency level is determined based on the time from when a specific financial term is displayed on the display device 1 to when any key on the input panel display 84 is pressed. Specific financial terms include, for example, financial terms such as "ordinary", "current account", "transfer card", "cash transfer", and "account transfer" (term proficiency level determination processing).

[0126]

1319 FIG. 21 is a flowchart showing proficiency level determination processing by the control unit CPU according to the third embodiment.

1321 In FIG. 21, the proficiency level determination process is started when the control unit CPU displays a transaction screen 70 on the display device 1 of the ATM. However, here, it is assumed that the above-described numerical input is used for determination processing, and as the transaction screen 70, a personal identification number input screen (not shown) (transaction screen 70 displayed in the operation procedure for inputting a personal identification number) is displayed on the display device 1. shall be displayed on

[0127]

1330 In step S101, the control unit CPU stops and resets (clears) the timers A and B, and then advances the process to step S102.

1332 In step S102, the control unit CPU waits until any one of the numeric keys displayed on the password input screen (not shown) is pressed. After that, when the control unit CPU determines that any one of the numeric keys has been pressed (step S012; YES), the process proceeds to step S103. When the process proceeds to step S103, the control unit CPU stops the timer B and then advances the process to step S104.

[0128]

1340 In step S104, the control unit CPU determines whether or not the first digit of the four-digit personal identification number has been input with the key pressed in step S102.

1342 At this time, if the control unit CPU determines that the first digit number has been input (step S104; YES), the process proceeds to step S105, and the timer A starts counting time. After that, the control unit CPU returns the process to step S102 and waits for the numeric keypad displayed on the personal identification number input screen (not shown) to be pressed again. On the other hand, if the control unit CPU determines that the first digit number has not been input (step S104; NO), the process proceeds to step S106.

[0129]

1351 When the process proceeds to step S106, the control unit CPU determines whether or not the fourth digit of the four-digit personal identification number has been input with the key pressed in step S102.

1354 At this time, if the control unit CPU determines that the fourth digit number has been input (step S106; YES), the process proceeds to step S111. On the other hand, if the control unit CPU determines that the fourth digit number has not been input (step S106; NO), the process proceeds to step S107.

[0130]

1361 When proceeding to step S107, the control unit CPU determines whether or not the correction key displayed on the password input screen (not shown) has been pressed.

1363 At this time, if the control unit CPU determines that the correction key has not been pressed (step S107; NO), the process proceeds to step S108, and the timer B starts counting time. After that, the control unit CPU returns the process to step S102 and waits for the numeric keypad displayed on the personal identification number input screen (not shown) to be pressed again. On the other hand, if the control unit CPU determines that the correction key has been pressed (step S107; YES), the process proceeds to step S109.

[0131]

1372 When the process proceeds to step S109, the control unit CPU refers to the time counted by the timer B stopped in step S103 (time from inputting a certain number to noticing an error and pressing a correction key). , determines whether or not the measured time is equal to or less than a specified value.

1376 At this time, if the control unit CPU determines that it is not equal to or less than the prescribed value (step 109; NO), the process proceeds to step S108. On the other hand, when the control unit CPU determines that it is equal to or less than the prescribed value (step S109; YES), the process proceeds to step S110.

[0132]

1383 When proceeding to step S110, the control unit CPU assumes that the user is an expert in operation and turns on the expert flag described in the first embodiment.

1385 After that, the control unit CPU advances the process to step S108. On the other hand, the control unit CPU makes a determination of YES in step S106, and when the process proceeds to step 111, the timer A stops counting time. After that, the control unit CPU advances the process to step S112.

[0133]

1392 In step S112, the control unit CPU refers to the time measured by the timer A stopped in step S111 (the time required to enter the 4-digit personal identification number), and determines whether or not the time is equal to or less than a specified value. judge.

1395 At this time, if the control unit CPU determines that the value is not equal to or less than the specified value (step 109; NO), it terminates the proficiency level determination process. On the other hand, if the control unit CPU determines that it is equal to or less than the specified value (step S109; YES), the process proceeds to step S113.

[0134]

1402 When the process proceeds to step S113, the control unit CPU assumes that the user is an expert in operation and turns on the expert flag described in the first embodiment.

1404 After that, the control unit CPU terminates the proficiency level determination process. When this proficiency level determination process ends, the control unit CPU (central processing unit 3) starts processing for displaying the next transaction screen 70 on the display device 1. FIG.

[0135]

1411 By turning on the expert flag, as described in the first embodiment, the same state as when the quick display button 107 is pressed, i.e., the screen transition is performed at high speed, and the help display 106 is displayed the number of times. is reduced.

[0136]

1417 Further, the proficiency level determination processing by character input is realized by the same processing as the flowchart shown in FIG.

1419 However, in the proficiency level determination process by character input, the process starts when the transaction screen 70 including the input panel display 84c of Japanese syllabary is displayed on the display device 1. FIG.

1422 Timer A counts the time until four characters of certain character data are input. Timer B counts the time from when the user enters arbitrary character data until he notices an error

and presses the correction key 101 . The prescribed values used in each of the processes in steps S109 and S112 are set to values different from those in the proficiency level determination process based on numerical input.

[0137]

1430 FIG. 22 is a flowchart showing proficiency level determination processing using terms.

1431 This determination process is started by the display of a transaction screen 70 including an input panel display 84 on which keys for inputting specific terms are displayed on the display device.

[0138]

1437 When the process starts, the control unit CPU stops and resets (clears) the timer A (step S201), and then starts the timer A to measure time (step S202).

1439 Subsequently, the control unit CPU determines whether or not a key for inputting a specific term has been pressed (step S203). At this time, if the control unit CPU determines that the corresponding key has been pressed (step S203; YES), the process proceeds to step S204. On the other hand, if it is determined that the corresponding key has not been pressed (step S203; NO), the process of step S203 is repeated until YES is determined in step S203.

[0139]

1447 The control unit CPU stops the time measurement by the timer A when proceeding to step S204.

1449 Subsequently, the control unit CPU refers to the measured time of the timer A and determines whether or not the measured time is equal to or less than a specified value. At this time, if the control unit CPU determines that it is not equal to or less than the specified value (step 205; NO), it terminates this determination process. On the other hand, if the control unit CPU determines that it is equal to or less than the specified value (step S205; YES), the process proceeds to step S206.

[0140]

1458 When the process proceeds to step S206, the control unit CPU assumes that the user is an expert in operation and turns on the expert flag described in the first embodiment.

1460 After that, the control unit CPU terminates this determination process.

[0141]

1464 The effect of the third embodiment is almost the same as the effect of the first embodiment.

1465 However, the proficiency level of the ATM user's operation is determined, and if the

proficiency level is high, the operating procedure is omitted. Therefore, a user with high proficiency can operate the ATM according to a simplified operating procedure, and a user with low proficiency can operate the ATM according to a detailed operating procedure. That is, according to the third embodiment, it is possible to automatically provide an operation procedure according to the proficiency level of the user. Therefore, many users can comfortably operate the ATM.

[0142]

1475 Each specified value used in each proficiency level determination process described above can be set as appropriate.

1477 Therefore, it is possible to absorb the difference in operating proficiency due to regional differences. For example, near a terminal station in an urban area, there are many users who are skilled in operating ATMs, so each specified value is set in a shorter time than in a local area. On the other hand, in local areas, there are fewer users skilled in ATM operation than in urban areas, so each prescribed value is set with a longer time than in urban areas. [Embodiment 4] Next, an ATM according to Embodiment 4 will be described. A conventional automatic transaction device defines a timeout period for canceling the entire transaction process if there is no input for a predetermined period of time after screen transition. An alarm was sounded before (for example, 5 seconds ago) to prompt for input. If there is no input after that, the automatic transaction device forcibly terminates the transaction at the same time as the time-out period is reached.

[0143]

1491 Such a handling method is effective when the user stops operating the automatic teller machine halfway and is absent, or when the user intentionally executes forced termination due to timeout.

1494 However, in some cases, such as when the user cannot understand what to do and cannot make an input, the prompting alarm only confuses the user. In this case, the user may be dissatisfied with being unable to do what he/she can do because he was panicked by the prompting alarm, or he/she may feel that he/she is being used by the machine.

[0144]

1501 The ATM according to Embodiment 4 is designed in view of the above problems.

1502 However, since the ATM according to the fourth embodiment has substantially the same configuration as the ATM according to the first embodiment, the description of the common points will be omitted and the differences will be described. FIG. 23 is a flowchart showing processing (timeout processing) by the control unit CPU in the fourth embodiment.

[0145]

1509 This timeout process starts when the screen transition of the transaction screen 70 is completed.

1511 First, the control unit CPU activates an input monitoring timer (not shown) held by itself (step S301). Subsequently, the control unit CPU determines whether or not there is a key input from the input device 2a (step S302). At this time, if the control unit CPU determines that there is a key input (step S302; YES), it ends the timeout process and starts the next process. On the other hand, if the control unit CPU determines that there is no key input (step S302; NO), the process proceeds to step S303.

[0146]

1520 When the control unit CPU proceeds to step S303, an input monitoring timer (not shown) counts a preset time-out period, and determines whether or not a time-out has occurred.

1522 At this time, if the control unit CPU determines that a timeout has occurred (step S303; YES), it forcibly terminates the transaction and ends this timeout process. On the other hand, when the control unit CPU determines that a timeout has not occurred (step S303; NO), the process proceeds to step S304.

[0147]

1529 When the process proceeds to step S304, the control unit CPU determines whether or not 10 seconds have elapsed since starting an input monitoring timer (not shown).

1531 At this time, if the control unit CPU determines that 10 seconds have not passed (step S304; YES), it gives an operation command to the audio output unit 60 (see FIG. 3) to generate a warning sound (step S305). After that, the control unit CPU returns the process to step S302. On the other hand, if the control unit CPU determines that 10 seconds have passed (step S304; NO), the process proceeds to step S306.

[0148]

1539 When the process proceeds to step S306, the control unit CPU determines whether or not 15 seconds have passed since the input monitoring timer (not shown) was activated.

1541 At this time, if the control unit CPU determines that 15 seconds have not elapsed (step S306; YES), the help display 106 is displayed on the transaction screen 70 of the display device 1 (step S307). After that, the control unit CPU returns the process to step S302. On the other hand, if the control unit CPU determines that 15 seconds have passed (step S306; NO), the process proceeds to step S308.

[0149]

1549 When the process proceeds to step S308, the control unit CPU determines whether or not 20

seconds have elapsed since starting an input monitoring timer (not shown).

1551 At this time, if the control unit CPU determines that 20 seconds have not elapsed (step S308; YES), the process proceeds to step S311. On the other hand, if the control unit CPU determines that 20 seconds have passed (step S308; NO), the process proceeds to step S309.

[0150]

1558 When proceeding to step S309, the control unit CPU determines whether or not it is 5 seconds before the input monitoring timer (not shown) counts the timeout time.

1560 At this time, if the control unit CPU determines that it is 5 seconds before (step S309; YES), it gives an operation command to the audio output unit 60 to generate a warning alarm. After that, the control unit CPU returns the process to step S302. On the other hand, if the control unit CPU determines that it is not 5 seconds before (step S308; NO), the process returns to step S302.

[0151]

1568 On the other hand, when proceeding to processing step S311, the control unit CPU displays a timeout notice (for example, a character string such as "Time will expire in a few seconds and the transaction will be forcibly terminated") on the transaction screen 70 of the display device 1. In addition to displaying it, the voice output unit 60 is caused to output voice guidance to the effect that a time-out will occur.

1573 Subsequently, the control unit CPU activates a suspend button (not shown) (a button for extending the timeout period) and an instruction display (not shown) (for example, characters such as "Press the suspend button if you want to continue trading"). column) is displayed on the transaction screen 70.

[0152]

1580 Thereafter, the control unit CPU enters a state of accepting input from the suspend button (not shown) for a predetermined time, and after the predetermined time has elapsed, determines whether or not the suspend button (not shown) has been pressed (step S313).

1583 At this time, if the control unit CPU determines that the suspend button (not shown) has not been pressed (step S313; NO), the process proceeds to step S309. On the other hand, if the control unit CPU determines that the suspend button (not shown) has been pressed (step S313; YES), the process returns to step S304. As a result, the control unit CPU jumps to the process of step S303, and the time-out period is extended until the next process of step S303 is performed.

[0153]

1592 According to the ATM according to the fourth embodiment, when data is not input to the input device 2a after the screen transition is performed, the ATM generates a warning sound as the first step, and displays the display device as the second step. In step 1, an operation method explanation display (help display 106) is displayed, in the third step, a timeout warning is displayed and voice guidance is given, and in the fourth step, a timeout warning alarm is generated.

1598 In this manner, time-out information is provided to the ATM user in stages, so that the user can operate the ATM without feeling any psychological pressure.

[0154]

1603 Further, by displaying the help display 106, the user who lacks operational knowledge can be relieved, so that the possibility of the transaction being forcibly terminated due to timeout can be reduced.

1606 Furthermore, a suspend button (not shown) is provided, and pressing this button extends the time until timeout, so that it is possible to give the user time to try to understand the operation method of the ATM. Therefore, it is possible to give satisfaction to the user as compared with the conventional automatic teller machine which inevitably terminates when the timeout time comes. [Embodiment 5] Next, an ATM according to Embodiment 5 will be described. In the conventional automated teller machine, there was no warning sound such as a signal sound when the transaction screen was switched. may not notice, and transactions may take time.

[0155]

1617 In view of this, conventional automated teller machines display characters on the transaction screen in large size or blink the characters in order to notify the user that the transaction screen has been switched and that data can be entered. However, if the user does not pay attention to the display device, the user will miss these signals, which is not sufficient.

[0156]

1624 The ATM according to Embodiment 5 has been made in view of the problems described above.

1626 Since the ATM according to the fifth embodiment is substantially the same as the ATM according to the first embodiment, the description of common points will be omitted, and differences will be described.

1629 FIG. 24 is a flow chart showing processing (attention calling processing) by the control unit CPU of the ATM according to the fifth embodiment.

[0157]

1634 This alerting process starts when any one of the operating procedures ends (step S401).

1635 When the control unit CPU advances the process to step S402, the transaction screen 70 is rewritten. That is, internal processing (screen display processing: see FIG. 4) for displaying the screen transition described in the first embodiment on the display device 1 is performed.

[0158]

1642 Subsequently, the control unit CPU transfers the data (video signal) of the transaction screen 70 to the display device 1, and displays the transaction screen 70 in the next operation procedure (step S403).

1645 When the transaction screen 70 is displayed on the display device 1 by the process of step S403, the control unit CPU gives an operation command to the voice output unit 60 to generate a signal sound (step S404). Then, the control unit CPU becomes in a state in which the user can input data, that is, in a state of waiting for a signal from the input device 2a (step S405).

[0159]

1653 According to the ATM according to the fifth embodiment, since a signal sound is generated when the transaction screen 70 is changed, the user can be made to pay attention to the transaction screen 70 .

1656 In addition, since the data input is made possible following the generation of the signal sound, the user can start data input to the ATM upon the generation of the signal sound. Therefore, it is possible to shorten the operation time of the ATM by the user, which in turn contributes to the improvement of the operation rate of the customer in the financial institution. [Embodiment 6] Next, an ATM according to Embodiment 6 will be described. Since the ATM according to Embodiment 6 is substantially the same as the ATM according to Embodiment 1, common points will be omitted and only differences will be described.

[0160]

1666 FIG. 25 is a flow chart showing a finger drag determination process in the customer operation unit UOP.

1668 This determination process starts when the transaction screen 70 is displayed on the display device 1 and data can be input.

[0161]

1673 In step S501, it is determined whether or not an object has been detected in contact with the touch panel of the input device 2a.

1675 At this time, if an object is detected (step S501; YES), the process proceeds to step S502. On

the other hand, if no object is detected (step S501; NO), the process of step S501 is repeated until YES is determined in step S501.

[0162]

1681 When the process proceeds to step S502, the object detected in step S501 remains detected, and the contact position coordinates between the object and the touch panel are the contact position detected in step S501. It is determined whether or not it differs from the coordinates.

1685 At this time, if the object is still detected and the contact position coordinates are different (step S502; YES), it is assumed that the finger is being dragged, and a signal to that effect is transferred to the control unit CPU. (step S503), and this determination process ends.

[0163]

1691 On the other hand, if the object is not in the state of being detected, or if the contact position coordinates do not differ (step S502; NO), then either key or button on the input panel display 84 is normally pressed. Then, a signal to that effect is transferred to the control unit CPU (step S504).

1695 Then, this determination processing ends.

[0164]

1699 FIG. 26 is a flow chart showing a drag warning sound generating process by the control unit CPU.

1701 This process starts when the transaction screen 70 is displayed on the display device 1 and data can be input.

[0165]

1706 First, the control unit CPU waits for key input (step S505), and determines whether or not there is key input (step S506).

1708 That is, it is determined whether or not a signal has been transferred from the input device 2a. At this time, if it is determined that the signal has been transferred from the input device 2a, the control unit CPU advances the process to step S507.

[0166]

1714 When proceeding to step S507, the control unit CPU determines whether or not the signal transferred from the input device 2a is a signal indicating a finger dragging action.

1716 At this time, if the control unit CPU determines that the signal does not indicate a drag motion, the process proceeds to step S508, performs other processes, and terminates the

drag warning sound generation process. On the other hand, if it is determined that the signal indicates a dragging motion, the control unit advances the process to step S509.

[0167]

1723 When the process proceeds to step S509, the control unit CPU gives an operation signal to the audio output unit 60 to generate a signal sound indicating a warning.

1725 Subsequently, the control unit CPU outputs to the display device 1, for example, "You are dragging your finger. A window containing the character string "Please move away from the screen" is displayed (step S510). After that, the control unit CPU returns the process to step S506.

[0168]

1732 According to the sixth embodiment, when a finger dragging action is performed, a signal sound is emitted, so that the user pays attention to the display device 1 .

1734 Then, the display device 1 displays a warning message about dragging the finger, so the user can check whether there is an error in the input data. will be corrected. For this reason, it is possible to prevent data input errors and erroneous operations of the device due to finger dragging. [Embodiment 7] Next, an ATM according to Embodiment 7 will be described. In a conventional automatic transaction device, each of a plurality of transaction screens is created individually according to the operation details required for transaction. Moreover, the display order of a plurality of transaction screens is determined by a processor device mounted on the automatic transaction device according to a sequence defined by a control program. Therefore, if you want to change the display order of multiple transaction screens, you have to modify the program. In addition, when the input object to be input to the automated teller machine is changed, it is necessary to change the data of the transaction screen as well as the program.

[0169]

1749 However, since control programs and transaction screen data for automated teller machines are usually stored in hard disks, it takes time and is extremely difficult to change them.

1751 Embodiment 7 has been made in view of the above-described problems.

[0170]

1755 FIG. 27 is a block diagram showing the central processing unit 3 (control unit CPU) of the ATM according to the seventh embodiment.

1757 However, since the ATM according to the fourth embodiment is substantially the same as the ATM according to the first embodiment, the same constituent elements are given the same reference numerals and explanations thereof are omitted, and only the points of difference

are explained. In FIG. 27, the central processing unit 3 has a hard disk 24 . A screen creation table 25 is held in the hard disk 24 .

[0171]

1765 FIG. 28 is an explanatory diagram of the screen creation table 25. As shown in FIG.

1766 28, the screen creation table 25 contains a plurality of output data (data defined in the control program recorded in the HD 10 shown in FIG. 3 and used for displaying the transaction screen 70 on the display device 1). data), an explanation display 83, and an input panel display 84 corresponding to each are stored. This screen creation table 25 is created by paying attention to the fact that the explanation display 83 and the input panel display 84 among the screen elements of the transaction screen 70 can be specified in a 1:1 relationship with respect to the input object. is. Also, the background 81 is uniquely determined by selecting the transaction type, so it is held as fixed data.

[0172]

1777 FIG. 29 is a flow chart showing processing by the processing control device 20 shown in FIG.

1778 In FIG. 29, among the processes of steps S601 to S609, the processes of steps S601 to S604 and the processes of steps S606 to S609 are the same as the processes of steps S01 to S04 and steps S06 to S09 shown in FIG. Therefore, the description is omitted, and step S605 will be described.

[0173]

1785 When the process proceeds to step S605, the subroutine of the screen creation process by the display data processing unit 21 is started.

1787 FIG. 30 is a flowchart showing screen creation processing. When the screen creation process starts, the display data processing unit 21 first receives the texture data of the background 81 corresponding to the transaction type from the image data holding unit 7 (step S701). Subsequently, the display data processing unit 81 receives the texture data of the procedure display 82 corresponding to the transaction type from the image data holding unit 7 (step S702).

[0174]

1796 Subsequently, the display data processing unit 21 searches the screen creation table 25 based on the output data defined in the control program, and identifies the corresponding input target (step S703).

1799 Subsequently, the display data processing unit 21 identifies the explanation display 83 corresponding to the input object identified in step S703, and reads the texture data of the corresponding explanation display 83 from the image data holding unit 7 (step S704).

[0175]

1805 Subsequently, the display data processing unit 21 identifies the input panel display 84 corresponding to the input target identified in step S703, and reads the texture data of the corresponding input panel display 84 from the image data holding unit 7 (step S705). .

1808 The display data processing unit 21 then receives necessary character data from the CG unit 6 . Then, the screen creation process ends, and the process proceeds to step S606 in the main routine.

[0176]

1814 According to the ATM according to Embodiment 7, the transaction screen 70 is created based on the contents stored in the screen creation table 25. Therefore, if the contents stored in the screen creation table 25 are changed, the display contents of the transaction screen 70 and the transaction screen 70 can be changed. You can change the display order of

1819 Therefore, there is no need to change the content of the control program recorded on the HD 10. FIG.

[0177]

1824 EFFECTS OF THE INVENTION According to the automated teller machine according to the present invention, operability can be improved as compared with the conventional one, regardless of the user's proficiency level of operation.

[0178]

1830 Brief description of the drawing

[0179]

1834 Figure 1 Block diagram showing main parts of ATM

[0180]

1838 Figure 2 ATM external configuration diagram

[0181]

1842 Block diagram showing the specific configuration of Figure 3 ATM

[0182]

1846 FIG. 4 Flowchart showing processing by control unit

[0183]

1850 Fig. 5 Explanatory diagram of transaction screen

[0184]

1854 Figure 6 Explanatory diagram of the screen elements of the transaction screen

[0185]

1858 Fig. 7 Explanatory diagram of procedure display

[0186]

1862 Figure 8 Explanatory diagram of procedure display

[0187]

1866 Fig. 9 Explanatory diagram of procedure display

[0188]

1870 Fig. 10 Explanatory diagram of input panel display

[0189]

1874 Fig. 11 Explanatory diagram of input panel display

[0190]

1878 Fig. 12 Explanatory diagram of input panel display

[0191]

1882 Fig. 13 Explanatory diagram of input panel display

[0192]

1886 Fig. 14 Explanatory diagram of confirmation screen

[0193]

1890 Figure 15 Explanatory diagram of return button

[0194]

1894 Figure 16 Explanatory diagram of help display

[0195]

1898 Figure 17 Conceptual diagram of operation procedure

[0196]

1902 Figure 18 Diagram showing an example of operation procedure

[0197]

1906 FIG. 19 Explanatory diagram of transaction screen according to Embodiment 2

[0198]

1910 Block diagram showing the configuration of the ATM according to FIG. 20 Embodiment 3

[0199]

1914 FIG. 21 Flowchart showing proficiency level determination processing

[0200]

1918 FIG. 22 Flowchart showing proficiency level determination processing

[0201]

1922 FIG. 23 Flowchart showing timeout processing

[0202]

1926 FIG. 24 Flowchart showing alerting process

[0203]

1930 FIG. 25 Flowchart showing drag determination processing

[0204]

1934 FIG. 26 Flowchart showing drag warning sound generation processing

[0205]

1938 Figure 27 Block diagram of ATM according to Embodiment 7

[0206]

1942 Fig. 28 Explanatory diagram of screen creation table

[0207]

1946 FIG. 29 Flowchart showing screen creation processing

[0208]

1950 Flowchart showing FIG. 30 screen creation processing

[0209]

1954 FIG. 31 Explanatory diagram of conventional technology

[0210]

1958 FIG. 32 Explanatory diagram of conventional technology

[0211]

1962 Fig. 33 Explanatory diagram of conventional technology

[0212]

1966 Code explanation

[0213]

1970 A, B Timer CPU Control device 1 Display device 2a Input device 3 Central processing unit 6 CG unit 7 Image data holding unit 8 ROM 9 RAM 20 Processing control unit 21 Display data processing unit 22 Display control unit 23 Interrupt processing unit 24 EEPROM 25 Screen creation table 70 Transaction screen 71 Transaction type display area 72 Operation explanation area 73 Input object display area 74 Input data display area 75 Operation area 80 Attention area 81 Background 81a Transaction type display column 81b Cancel button 82 Procedure display 83, 183 Explanation display 84, 184 Input panel Display 87 Input data column 92 First confirmation button 101 Correction button 102 Back button 105 Second confirmation button 106 Help display 107 Quick display button 108 Detailed explanation button

Patent Translate
Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

CLAIMS JPH1125320A

1.

13 a display device for displaying information; an input device for inputting information relating to transactions; and a controller for controlling information display on the display device and based on information input from the input device according to the information displayed on the display device. and a control unit configured to perform transaction processing by arranging a plurality of input item fields in which a plurality of items of information input from the input device are displayed on the display device in order of input. and, when each of the plurality of information is input from the input device in accordance with the input order, an operation screen corresponding to each information is displayed in a state superimposed on the procedure display. An automatic transaction device characterized by

2.

25 The automated teller machine according to claim 1, wherein said procedure display is always displayed on said display device.

3.

30 a display device for displaying information; an input device for inputting information relating to transactions; and a controller for controlling information display on the display device and based on information input from the input device according to the information displayed on the display device. a specific area is set on the screen of the display device, and the control unit displays a plurality of information items input from the input device to the display device a plurality of input item fields each indicated with are arranged in order of input, and the procedure display is displayed substantially orthogonal to the longitudinal direction of each of the input item fields in accordance with the progress of the operation procedure of the

transaction. An automated teller machine characterized by displaying an input item column corresponding to an operation currently being performed among the plurality of input item columns in the specific area by moving in a direction.

4.

44 The operation screen is arranged below the specific area, an explanation display showing an explanation of the operation screen is arranged above the specific area, and a transaction type display showing a transaction type above the explanation display. 3. The automated teller machine according to claim 2, wherein columns are arranged.

5.

51 An input information display area for displaying information corresponding to the input item is formed in each of the input item fields, and the control unit includes holding means for holding information input from the input device. returning the display contents of the display device to the state at the time of inputting the information held in the holding means in response to a request from the user, reading the corresponding information from the holding means and displaying it in the input information display area. 3. The automatic transaction device according to claim 2, characterized by:

6.

61 In response to a request from a user, the control unit excludes an operation screen in a range overlapping at least the procedure display from the display contents of the display, and displays the information held by the holding means as input information in the corresponding input item column. 6. The automated teller machine according to claim 5, wherein the information is displayed in an area.

7.

69 2. The automated teller machine according to claim 1, wherein said control unit changes the speed of changing the display contents of said display device according to a request from a user.

8.

75 The control unit has information presenting means for displaying operation information related to the input of information on the display device when information is input from the input device, and the operation information is displayed on the display device by the information presenting means. 2. The automated teller machine according to claim 1, wherein the number of times the is displayed is changed according to a request from the user.

9.

83 When displaying the procedure display on the display device, the control unit fixes the number of input item columns constituting the procedure display and the threshold value for determining whether to display the procedure display fixedly. 3. The automatic teller machine according to claim 2, wherein the procedure display is fixedly displayed on the display device when the number of input item fields is less than a fixed threshold value by comparing with a threshold value.

10.

92 The method according to claim 3, wherein said control unit enlarges and displays an input information display area of an input item column displayed in said specific area and information displayed in this input information display area. Automatic trading device.

11.

98 10. The automated teller machine according to claim 1, wherein a part of said operation screen is displayed translucently.

12.

103 10. The automated teller machine according to claim 4, wherein said transaction type display field is provided with a cancel button for forcibly terminating processing related to the transaction.

13.

109 10. The automated teller machine according to claim 5, wherein an input information display area in each of said plurality of input item fields is provided with a button for correcting information displayed in the input information display area. .

14.

115 10. When all the information in the transaction is input, the control unit causes the display to display the procedure display as a confirmation screen for each input information, and displays the input information corresponding to each of the all information. 6. The automated teller machine according to claim 5, wherein the information is displayed in an area.

15.

123 10. A plurality of input item fields are divided into a plurality of operation sets according to attributes of information input from the input device, and the operation sets are displayed in different colors. 3. The automatic transaction device according to 3.

16.

129 The automated teller machine according to claim 15, wherein a plurality of input item fields constituting said operation set are color-coded in a state of drawing a gradation according to the order of information input.

17.

135 16. The automated teller machine according to claim 15, wherein the background color of the screen forming the display contents of said display device changes according to the color of the input item column displayed in said specific area.

18.

141] The control unit detects an input time, which is the time required for a user to input specific information, and compares the detected input time with a proficiency level threshold, which is a threshold for judging the user's proficiency level of operation. 2. The automated teller machine according to claim 1, wherein, in contrast, when said input time is equal to or less than said proficiency level threshold, the change speed of the display contents of said display device is increased.

19.

150 10. The control unit has information presenting means for displaying operation information related to the input of information on the display device when information is input from the input device, and the input time is equal to or less than the proficiency level threshold. 19. The automated teller machine according to claim 18, wherein the number of times the operation information is displayed on the display device by the information presenting means is reduced.

20.

159 10. A display device for displaying information; an input device for inputting information relating to transactions; and a control unit for performing transaction processing based on the user, wherein the control unit selects either one of one procedure consisting of a plurality of operations and a plurality of procedures corresponding to the plurality of operations included in the one procedure. An automatic transaction device characterized by providing in

response to a request from.

21.

168 The automatic transaction according to claim 1 or 20, wherein said control unit causes said display device to display a caution display for prompting the input of information when there is no information input from said input device for a predetermined time. Device.

22.

174 21. The automated teller machine according to claim 1 or 20, wherein said control unit causes said display device to display information input operation guidance when there is no information input from said input device for a predetermined time.

23.

180 10. A screen displayed on the display when information is input from the input device is generated by synthesizing a plurality of image data by the control section, and an image corresponding to each image data is generated by the 21. The automatic transaction device according to claim 1 or 20, wherein the information is displayed in a predetermined area set on the screen of the display device.

24.

188] The control unit has a plurality of types of image data for the explanation display and a plurality of types of image data for the operation screen, generates image data for a procedure display according to the type of transaction, and stores a plurality of input item fields for the procedure display. according to the input order of the information, acquire the image data of the explanation display and the image data of the operation screen corresponding to the specified items in the input item column, and acquire the image data of the procedure display and the image of the operation screen 5. The automated teller machine according to claim 4, wherein data of an image to be displayed on said display device is generated using the data and image data of the generated procedure display.

25.

200 21. The automated teller machine according to claim 1 or 20, further comprising voice output means for outputting voice when said control unit is ready to receive information from said input device.

26.

206 10. The automatic processing method according to claim 3, further comprising voice output means for outputting voice when said control unit moves said procedure display in a direction substantially orthogonal to the longitudinal direction of each of said input item columns. trading device.

27.

213 10. The input device is a touch panel, position detection means for detecting position information of an object in contact with the touch panel, and whether the position of the object in contact with the touch panel is changed based on the detected position information. and a voice output means for outputting a warning sound when the determination means determines that the object is changing its position while in contact with the touch panel. The automatic transaction device according to claim 1 or 20.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－25320

(43)公開日　平成11年(1999)１月29日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０７Ｄ　9/00	４２６	Ｇ０７Ｄ　9/00	４２６Ｃ
Ｇ０６Ｆ　3/14	３３０	Ｇ０６Ｆ　3/14	３３０Ａ
19/00		15/30	Ａ
			３２０

審査請求　未請求　請求項の数27　ＯＬ　（全 33 頁）

(21)出願番号　特願平9－182881

(22)出願日　平成９年(1997)７月８日

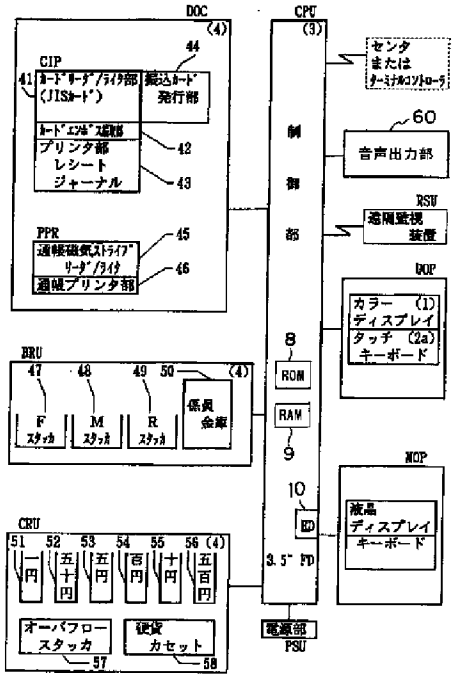
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　塩田　拓治
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　深井　みどり
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　弁理士　遠山　勉　（外１名）

最終頁に続く

(54)【発明の名称】　自動取引装置

(57)【要約】
【課題】利用者の操作の習熟度に関係なく操作性の向上を図ることができる自動取引装置を提供すること。
【解決手段】本発明による自動取引装置によれば、制御部ＣＰＵがユーザからの要求に応じた取引の取引画面７０をディスプレイ装置１に表示させる。ディスプレイ装置１には、入力対象を示す入力データ欄８７を入力順に並べてなる手順表示８２が表示される。そして、制御部ＣＰＵは、入力対象の何れかをユーザに入力させる際には、入力対象に応じた種類の操作画面８４を、取引画面７０の手順表示７２の上に重ねた状態で表示させる。これによって、ユーザが手順表示８２から取引の操作手順の流れ、入力対象等を適正に把握した上で、データ入力を行うことが可能となる。

ＡＴＭの具体的構成を示すブロック図



Petitioner Exhibit 1002-3098

【特許請求の範囲】
【請求項１】情報を表示するディスプレイ装置と、取引に係る情報を入力する入力装置と、前記ディスプレイ装置の情報表示を制御し且つ前記ディスプレイ装置に表示された情報に応じて前記入力装置から入力された情報に基づいて取引処理を行う制御部とを備え、
前記制御部が、前記ディスプレイ装置に対し、前記入力装置から入力される複数の情報の項目が夫々示された複数の入力項目欄を入力順に並べて形成された手順表示を表示させるとともに、前記複数の情報の夫々が前記入力順に従って前記入力装置から入力される際に各情報に対応する操作画面を前記手順表示の上に重ねた状態で夫々表示させることを特徴とする自動取引装置。
【請求項２】前記手順表示が、前記ディスプレイ装置に常時表示されることを特徴とする請求項１記載の自動取引装置。
【請求項３】情報を表示するディスプレイ装置と、取引に係る情報を入力する入力装置と、前記ディスプレイ装置の情報表示を制御し且つ前記ディスプレイ装置に表示された情報に応じて前記入力装置から入力された情報に基づいて取引処理を行う制御部とを備え、
前記ディスプレイ装置の画面には、特定領域が設定されており、前記制御部が、前記ディスプレイ装置に対し、前記入力装置から入力される複数の情報の項目が夫々示された複数の入力項目欄を入力順に並べて形成された手順表示を表示させるとともに、前記取引の操作手順の進行に応じて前記手順表示を前記各入力項目欄の長手方向とほぼ直交する方向へ移動させることによって、前記複数の入力項目欄のうち現在行われている操作に対応する入力項目欄を前記特定領域にて表示させることを特徴とする自動取引装置。
【請求項４】前記特定領域の下側に前記操作画面が配置され、前記特定領域の上側に前記操作画面の説明が示された説明表示が配置され、この説明表示の上側に取引種別が示された取引種別表示欄が配置されることを特徴とする請求項２記載の自動取引装置。
【請求項５】前記各入力項目欄の夫々には、入力項目に対応する情報が示される入力情報表示域が形成されており、前記制御部は、前記入力装置から入力された情報を保持する保持手段を有し、ユーザからの要求に応じて前記ディスプレイ装置の表示内容を前記保持手段に保持された情報の入力時の状態に戻し、前記保持手段から該当する情報を読み出して当該入力情報表示域に表示させることを特徴とする請求項２記載の自動取引装置。
【請求項６】前記制御部が、ユーザからの要求に応じて少なくとも前記手順表示と重なる範囲の操作画面を前記ディスプレイの表示内容から除外し、前記保持手段に保持された情報を該当する入力項目欄の入力情報表示域に表示させることを特徴とする請求項５記載の自動取引装置。
【請求項７】前記制御部が、前記ディスプレイ装置の表示内容の変更速度をユーザからの要求に応じて変化させることを特徴とする請求項１記載の自動取引装置。
【請求項８】前記制御部が、前記入力装置から情報が入力される際にその情報の入力に係る操作情報を前記ディスプレイ装置に表示させる情報提示手段を有するとともに、前記情報提示手段によって前記ディスプレイ装置に前記操作情報が表示される回数をユーザからの要求に応じて変更することを特徴とする請求項１記載の自動取引装置。
【請求項９】前記制御部は、前記手順表示を前記ディスプレイ装置に表示させる際に、その手順表示を構成する入力項目欄の数と手順表示を固定して表示させるか否かを判定するための閾値である固定閾値とを対比し、前記入力項目欄の数が固定閾値未満である場合に、前記手順表示を前記ディスプレイ装置に固定して表示させることを特徴とする請求項２記載の自動取引装置。
【請求項１０】前記制御部は、前記特定領域にて表示される入力項目欄の入力情報表示域，及びこの入力情報表示域に表示される情報を拡大して表示することを特徴とする請求項３記載の自動取引装置。
【請求項１１】前記操作画面の一部が半透明で表示されることを特徴とする請求項１記載の自動取引装置。
【請求項１２】前記取引種別表示欄には、取引に係る処理を強制終了させる取消ボタンが設けられていることを特徴とする請求項４記載の自動取引装置。
【請求項１３】前記複数の入力項目欄の夫々における入力情報表示域にはこの入力情報表示域に表示された情報を修正するためのボタンが設けられていることを特徴とする請求項５記載の自動取引装置。
【請求項１４】前記制御部は、取引における全ての情報が入力された場合に、入力された各情報の確認画面として前記手順表示を前記ディスプレイに表示させるとともに、前記全ての情報の夫々を該当する入力情報表示域に表示させることを特徴とする請求項５記載の自動取引装置。
【請求項１５】前記複数の入力項目欄が、前記入力装置から入力される情報の属性に応じて複数の操作セットに区分けされており、操作セット毎に異なる色で表示されていることを特徴とする請求項３記載の自動取引装置。
【請求項１６】前記操作セットを構成する複数の入力項目欄が、情報の入力順に沿ったグラデーションを描く状態で色分けされていることを特徴とする請求項１５記載の自動取引装置。
【請求項１７】前記ディスプレイ装置の表示内容をなす画面の背景の基調色が、前記特定領域にて表示される入力項目欄の色に応じて変化することを特徴とする請求項１５記載の自動取引装置。
【請求項１８】前記制御部は、ユーザが特定の情報を入力するに要した時間である入力時間を検出し、検出した

Petitioner Exhibit 1002-3099

入力時間とユーザの操作の習熟度を判定するための閾値である習熟度閾値とを対比し、前記入力時間が前記習熟度閾値以下である場合には、前記ディスプレイ装置の表示内容の変更速度を上昇させることを特徴とする請求項１記載の自動取引装置。

【請求項１９】前記制御部は、前記入力装置から情報が入力される際にその情報の入力に係る操作情報を前記ディスプレイ装置に表示させる情報提示手段を有し、前記入力時間が前記習熟度閾値以下である場合には、前記情報提示手段によって前記ディスプレイ装置に前記操作情報が表示される回数を低減することを特徴とする請求項１８記載の自動取引装置。

【請求項２０】情報を表示するディスプレイ装置と、取引に係る情報を入力する入力装置と、前記ディスプレイ装置の情報表示を制御し且つ前記ディスプレイ装置に表示された情報に応じて前記入力装置から入力された情報に基づいて取引処理を行う制御部とを備え、

前記制御部が、複数の操作からなる一つの手順と前記一つの手順に含まれる複数の操作に夫々対応する複数の手順との何れか一方をユーザからの要求に応じて提供することを特徴とする自動取引装置。

【請求項２１】前記制御部は、前記入力装置から所定時間情報の入力がない場合に、情報の入力を促すための注意表示を前記ディスプレイ装置に表示させることを特徴とする請求項１又は２０記載の自動取引装置。

【請求項２２】前記制御部は、前記入力装置から所定時間情報の入力がない場合に、情報の入力操作ガイダンスを前記ディスプレイ装置に表示させることを特徴とする請求項１又は２０記載の自動取引装置。

【請求項２３】前記入力装置から情報が入力される際に前記ディスプレイに表示される画面は、前記制御部が複数の画像データを合成することによって生成されており、前記各画像データに対応する画像は、前記ディスプレイ装置の画面に設定された所定領域にて表示されることを特徴とする請求項１又は２０記載の自動取引装置。

【請求項２４】前記制御部は、前記説明表示の画像データ及び前記操作画面の画像データを夫々複数種類保有し、取引種別に応じた手順表示の画像データを生成し、この手順表示をなす複数の入力項目欄の何れかを情報の入力順に従って特定し、特定した入力項目欄の項目に夫々対応する説明表示の画像データ及び操作画面の画像データを取得し、取得した手順表示の画像データ，操作画面の画像データ，及び作成した手順表示の画像データを用いて前記ディスプレイ装置に表示させる画像のデータを生成することを特徴とする請求項４記載の自動取引装置。

【請求項２５】前記制御部が前記入力装置から情報を受け取り可能となった場合に音声を出力する音声出力手段をさらに備えたことを特徴とする請求項１又は２０記載の自動取引装置。

【請求項２６】前記制御部が前記手順表示を前記各入力項目欄の長手方向とほぼ直交する方向へ移動させた場合に音声を出力する音声出力手段をさらに備えたことを特徴とする請求項３記載の自動取引装置。

【請求項２７】前記入力装置がタッチパネルであり、このタッチパネルに接触した物体の位置情報を検出する位置検出手段と、検出された位置情報に基づいて前記物体が前記タッチパネルと接触した状態でその位置を変えているか否かを判定する判定手段と、前記判定手段が前記物体がタッチパネルと接触した状態でその位置を変えていると判定した場合に警告音を出力する音声出力手段とを備えたことを特徴とする請求項１又は２０記載の自動取引装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、現金自動預金支払装置(ＡＴＭ：Automatic Teller's Machine)，現金自動支払装置(ＣＤ：Cash Dispenser)，現金自動預金装置，振込専用装置，或いは証券発行装置等と称される自動取引装置に関する。

【０００２】

【従来の技術】近年、銀行等の金融機関において、行員等を介さないで取引を可能にする自動取引装置が実用化されている。このような自動取引装置では、顧客が装置のディスプレイの画面表示を見ながら対話的に情報の入力等の操作を行うことによって、所望の取引が行われる。

【０００３】即ち、自動取引装置のディスプレイ装置には、初期画面として取引可能な項目を全て表示したスタート画面が表示される。そして、顧客がこのスタート画面で目的とする取引項目を選択すると、自動取引装置による処理が開始される。ディスプレイはタッチパネルを備えており、顧客がディスプレイ装置に表示されたボタンを押すことによって、自動取引装置に対する操作やデータ入力がなされる。

【０００４】スタート画面で任意の取引が選択される(ディスプレイ装置に表示された任意の取引種別ボタンが押される)と、自動取引装置は、当該取引に対応した処理を実行する。即ち、自動取引装置は、当該取引が顧客との間でなされるように予め定められた操作手順に従って、自動取引装置の操作内容を示す複数の取引画面をディスプレイ装置に順次表示する。これに対し、顧客が各取引画面の表示内容に従ってその画面内に設定されたボタンを押すことで、操作手順が進められ、次の取引画面がディスプレイ装置に表示される。そして、全ての操作手順が終了すると、自動取引装置による取引処理が終了し、当該取引が顧客と金融機関との間で実行されたものとして取り扱われる。

【０００５】日常生活を営む上で金融機関との取引は不可欠であり、あるデータによれば、銀行等の金融機関の

Petitioner Exhibit 1002-3100

来店客の約８０％は自動取引装置を利用して取引を行っている。このような大多数の人が利用する自動取引装置は、非常に公共性の高い装置であるといえる。

【０００６】

【発明が解決しようとする課題】しかしながら、従来における自動取引装置は、以下の問題を有していた。即ち、自動取引装置の利用者は、若年層から高齢層までと広い年齢層にまたがっている。また、自動取引装置の操作についての知識，或いは金融機関との取引知識等も利用者によって千差万別である。即ち、自動取引装置の操作に対する習熟度は、利用者によって大きく異なる。これに対処すべく、自動取引装置は、利用者の習熟度に関係なく利用者の全てに対し平等な操作環境を提供するように構成されることが望まれる。

【０００７】ところが、従来における自動取引装置では、自動取引装置の操作は、各取引画面に表示された指示に従って行われるが、各取引画面には、その時点での操作内容が示されるのみであった。また、各取引画面は、操作手順が進む度に次の取引画面と完全に切り替わっていた(図３２，図３３参照)。このため、利用者は、既に行った操作，既に入力したデータの内容，これから行う操作の内容，或いは操作手順の全体の流れ等を、現在ディスプレイに表示されている取引画面の表示内容から把握することができなかった。従って、利用者が現在行っている操作や操作手順の進み具合を把握できなくなり、データの誤入力，装置の誤操作を行ってしまう場合があった。

【０００８】また、従来における自動取引装置では、自動取引装置を用いて実行可能な複数の取引の夫々に対して１通りの操作手順のみが設定され、この操作手順に従った複数の取引画面がディスプレイに順次表示されるのみであった(図３１，図３２，図３３参照)。このため、自動取引装置の利用者は、その習熟度に拘わらず同一の操作手順に従って自動取引装置の操作を行わなくてはならなかった。ここで、自動取引装置の操作手順は、可能な限り広い範囲の利用者に対応すべく、平均的な操作の習熟度を持つ利用者に合わせて設定されていた。

【０００９】このため、操作手順は、習熟度の低い利用者にとっては簡略的であり、習熟度の高い利用者にとっては冗長なものとなっていた。従って、習熟度の低い利用者が自動取引装置の操作手順の順序，或いは操作方法等について把握又は予測できず、誤った操作を行ってしまう場合があった。一方、習熟度が高い利用者が、冗長な操作手順に従って自動取引装置を操作することに煩わしさを覚え、この煩わしさのために取引画面の表示内容(入力対象等)の確認を疎かにし、データの誤入力，或いは誤操作を行ってしまう場合があった。

【００１０】本発明は上記問題に鑑みなされたものであり、利用者の操作の習熟度に関係なく操作性の向上を図ることができる自動取引装置を提供することを課題とする。

【００１１】

【課題を解決するための手段】本発明は、上述した課題を解決するために以下の構成を採用する。すなわち、請求項１の発明は、情報を表示するディスプレイ装置と、取引に係る情報を入力する入力装置と、前記ディスプレイ装置の情報表示を制御し且つ前記ディスプレイ装置に表示された情報に応じて前記入力装置から入力された情報に基づいて取引処理を行う制御部とを備えた自動取引装置である。この自動取引装置は、前記制御部が、前記ディスプレイ装置に対し、前記入力装置から入力される複数の情報の項目が夫々示された複数の入力項目欄を入力順に並べて形成された手順表示を表示させるとともに、前記複数の情報の夫々が前記入力順に従って前記入力装置から入力される際に各情報に対応する操作画面を前記手順表示の上に重ねた状態で夫々表示させることを特徴とする。

【００１２】請求項１の発明によると、制御部がディスプレイ装置に対し、手順表示を表示させる。そして、複数の情報の夫々が入力される際には、制御部は、各情報に対応する操作画面を手順表示の上に重ねた状態で表示させる。従って、自動取引装置のユーザは、手順表示から複数の入力項目，入力項目数，入力順等の情報を把握した上で、手順画面の上に重ねて表示された操作画面を用いて操作することが可能となる。

【００１３】請求項２の発明は、請求項１の手順表示が、前記ディスプレイ装置に常時表示されることで、特定したものである。請求項３の発明は、情報を表示するディスプレイ装置と、取引に係る情報を入力する入力装置と、前記ディスプレイ装置の情報表示を制御し且つ前記ディスプレイ装置に表示された情報に応じて前記入力装置から入力された情報に基づいて取引処理を行う制御部とを備えた自動取引装置である。この自動取引装置は、前記ディスプレイ装置の画面には、特定領域が設定されており、前記制御部が、前記ディスプレイ装置に対し、前記入力装置から入力される複数の情報の項目が夫々示された複数の入力項目欄を入力順に並べて形成された手順表示を表示させるとともに、前記取引の操作手順の進行に応じて前記手順表示を前記各入力項目欄の長手方向とほぼ直交する方向へ移動させることによって、前記複数の入力項目欄のうち現在行われている操作に対応する入力項目欄を前記特定領域にて表示させることを特徴とする自動取引装置である。

【００１４】請求項４の発明は、請求項２の特定領域の下側に前記操作画面が配置され、前記特定領域の上側に前記操作画面の説明が示された説明表示が配置され、この説明表示の上側に取引種別が示された取引種別表示欄が配置されることで、特定したものである。

【００１５】請求項５の発明は、請求項２の各入力項目欄の夫々には、入力項目に対応する情報が示される入力

Petitioner Exhibit 1002-3101

情報表示域が形成されており、前記制御部は、前記入力装置から入力された情報を保持する保持手段を有し、ユーザからの要求に応じて前記ディスプレイ装置の表示内容を前記保持手段に保持された情報の入力時の状態に戻し、前記保持手段から該当する情報を読み出して当該入力情報表示域に表示させることで、特定したものである。

【００１６】請求項６の発明は、請求項５の制御部が、ユーザからの要求に応じて少なくとも前記手順表示と重なる範囲の操作画面を前記ディスプレイの表示内容から除外し、前記保持手段に保持された情報を該当する入力項目欄の入力情報表示域に表示させることで、特定したものである。

【００１７】請求項７の発明は、請求項１の制御部が、前記ディスプレイ装置の表示内容の変更速度をユーザからの要求に応じて変化させることで、特定したものである。請求項８の発明は、請求項１の制御部が、前記入力装置から情報が入力される際にその情報の入力に係る操作情報を前記ディスプレイ装置に表示させる情報提示手段を有するとともに、前記情報提示手段によって前記ディスプレイ装置に前記操作情報が表示される回数をユーザからの要求に応じて変更することで、特定したものである。

【００１８】請求項９の発明は、請求項２の制御部が、前記手順表示を前記ディスプレイ装置に表示させる際に、その手順表示を構成する入力項目欄の数と手順表示を固定して表示させるか否かを判定するための閾値である固定閾値とを対比し、前記入力項目欄の数が固定閾値未満である場合に、前記手順表示を前記ディスプレイ装置に固定して表示させることで、特定したものである。

【００１９】請求項１０の発明は、請求項３の制御部が、前記特定領域にて表示される入力項目欄の入力情報表示域，及びこの入力情報表示域に表示される情報を拡大して表示することで、特定したものである。

【００２０】請求項１１の発明は、請求項１の操作画面の一部が半透明で表示されることで、特定したものである。請求項１２の発明は、請求項４の取引種別表示欄には、取引に係る処理を強制終了させる取消ボタンが設けられていることで、特定したものである。

【００２１】請求項１３の発明は、請求項５の複数の入力項目欄の夫々における入力情報表示域には、この入力情報表示域に表示された情報を修正するためのボタンが設けられていることで、特定したものである。

【００２２】請求項１４の発明は、請求項５の制御部が、取引における全ての情報が入力された場合に、入力された各情報の確認画面として前記手順表示を前記ディスプレイに表示させるとともに、前記全ての情報の夫々を該当する入力情報表示域に表示させることで、特定したものである。

【００２３】請求項１５の発明は、請求項３の複数の入力項目欄が、前記入力装置から入力される情報の属性に応じて複数の操作セットに区分けされており、セット毎に異なる色で表示されていることで、特定したものである。

【００２４】請求項１６の発明は、請求項１５の操作セットを構成する複数の入力項目欄が、情報の入力順に沿ったグラデーションを描く状態で色分けされていることで、特定したものである。

【００２５】請求項１７の発明は、請求項１５のディスプレイ装置の表示内容をなす画面の背景の基調色が、前記特定領域にて表示される入力項目欄の色に応じて変化することで、特定したものである。

【００２６】請求項１８の発明は、請求項１の制御部が、ユーザが特定の情報を入力するに要した時間である入力時間を検出し、検出した入力時間とユーザの操作の習熟度を判定するための閾値である習熟度閾値とを対比し、前記入力時間が前記習熟度閾値未満である場合には、前記ディスプレイ装置の表示内容の変更速度を上昇させることで、特定したものである。

【００２７】請求項１９の発明は、請求項１８の制御部が、前記入力装置から情報が入力される際にその情報の入力に係る操作情報を前記ディスプレイ装置に表示させる情報提示手段を有し、前記入力時間が前記習熟度閾値未満である場合には、前記情報提示手段によって前記ディスプレイ装置に前記操作情報が表示される回数を低減することで、特定したものである。

【００２８】請求項２０の発明は、情報を表示するディスプレイ装置と、取引に係る情報を入力する入力装置と、前記ディスプレイ装置の情報表示を制御し且つ前記ディスプレイ装置に表示された情報に応じて前記入力装置から入力された情報に基づいて取引処理を行う制御部とを備えた自動取引装置である。この自動取引装置は、前記制御部が、複数の操作からなる一つの手順と前記一つの手順に含まれる複数の操作に夫々対応する複数の手順との何れか一方をユーザからの要求に応じて提供することを特徴とする。

【００２９】請求項２１の発明は、請求項１又は２０の制御部が、前記入力装置から所定時間情報の入力がない場合に、情報の入力を促すための注意表示を前記ディスプレイ装置に表示させることで、特定したものである。

【００３０】請求項２２の発明は、請求項１又は２０の制御部が、前記入力装置から所定時間情報の入力がない場合に、情報の入力操作ガイダンスを前記ディスプレイ装置に表示させることで、特定したものである。

【００３１】請求項２３の発明は、請求項１又は２０において、入力装置から情報が入力される際に前記ディスプレイに表示される画面は、前記制御部が複数の画像データを合成することによって生成されており、前記各画像データに対応する画像は、前記ディスプレイ装置の画面に設定された所定領域にて表示されることで、特定し

Petitioner Exhibit 1002-3102

たものである。

【００３２】請求項２４の発明は、請求項４の制御部が、前記説明表示の画像データ及び前記操作画面の画像データを夫々複数種類保有し、取引種別に応じた手順表示の画像データを生成し、この手順表示をなす複数の入力項目欄の何れかを情報の入力順に従って特定し、特定した入力項目欄の項目に夫々対応する説明表示の画像データ及び操作画面の画像データを取得し、取得した手順表示の画像データ，操作画面の画像データ，及び作成した手順表示の画像データを用いて前記ディスプレイ装置に表示させる画像のデータを生成することで、特定したものである。

【００３３】請求項２５の発明は、請求項１又は２０の自動取引装置が、前記制御部が前記入力装置から情報を受け取り可能となった場合に音声を出力する音声出力手段をさらに備えたことで、特定したものである。

【００３４】請求項２６の発明は、請求項３の自動取引装置が、前記制御部が前記手順表示を前記各入力項目欄の長手方向とほぼ直交する方向へ移動させた場合に音声を出力する音声出力手段をさらに備えたことで、特定したものである。

【００３５】請求項２７の発明は、請求項１又は２０の入力装置がタッチパネルであり、このタッチパネルに接触した物体の位置情報を検出する位置検出手段と、検出された位置情報に基づいて前記物体が前記タッチパネルと接触した状態でその位置を変えているか否かを判定する判定手段と、前記判定手段が前記物体がタッチパネルと接触した状態でその位置を変えていると判定した場合に、警告音を出力する音声出力手段とを備えたことで、特定したものである。

【００３６】

【発明の実施の形態】以下、本発明の実施形態を図面に基づいて説明する。

〔実施形態１〕最初に、本発明による実施形態１を説明する。

〔自動取引装置の構成〕図１は、実施形態１による現金自動預金支払装置（以下、「ＡＴＭ」という：自動取引装置に相当）の主要構成を示すブロック図である。図１において、ＡＴＭは、ディスプレイ装置１，入力装置２ａ，中央処理部３および媒体処理装置４を備えている。

【００３７】ディスプレイ装置１は、例えばＣＲＴ表示器または液晶ディスプレイパネルを利用し、ＡＴＭの操作情報等を表示する。入力装置２ａは、ディスプレイ装置１の表示面に重ねられた透明な板状のスイッチ(タッチパネル)である。入力装置２ａは、利用者がタッチパネルに触れた位置を検出し、この位置に応じた情報を中央処理部３に入力する。媒体処理装置４は磁気カード、通帳、伝票、現金等を含む媒体を取り扱う。

【００３８】中央処理部３は、入力制御部５，ＣＧ(Character Generator)部６，イメージデータ保持部７，及び処理制御装置２０を備えている。入力制御部５は、入力装置２ａを制御する。ＣＧ部６は、例えば表示に必要な文字パターン(キャラクタコード，フォントデータ)を記憶するデータセットからなるキャラクタジェネレータを有し、ディスプレイ装置１に表示されるメッセージ等の表示情報を構成する文字データを生成する。イメージデータ保持部７には、予めディスプレイ装置１に表示する表示画面を形成する複数のイメージデータが格納されている。複数のイメージデータの夫々は、必要に応じてこのイメージデータ保持部７から読み出され、表示に供される。また、各イメージデータは、必要に応じてＣＧ部６が発生する文字パターンと合成して表示に供される。

【００３９】なお、イメージデータ保持部７に格納されるイメージデータは、例えば、ＡＴＭの描画データであっても良く、実物のＡＴＭをビデオカメラ等の撮像装置で撮像し必要な部分のみを切り出したイメージデータであっても良い。

【００４０】処理制御装置２０は、表示データ処理部２１、表示制御部２２および割り込み制御部２３を有している。処理制御装置２０は、ディスプレイ装置１による情報表示を制御するとともに、入力制御部５を介して入力装置２ａから入力される情報に基づいて取引処理を行う。処理制御装置２０は、中央処理部３の例えばソフトウェア主導で機能して主たる処理制御を行う装置であり、例えばマイクロプロセッサユニットにより構成される。

【００４１】表示データ処理部２１は、入力制御部５，ＣＧ部６，イメージデータ保持部７，及び割り込み処理部２３から得られる入力情報，表示文字データ，イメージデータ，及び割り込み等の情報に基づいて、ディスプレイ装置１に表示するための表示データを生成し、表示制御部２２に供給する。

【００４２】表示制御部２２は、表示データ処理部２１から受け取った表示データをもとにディスプレイ装置１を制御してこの表示データに応じた画面表示を行う。割り込み処理部２３は、タイマ割り込みのためのタイマ制御部２３ａを有し、入力制御部５および媒体処理装置４からの情報に応じて、表示データ処理部２１に対する割り込み制御を行う。

【００４３】図2は、図3に示す構成が組み込まれたＡＴＭの外観構成を示す斜視図である。図２には、ＡＴＭの筐体，図１に示したディスプレイ装置１と入力装置２ａとからなる表示入力部３１，預金通帳の挿入・取り出しのための通帳挿抜口３２，カードや伝票の挿入・取り出しのためのカード挿抜口３３，硬貨の挿入・取り出しのための硬貨挿抜口３４，及び紙幣の挿入・取り出しのための紙幣挿抜口３５とが示されている。

【００４４】図3は、ＡＴＭの具体的な内部構成を示すブロック図である。図３において、ＡＴＭは、証書出力

Petitioner Exhibit 1002-3103

・カード読み書き部ＤＯＣ，紙幣リサイクル部ＢＲＵ，コインリサイクル部ＣＲＵ，顧客操作部ＵＯＰ，管理操作部ＭＯＰ，制御部ＣＰＵ，及び電源部ＰＳＵを、その内部に搭載している。

【００４５】制御部ＣＰＵは、上述した中央処理部３に相当する(図１参照)。制御部ＣＰＵは、通信回線等の伝送路を介してセンタのホストコンピュータに接続されている。或いは、制御部ＣＰＵは、通信回線等の伝送路からターミナルコントローラ(ターミナルコントローラには複数のＡＴＭ等の端末装置が接続される)に接続され、このターミナルコントローラを介してセンタのホストコンピュータに結合されている。ＡＴＭは、センタとの交信を行って、センタの元帳、すなわち個人の残高、取引履歴等が格納されているファイルを更新しながら取引を進める。

【００４６】また、制御部ＣＰＵには、特に支店，無人化店舗(ＡＴＭ装置だけが設置してある店舗)等に設置されたＡＴＭの状態を遠隔地から監視するための遠隔監視装置ＲＳＵが、通信回線等の伝送路を介して結合されている。遠隔監視装置ＲＳＵは、複数台のＡＴＭを監視して、それらの障害予防，障害発見，障害対策，或いは保守等を行う。

【００４７】証書出力・カード読み書き部ＤＯＣ，紙幣リサイクル部ＢＲＵ，及びコインリサイクル部ＣＲＵは、上述した媒体処理装置４に相当する(図１参照)。証書出力・カード読み書き部ＤＯＣは、カード読み書き・画像読み取り・プリンタ部ＣＩＰ，及び通帳プリンタ部ＰＰＲからなる。カード読み書き・画像読み取り・プリンタ部ＣＩＰは、カードリーダ／ライタ部４１，カードエンボス読み取り部４２、プリンタ部４３，及び振込カード発行部４４からなる。

【００４８】カードリーダ／ライタ部４１は、取引を行うためにカード挿抜口３３に挿入されたカードの磁気ストライプの口座番号、支店番号等の情報の読み取りを行い、必要に応じてその磁気ストライプに書き込みを行う。カードエンボス読み取り部４２は、カード挿抜口３３に挿入されたカードのカードのエンボス加工部の名前、口座番号等をイメージ的に読み取る。プリンタ部４３は、カードから読み取った口座番号、取引額等をレシート(明細票)に印字してカード挿抜口３３から出力し、且つレシートに印字した同じデータを装置内に印字情報の控えすなわちジャーナルとして残す。振込カード発行部４４は、振込取引に使用する振込カードに、裏面の磁気ストライプに振込先等の振込情報を書き込み且つ表面の空白部分に必要情報を印字し、振込カードを発行する。この振込カードもカード挿抜口３３から出力される。

【００４９】通帳プリンタＰＰＲは、通帳磁気ストライプリーダ／ライタ部４５および通帳プリンタ部４６を有している。通帳磁気ストライプリーダ／ライタ部４５は、例えば通帳挿抜口３２に挿入された通帳の磁気ストライプの読み書きを行う。通帳プリンタ部４６は、通帳への取引履歴の印字を行う。紙幣リサイクル部ＢＲＵは、例えば３つのスタッカ４７，４８，４９と係員金庫５０とを有し、紙幣を取り扱う。

【００５０】３つのスタッカ４７～４９は、例えば千円札を格納する１つのスタッカ４７、一万円札を格納する２つのスタッカ４８，４９である。出金取引を行う場合には、指定された金額分だけ、各スタッカ４７～４９より紙幣挿抜口３５に払い出し、入金取引を行う場合には、紙幣挿抜口３５に挿入された紙幣を金種毎に各スタッカ４７～４９に収納する。なお、五千円札は、回収専用のスタッカ(図示せず)に収納される。さらに、３つのスタッカ４７～４９は、着脱可能な係員金庫５０との間で、必要に応じて紙幣のやりとりを行う。すなわち、出金取引が連続して行われることにより３つのスタッカ４７～４９の何れかの紙幣が減少した場合には、係員金庫５０から紙幣が減少したスタッカに紙幣が補充され、入金取引が連続して行われる。一方、スタッカ４７～４９の何れかが紙幣で満杯になった場合には、満杯となったスタッカから紙幣が回収され係員金庫５０に搬送される。

【００５１】硬貨リサイクル部ＣＲＵは、各硬貨毎のスタッカ５１，５２，５３，５４，５５，５６，オーバフロースタッカ５７，及び硬貨カセット５８からなり、硬貨を取り扱う。出金取引や振込取引のように釣り銭が必要な取引等により、硬貨の払い出しが必要になった場合には、各スタッカ５１～５６から必要な枚数、必要な金額分の硬貨が、硬貨挿抜口３４から払い出される。また、硬貨が硬貨挿抜口３４に挿入された場合には、挿入された硬貨は、金種毎に各スタッカ５１～５６に格納される。さらに、硬貨の払い出しが連続し、各スタッカ５１～５６の硬貨が不足すると、硬貨が硬貨カセット５８から各スタッカ５１～５６へ補充される。さらに、硬貨の収納が連続することによって、各スタッカ５１～５６からオーバフローした硬貨は、オーバフロースタッカ５７に格納される。なお、オーバフロースタッカ５７，及び硬貨カセット５８は着脱可能であり、硬貨の補充・取り出しに用いられる。

【００５２】顧客操作部ＵＯＰは、ディスプレイ装置１としてのカラーディスプレイ装置５９，及びその表示画面上に重ね合わされた入力装置２ａとしてのタッチパネルからなるタッチキーボード６０を有している。すなわち、カラーディスプレイ装置５９の表示面およびタッチキーボード６０が、図３に示す表示入力部３１を構成する。

【００５３】管理操作部ＭＯＰは、液晶ディスプレイ６１，及びキーボード６２を有し、遠隔監視装置ＲＳＵと同様に、ＡＴＭの内部状態を把握するとともに、必要な保守操作を可能とする。

Petitioner Exhibit 1002-3104

【００５４】音声出力部６０は、音声処理プロセッサ，増幅回路，及びスピーカ等からなる。この音声出力部６０は、制御部ＣＰＵからの命令に応じて音声を外部に出力する。

〔ＡＴＭによる処理〕次に、上述したＡＴＭによる処理として、制御部ＣＰＵによる顧客操作部ＵＯＰに対する処理を説明する。図１において、中央処理部３(制御部ＣＰＵ)の処理制御装置２０は、図３に示す電源部ＰＳＵがＯＮとされると、自身が保有するＲＯＭ８又はハードディスク(ＨＤ)１０に記録された制御プログラムをＲＡＭ９にロードし、ＲＡＭ９にロードされた制御プログラムを実行し、ディスプレイ装置１に対する画面表示処理をスタートする。

【００５５】図４は、ディスプレイ装置１に対する画面表示処理を示すフローチャートである。図４において、処理がスタートすると、表示データ処理部２１は、入力装置２ａであるタッチパネルから位置情報が入力制御部５を介して転送されてきたか否かを判定する(ステップＳ０１)。このとき、表示データ処理部２１は、位置情報がきていないと判定した場合には、処理をステップＳ０４へ進める。これに対し、表示データ処理部２１は、位置情報がきたと判定した場合には、その位置情報を取得する(ステップＳ０２)。

【００５６】続いて、表示データ処理部２１は、取得した位置情報に基づいて、利用者によってディスプレイ装置１に表示された「取消」「修正」等のＡＴＭの操作ボタンが押されたのか否かを判定する。このとき、表示データ処理部２１は、操作ボタンが押されたと判定した場合(ステップＳ０３；ＹＥＳ)には、処理をステップＳ０５へ進める。これに対し、表示データ処理部２１は、操作ボタンが押されなかったと判定した場合(ステップＳ０３；ＮＯ)には、データ入力キーが押されたものとして、処理をステップＳ０４へ進める。

【００５７】表示データ処理部２１は、ステップＳ０４へ処理を進めた場合には、ステップＳ０２にて取得した位置情報に対応する文字データ(押されたキー(ボタン)に対応する文字データ)をＣＧ部６から読み出し、処理をステップＳ０５へ進める。

【００５８】表示データ処理部２１は、ステップＳ０５へ処理を進めた場合には、制御プログラムに従ってＣＧ部６から文字データを読み出すとともに、イメージデータ保持部７からイメージデータ(テクスチャデータ)を読み出す。続いて、表示データ処理部２１は、自身が保有する図示せぬＶＲＡＭ(Video RAM)上において、文字データとイメージデータとを合成した画面データを生成する(ステップＳ０６)。続いて、表示データ処理部２１は、図示せぬＶＲＡＭの記憶内容を表示制御部２２に転送する(ステップＳ０７)。

【００５９】すると、表示制御部２２が、図示せぬＶＲＡＭの記憶内容をビデオ信号に変換し(ステップＳ０８)、ディスプレイ装置１に転送する(ステップＳ０９)。これによって、ディスプレイ装置１には、ＡＴＭの取引画面７０(図５参照)が表示されるとともに、入力装置２ａから入力された情報が表示される。なお、ステップＳ０９の処理が終了すると、処理がステップＳ０１に戻る。

〔ディスプレイ装置の表示内容〕次に、ディスプレイ装置１の表示内容を説明する。

〈取引画面〉図５は、ディスプレイ装置１に表示される取引画面７０の説明図である。ＡＴＭの利用者は、ディスプレイ装置１に表示された取引画面７０の表示内容に従ってＡＴＭを操作し取引を行う。ディスプレイ装置１には、ＡＴＭに予め設定されている操作手順に従って、複数の取引画面７０が表示される。このとき、取引画面７０が他の取引画面７０に切り替わっても利用者が適正に取引画面７０の表示内容を把握できるように、取引画面７０は、以下のように構成されている。

【００６０】図５において、取引画面７０は、矩形に設定されており、取引種別表示領域７１と、操作説明領域７２と、入力対象表示領域７３と、入力データ表示領域７４と、操作領域７５とからなる。

【００６１】取引種別表示領域７１は、取引画面７０の最も上側に設定された帯状の領域であり、取引種別(例えば、「振込」「払出」「預入」等)が表示される。また、操作説明領域７２は、取引種別表示領域７１のすぐ下側に設定された帯状の領域であり、利用者に対するＡＴＭの操作説明を示す文字列が表示される。

【００６２】入力対象表示領域７３及び入力データ表示領域７４は、操作説明領域７２のすぐ下側に設定された帯状の領域である。入力対象表示領域７３は、取引画面７０の左側に配置されており、入力データ表示領域７４は、取引画面７０の右側に配置されている。入力対象表示領域７３には、入力対象(例えば、「依頼人名」「預入金額」「口座番号」等)を示す文字列が表示される。入力データ表示領域７４には、ＡＴＭの利用者が入力装置２ａを介して入力したデータを示す文字列が表示される。

【００６３】操作領域７５は、取引画面７０の最も下側に設定された矩形の領域である。この操作領域７５には、利用者がＡＴＭにデータを入力するためのキーやＡＴＭの操作ボタンが表示される。

【００６４】上述した各領域７２～７５の位置は、ディスプレイ装置１の表示内容の変更に関係なく固定されている。このため、ＡＴＭの利用者は、ＡＴＭの操作を進めていくうちにどの情報がどの位置に表示されるのかを把握又は予測できる。従って、取引画面７０が他の取引画面７０に切り替わった場合でも、利用者は取引画面７０に表示された内容を適正に把握できるので、利用者は円滑にＡＴＭを操作し、取引を行うことができる。

〈取引画面の画面要素〉図６は、取引画面７０を構成す

Petitioner Exhibit 1002-3105

る画面要素の説明図である。図６には、「振込」の場合における取引画面７０の画面要素が示されている。図６に示すように、取引画面７０は、背景８１，手順表示８２，入力パネル表示８３，及び説明表示８４の各画面要素をＡＴＭの操作手順に従って重ねることによって構成される。これらの画面要素は、図１に示すイメージデータ保持部７内にテクスチャデータとして格納されている。また、イメージデータ保持部７は、これらのテクスチャデータに対応するカラーパレットデータを有している。そして、上述した画面表示処理(図４参照)が行われることによって、取引画面７０がディスプレイ装置１に表示される。

〈背景〉図６において、背景８１は、矩形に設定されており、取引画面７０の全体に亘って配置される。背景８１の上部には、帯状の取引種別表示欄８１ａが設けられており、図５に示した取引種別表示領域７１に配置される。この取引種別表示欄８１ａには、取引種別を示す文字列が表示される(図６では、例として「お振込み」の文字列を図示)。

〈手順表示〉手順表示８２は、背景８１の上に重ねて表示される。この手順表示８１は、図５に示した操作説明領域７２，入力対象表示領域７３，入力データ表示領域７４，及び操作領域７５に亘って配置される。この手順表示８２には、取引の際にＡＴＭの利用者が行う操作手順が示されている。即ち、手順表示７２は、複数の帯状の入力データ欄８７(図６には、例として入力データ欄８７ａ～８７ｇを図示)からなる。各入力データ欄８７は、ＡＴＭの操作手順に従ってＡＴＭに入力されるデータ等が表示される欄であり、操作手順に従ってＡＴＭに入力される順で取引画面７０の上から下へ向かって並べられている。

【００６５】複数の入力データ欄８７の夫々における最も左側には、操作手順の順番である手順番号を示す数字が表示され、その右側には、入力対象名(操作項目名)が表示される。そして、入力対象名の右側には、入力装置２ａを介して入力されたデータを示す文字列が表示される。

【００６６】図７は、背景８１の上に手順表示８２が重ねられた取引画面７０の画面表示例を示す図である。この図７に示す例では、各入力データ欄８７ａ～８７ｇには、その最も左側に手順番号を示す数字が表示され、その右側には、入力対象名として、「振込先金融機関」「振込先支店名」「口座番号」「受取人名」「振込金額」「依頼人名」「電話番号」の項目名が夫々表示されている。そして、各入力対象名の右側には、各入力対象名に対応する入力データが表示されている。

【００６７】ところで、操作手順は、関連づけ可能な手順からなる複数の操作セットで構成されている。これに対応して、各入力データ欄８７は、操作セットを構成する複数の入力データ欄８７が一かたまりで配置され、互いに異なる操作セットを構成する入力データ欄８７同士は、間隔をあけて配置されている。

【００６８】例えば、図７に示す例では、「振込」の操作手順は、振込先に係る操作セット，金額に係る操作セット，及び依頼人に係る操作セットからなる。このような操作セットの構成に応じて、振込先に係る操作セットに対応する入力データ欄８７ａ～８７ｄ，及び依頼人に係る操作セットに対応する入力データ欄８７ｆ,８７ｇが、夫々一つの塊をなす状態で配置されている。そして、入力データ欄８７ｄと入力データ欄８７ｅとの間，入力データ欄８７ｅと入力データ欄８７ｆとの間には、それぞれスペース(空白)が設けられている。

【００６９】従って、ＡＴＭの利用者は、手順表示８２を見ることによって、操作手順の手順数，操作セット数，操作手順の順序，及び入力対象を容易に把握することができる。

〈手順番号の背景色〉図７において、図示することはできないが、各手順番号の背景色は、操作セットに応じて異なる色で表示されている。具体的には、入力データ欄８７ａ～８７ｄにおける各手順番号の背景色は、番号順に沿った赤色のグラデーションで設定されており、入力データ欄８７ｅにおける手順番号の背景色は、緑色で設定されており、入力データ欄８７ｆ,８７ｇにおける手順番号の背景色は、番号順に沿った青色のグラデーションで設定されている。

【００７０】これによって、ＡＴＭの利用者は、操作セットの意味を理解しなくても操作セットを把握することができる。また、操作手順が進むことによって、手順番号の背景色が長波長の色から短波長の色へと変化するので、利用者は手順番号の背景色から操作手順の進行状況を把握又は予測できる。

【００７１】また、取引画面７０の背景８１の基調色は、手順番号の背景色に応じて変化するようになっている。例えば、現在行われている操作手順に該当する手順番号の背景色が赤色である場合には、背景８１の基調色は赤色となる。これによって、利用者は現在行っている操作がどの操作セットに属するのかを容易に把握することができる。

〈注視領域〉図７において、取引画面７０の上縁から約１０分の３から約１０分の４までの帯状の範囲は、注視領域８０として設定されている。この注視領域８０は、人間工学において情報を精度良く受容できるとされている範囲である。上述した入力対象表示領域７３及び入力データ表示領域７４は、この注視領域８０に配置されている。このように、横長の注視領域８０を設定し、注視領域８０の上側に操作説明領域７２を設定し、注視領域８０の下側に操作領域７５が設定されているので、無駄な視線移動が抑えられる。従って、取引画面７０の視認性の向上を図ることができるとともに、取引画面７０の分かりにくさ，及び操作のしずらさを改善することがで

Petitioner Exhibit 1002-3106

きる。

【００７２】上述した複数の入力データ欄８７の夫々は、操作手順に従って注視領域８０(入力対象表示領域７３及び入力データ表示領域７４)に表示される。例えば、図７に示すように、取引が「振込」であれば、最初に、手順番号“１”を表示した入力データ欄８７(入力データ欄８７ａ)が、注視領域８０にて表示される。その後、データ入力が終了し、操作手順が次に進むと、図８に示すように、手順表示８２が画面の上側にスクロールし、次の手順番号“２”を表示した入力データ欄(入力データ欄８７ｂ)が、注視領域８０にて表示される。

【００７３】即ち、手順表示８２は、操作手順が進む度に画面の上側へスクロールし、次の手順番号を表示した入力データ欄８７が、注視領域８０にて表示される。注視領域８０にて入力データ欄８７に表示される各データのうち、手順番号及び入力対象名は、注視領域８０内の入力対象表示領域７３に表示され、入力データを示す文字列は、注視領域８０内の入力データ表示領域７４に表示される。

【００７４】このように、現在進行中の操作手順を示す入力データ欄８７が注視領域８０に表示される。従って、ＡＴＭの利用者は、取引画面７０の最も見やすい部分である注視領域８０さえ見ていれば、注視領域８０にて表示される手順番号や入力対象を示す文字列から、現在自身が行っている操作手順や操作手順の進行状況を容易に把握することができる。また、手順表示８２がスクロールすることで、利用者は操作手順が進行していることを直感的に把握することができる。

【００７５】また、手順表示８２がスクロールする際には、ＡＴＭからシグナル音が発生する。この機能は、手順表示８２をスクロールさせる処理が行われている際に、制御部ＣＰＵから音声出力部６０(図３参照)に動作命令が与えられ、音声出力部６０がシグナル音を出力することで実現できる。このシグナル音によって、利用者を取引画面７０に注目させることができ、操作手順が進んだことを利用者に適正に把握させることができる。従って、利用者が操作手順の進行に気付かない場合に生じるタイムロスをなくし、ＡＴＭの操作時間の短縮を図ることができる。

【００７６】また、図７に示す例のように、取引の操作手順数が少ない場合には、取引開始時において手順表示８２を構成する複数の入力データ欄８７の全てが、ディスプレイ装置１に表示される。これに対し、取引における操作手順数が多く、取引開始時において複数の入力データ欄８７の全てを一度にディスプレイ装置１に表示できない場合には、図９(ａ)の画面表示例に示すように、表示可能な入力データ欄８７のみがディスプレイ装置１に表示される。

【００７７】上述した機能は、例えば以下のようにして実現される。即ち、図１に示す表示データ処理部２１は、ディスプレイ装置１に一度に表示可能な入力データ欄８７の数(閾値)を保有している。表示データ処理部２１は、取引開始時において、該当する手順表示８２のデータをイメージデータ保持部７から受け取り、その手順表示８２を構成する入力データ欄８７の数と上述した閾値とを対比する。このとき、入力データ欄８７の数が閾値を下回っている場合には、表示データ処理部２１は、ディスプレイ装置１に手順表示８２を構成する入力データ欄８７の全てを表示させる。これに対し、入力データ欄８７の数が閾値を下回っている場合には、表示データ処理部２１は、ディスプレイ装置１に手順表示８２を構成する入力データ欄８７の一部を表示させる。

【００７８】そして、図９(ｂ)の画面表示例に示すように、一つの操作手順が終了し、手順表示８２が画面の上側にスクロールする度に、取引開始時に表示できなかった入力データ欄８７の何れかが画面内に表示される。このとき、手順表示８２が画面の上側へスクロールすることによって、手順表示８２の一部が取引種別表示欄８１ａの上に重なることとなる場合には、その取引種別表示欄７１ａと重なる範囲の手順表示８２は、取引画面７０から消える。

【００７９】ところで、取引の操作手順数が少ない場合(例えば「払い戻し」の取引のように、「暗証番号」と「払い戻し金額」とを入力すれば操作手順が終了する場合)には、操作手順が次に進んでも手順表示８２がスクロールしない。この場合には、図１６に示すように、説明表示８３と入力パネル表示８４とが接した状態で、取引画面７０の下部に配置される。

【００８０】この機能は、図１に示す処理制御装置２０を以下のように構成することで実現できる。即ち、上述したように、表示データ処理部２１が表示すべき手順表示８２の入力データ欄８７の数と閾値とを対比し、入力データ欄８７の数が閾値を上回っている場合には、操作手順が次に進む際に手順表示８２のスクロール処理を行い、入力データ欄８７の数が閾値を下回っている場合には、図１６に示す取引画面７０をディスプレイ装置１に表示し、操作手順が次に進んでも手順表示８２のスクロール処理を行わないようにする。

〈説明表示及び入力パネル表示〉図６に戻って、説明表示８３は、帯状に設定されており、各操作手順における操作説明を示す文字列を表示する(図６では、「ご依頼人を入れ確認を押して下さい」の文字列を表示)。この説明表示８３は、手順表示８２の上に重ねた状態で、図５に示す操作説明領域７２に配置される。

【００８１】また、入力パネル表示８４は、矩形に設定されており、各操作手順において入力対象表示領域７３に表示された入力対象を入力するためのキーやボタンを表示する。この入力パネル表示８４は、手順表示８２の上に重ねた状態で、図５に示す操作領域７５に配置される。

Petitioner Exhibit 1002-3107

【００８２】図１０～図１２は、説明表示８３及び入力パネル表示８４の画面表示例を示す説明図である。図１０～図１２に示すように、説明表示８３及び入力パネル表示８４は、利用者の入力対象に応じて複数種類用意されている。例えば、口座番号を入力するための説明表示８３ａ及び入力パネル表示８４ａ(図１０参照)，金額を入力するための説明表示８３ｂ及び入力パネル８４ｂ(図１１参照)，文字を入力するための説明表示８３ｃ及び入力パネル表示８４ｃ(図１２参照)等が用意されている。

【００８３】図１０に示すように、入力パネル表示８４ａには、口座番号を入力するためのテンキー９１や、入力した口座番号を一旦確定させるための第１確認ボタン９２が設けられている。また、図１１に示すように、入力パネル表示８４ｂには、金額を入力するためのテンキー９１，桁(万,千)を入力するための桁ボタン９３，及び入力した金額を一旦確定させるための第１確認ボタン(円ボタン)９２等が設けられている。また、図１２に示すように、入力パネル表示８４ｃには、文字を入力するための５０音キー群９４，特定の単語(株式会社，有限会社，営業所，支店)を入力するための単語キー群９５，第１確認ボタン９２等が設けられている。

【００８４】このように、操作領域７５に配置される入力パネル表示８４を手順表示８２と別個の画面要素としてあるので、入力パネル表示８４(操作領域７５)が取引画面７０を占める割合を大きくとることができる。このため、入力パネル表示８３に表示されるキーやボタンの大きさ，或いはこれらの配置等を最適化することができる。従って、キーやボタンの押し間違いによる誤入力，及び誤操作の可能性を低減できる。これは、ＡＴＭの操作の習熟度の低い利用者，或いは視覚機能や手指の巧緻性の衰えた利用者にとって特に有効である。

【００８５】なお、入力パネル表示８４に表示されるキーやボタンに代えてアイコンが設けられていても良い。

〈取引画面の切り替え〉ところで、上述した背景８１と手順表示８２とは、ＡＴＭの利用者によるＡＴＭの操作開始から操作終了までのほぼ全体に亘ってディスプレイ装置１に表示される。従って、利用者は、これから行う入力操作の全体像を把握し、前後の項目間の関係を理解することができる。このため、事前に各入力対象(各操作手順)に対して精神的に準備が可能である。また、各操作手順において、操作手順の全体が把握できないことによる不安や苛立ちを感ずることがない。さらに、入力要求内容の解釈を誤り誤入力を行う等の危険性を回避することができる。

【００８６】これに対し、説明表示８３と入力パネル表示８４とは、操作手順に応じた種類のものが、各操作手順の開始に当たってディスプレイ装置１に表示される。実施形態１によるＡＴＭでは、操作手順に応じた説明表示８３及び入力パネル表示８４の切り替えによって、取引画面７０の切り替えが行われる。各操作手順が開始される際には、図１３の画面表示例に示すように、説明表示８３が画面の下縁から出現し、上述した操作説明領域７２に収まるまで画面の上縁へ向かって移動する。また、説明表示８３の出現と同時に、或いは説明表示８３の出現に続いて、入力パネル表示８４が画面の下縁から出現し、上述した操作領域７５に収まるまで画面の上縁へ向かって移動する。

【００８７】そして、説明表示８３が操作説明領域７２に収まり、且つ入力パネル表示８４が操作領域７５に収まると、手順表示８２のうち、操作説明領域７２に存する部位，及び操作領域７５に存する部位(説明表示８３又は入力パネル表示８４と重なる部位)が、説明表示８３又は入力パネル表示８４とによって隠された状態となる。これによって、ＡＴＭの利用者には、手順表示７２に示された入力対象名のうち、注視領域８０にて表示されている入力対象名のみが見える状態となる。従って、利用者は、現在行っている操作手順を明確に把握することができる。

【００８８】但し、説明表示８３及び入力パネル表示８４は、手順表示８２における各手順番号を示す数字の上に重ならないように設定されている。従って、ＡＴＭの利用者は、データの入力中においても操作手順数を把握できると共に、現在の操作手順がどのあたりまで進んでいるかを把握することができる。

【００８９】その後、入力パネル表示８４を用いてデータが入力され、操作手順が終了すると、説明表示８３及び入力パネル表示８４は、画面の下縁へ向かって移動し、ディスプレイ装置１から消える。そして、操作手順が次に進むと、その操作手順に応じた説明表示８３及び入力パネル表示８４が、上述した手法によってディスプレイ装置１内に現れる。また、手順表示８２が画面の上側へスクロールし、次の手順番号が示された入力データ欄８７が注視領域８０にて表示される。

【００９０】以下、操作手順が進む際に行われる説明表示８３及び入力パネル表示８４の切り替えと、手順表示８２のスクロールとを合わせて「画面遷移」と称する。

〈注視領域における拡大表示〉図１０～図１２に示すように、各入力データ欄８７は、注視領域８０にて表示される場合には、その入力データ表示領域７４に存する範囲が拡大して表示されるとともに、入力データを示す文字が他の入力データ欄８７における入力データを示す文字よりも拡大して表示される。これは、図１に示す表示データ処理部２１が、注視領域８０にて表示される入力データ欄８７の入力データ表示領域７４を拡大するとともに、当該入力データ表示領域７４にて表示される文字のフォントを拡大する処理を行うことで実現される。

【００９１】このように、入力されたデータを拡大表示することで、視力の低いＡＴＭの利用者が入力データを容易に判読可能となり、利用者の視力負担の軽減を図る

Petitioner Exhibit 1002-3108

ことができる。従って、データの誤入力やＡＴＭの誤操作の可能性を低減できる。また、視力負担の軽減が図られるので、高齢者，或いは弱視等の軽度の視覚障害者等をＡＴＭの利用者として加えることが可能となり、ＡＴＭの利用者の範囲拡大を図ることができる。

【００９２】また、注視領域８０の入力データ表示領域７４に表示される文字は、他の入力データ欄８７における入力データの文字よりも大きく表示されるので、他の入力データよりも強調された状態となる。従って、他の入力データ領域８７における文字との判別が容易に可能となるため、利用者の情報認知精度が向上する。

〈修正ボタン〉図６に示すように、複数の入力データ欄８７の夫々における最も右側には、修正ボタン１０１が夫々設けられている。各修正ボタン１０１は、ＡＴＭの利用者がデータ入力をミスした場合にそのデータの修正を行うためのボタンである。修正ボタン１０１の何れかが押されると、その修正ボタン１０１が属する入力データ欄８７における入力済みのデータを示す文字がクリアされ、利用者が新たにデータを入力可能な状態となる。

【００９３】このように、入力データ毎にその修正ボタン１０１を設けてあり、入力されたデータの隣に修正ボタン１０１を配置してあるので、利用者は、修正ボタン１０１の意味を適正に把握できるとともに、データ入力をミスした場合にその修正ボタン１０１を迷うことなく見つけることができる。また、利用者が、誤って別の修正ボタンを押してしまい修正を要しないデータが消えてしまうこと等を防止できる。また、利用者が修正ボタン１０１と誤認して取消ボタン８１ｂを押してしまうことも防止できる。従って、利用者によるＡＴＭ操作の正確性と操作速度の向上を図ることができる。

〈確認ボタン〉図１０～図１２に示すように、各入力パネル表示８４(例えば、８４ａ～８４ｃ)の右下のコーナーには、第１確認ボタン９２が夫々設けられている。この第１確認ボタン９２が押されると、入力装置２ａから確認信号が割込み処理部２３に対して与えられ、割込み処理部２３が表示データ処理部２１に対して確認処理命令を与える。

【００９４】すると、表示データ処理部２１が確認処理を行いＶＲＡＭの記憶内容を変更する。これによって、図１４に示すように、説明表示８３及び入力パネル表示８４が取引画面７０から消えるとともに、手順表示８２が画面の下側にスクロールし、これまでに入力されたデータを表示する状態となる。そして、利用者は、各入力データ領域８７に設けられた修正ボタン１０１の何れかを押すことによって、対応する入力データの修正を行うことができる。

【００９５】さらに、手順表示８２の下側には、矩形の確認表示１０４が表示される。確認表示１０４には、その左側に入力データの確認を促す指示が表示されるとともに、その右側に第２確認ボタン１０５が表示される。そして、ＡＴＭの利用者が第２確認ボタン１０５を押すと、当該操作手順が終了したものとして、操作手順が次に進められる。

【００９６】このように、手順表示８２を入力データの確認画面として用いるので、ＡＴＭの利用者は、今までに入力したデータを一括して確認・修正できるとともに、操作手順の順序，各操作手順の関連，入力データ間の関係等を理解できる。

〈取消ボタン〉図６に示すように、取引種別表示欄８１ａの右側には、取消ボタン８１ｂが設けられている。この取消ボタン８１ｂは、取引を取り消す(ＡＴＭの操作を強制終了させる)ためのボタンである。取消ボタン８１ｂが押されると、リセット信号が入力装置２ａから割込み処理部２３に与えられる。すると、割込み処理部２３が、リセット信号に基づいて強制終了命令を表示データ処理部２１に与える。これによって、表示データ処理部２１が取引を強制終了させる。その後、表示データ処理部２１は、図示せぬ取引種別選択画面をディスプレイ装置１に表示させる。

【００９７】このように、取引種別名と取消ボタン８１ｂとが同一の欄内に配置されているので、ＡＴＭの利用者が取消ボタン８１ｂに表示された「取消」の文字の意味を適正に把握することができる。従って、ＡＴＭの利用者が誤って取消ボタン８１ｂを押してしまい、それまでに行っていた操作が無駄となってしまうことを防止できる。

〈戻りボタン〉従来における自動取引装置では、入力すべきデータを全て入力する前に、既に入力したデータを利用者が見ることができなかった。また、利用者が既に入力したデータの一部を修正したい場合があってもその要求に応える機能が従来における自動取引装置には備わっていなかった。このため、利用者が既に行った操作手順をもう一度行いたい場合には、利用者は「取消」ボタンを押すしかなかった。

【００９８】ところが、利用者が「取消」ボタンを押した場合には、操作手順が一番最初に戻るとともに、既に入力されたデータが消去されてしまう。このため、利用者は操作をもう一度始めからやり直さなければならなかった。即ち、例えば利用者が既に入力したデータの誤りに気付いた場合には、「取消」ボタンを押して操作をやり直すしかないので、利用者が苛立ちを感じてしまい、これを起因としてデータ入力や操作を誤る場合があった。

【００９９】この問題に鑑み、実施形態１によるＡＴＭでは、図１０,図１１,図１２,及び図１５に示すように、入力パネル表示８４に戻りボタン１０２が設けられている。戻りボタン１０２が押されると、ＡＴＭの操作手順が一つ前の操作手順に戻る。例えば、図１５(ａ)に示すように、操作手順が手順番号“２”まで進み、注視領域８０にて入力データ欄８７ｂが表示されている場合

Petitioner Exhibit 1002-3109

において、戻りボタン１０２が押されたとする。
【０１００】すると、手順表示８２が画面の下側へスクロールし、図１５(ｂ)に示すように、一つ前の操作手順である手順番号“１”が示された入力データ欄８７ａを注視領域８０にて表示する状態となる。このとき、入力データ欄８７ａの入力データ表示領域７４には、既に入力したデータが表示される。
【０１０１】上述した機能は、以下のようにして実現される。即ち、各操作手順において入力されたデータは、図１に示す処理制御装置２０の図示せぬ記憶装置に保持される。戻りボタン１０２が押されると、割込み信号が入力装置２ａから割込み処理部２３に入力される。割込み処理部２３は、割込み信号に従って、操作手順を一つ前に戻す旨の命令(手順回帰命令)を表示データ処理部２１に与える。表示データ処理部２１は、手順回帰命令に従って、取引画面７０の内容を一つ前の操作手順に戻すとともに、図示せぬ記憶装置から該当する入力データを読み出してディスプレイ装置１に表示させる。なお、図示せぬ記憶装置に保持された利用者の入力データは、取引(ＡＴＭの操作)が終了すると消去される。
【０１０２】また、戻りボタン１０２が押された場合には、説明表示８３及び入力パネル表示８４が、一つ前の操作手順に対応するものへ変更される。このとき、利用者が修正ボタン１０１を押せば、変更された入力パネル表示８４を用いて既に入力したデータの修正を行うことができる。また、変更された入力パネル表示８４に設けられた戻りボタン１０２が押されると、操作手順がさらに一つ前に戻る。従って、利用者は、既に行った操作手順の何れにも操作手順を戻すことができる。
【０１０３】このように、実施形態１のＡＴＭによれば、戻りボタン１０２を設けることによって、操作手順を既に行った操作手順に戻すことができる。また、操作手順を戻した際には、既に入力したデータが注視領域８０に表示される。このため、既に行った操作手順の確認・やり直しを操作手順毎に行うことができる。従って、ＡＴＭの利用者の操作性が向上を図ることができ、ひいては、利用者の誤操作や誤入力を回避することができる。データ入力のやり直しができる点で、特に習熟度の低い利用者に対する安心感を与えることができる。
【０１０４】また、戻りボタン１０２は、入力パネル表示８４の種類に拘わらず同一の位置(入力パネル表示８４の右上コーナー)に設けられている。このため、ＡＴＭの利用者は、戻りボタン１０２の位置を特に意識しなくても覚えることができる。従って、利用者は、操作手順を既に行った手順に戻したい場合には、適正に戻りボタン１０２を押すことができる。
〈ヘルプ表示〉図１６は、取引画面７０に表示されるヘルプ表示(解説画面)１０６の説明図である。図１６に示すように、ヘルプ表示１０６は、ＡＴＭの利用者が行うべき操作を示すものであり、入力パネル表示８４の上に重ねて表示される。ヘルプ表示１０６は、取引画面７０の画面要素に対する処理と同様の処理によってディスプレイ装置１に表示される。
【０１０５】図１６には、ヘルプ表示１０６の例として、カードの差込口を解説する画像が表示されている。このヘルプ表示１０６は、画面遷移が終了した際に所定時間表示され、所定時間が経過すると取引画面７０から消える。なお、ヘルプ表示１０６には、図示はしないが、文字列からなるものも用意されている。
〈快速表示ボタン及び丁寧説明ボタン〉図１０～図１２，及び図１６に示すように、入力パネル表示８４の左下コーナーには、快速表示ボタン１０７及び丁寧説明ボタン１０８が設けられている。快速表示ボタン１０７が押されると、各操作手順が通常モードから快速モードへ変更される。即ち、各操作手順におけるヘルプ表示１０６の表示回数が低減されるとともに、画面遷移が高速で行われる状態となる。なお、快速モードへの変更は、制御部ＣＰＵに保持されている熟練者フラグがＯＮとされることで行われる。
【０１０６】これに対し、丁寧説明ボタン１０８が押されると、各操作手順が通常モードから詳細モードへ変更される。即ち、画面遷移の様子が通常モードの場合よりも低速で表示されるとともに、各操作手順におけるヘルプ表示１０６の表示回数，種類が増加する。また、操作に関する詳細説明の文字列が取引画面７０に適宜表示される状態となる。
【０１０７】なお、快速モードの際に快速表示ボタン１０７が押されると、快速モードが通常モードへ戻る。また、詳細モードの際に快速表示ボタン１０７が押されると、詳細モードが快速モードへ変更される。一方、詳細モードの際に丁寧表示ボタン１０８が押されると、詳細モードが通常モードへ戻る。また、快速モードの際に丁寧表示ボタン１０８が押されると、快速モードが詳細モードへ変更される。
【０１０８】このように、快速表示ボタン１０７及び丁寧説明ボタン１０８が設けられているので、利用者はその習熟度に応じたモードを選択してＡＴＭを操作できる。快速モードで操作を行うことにより操作時間の短縮を図ることができる。また、詳細モードで操作を行うことにより、確実かつ正確に操作を行うことができ、操作ミスやデータ入力ミスの発生を回避できる。
〔ＡＴＭの操作手順〕図１７は、上述したＡＴＭにおける操作手順の概念図であり、図１８は、ＡＴＭにおける操作手順の例を示す図である。図１７に示すように、実施形態１におけるＡＴＭは、各取引の操作手順が複階層化されている。具体的には、操作手順は、メイン手順層(最短シーケンス)，選択手順層(サブシーケンス)，及び詳細手順層(サブシーケンス)から構成されている。
【０１０９】メイン手順層は、最短の手順(必要最小限の手順)からなる。選択手順層は、利用者の選択によっ

Petitioner Exhibit 1002-3110

て操作手順に加えられる手順からなる。詳細手順層は、選択手順層における各手順をさらに詳細化した複数の手順からなり、利用者の選択によって操作手順に加えられる。このように、操作手順が複階層化され、選択手順層及び詳細手順層に属する手順を操作手順に加えるか否かが利用者の選択にゆだねられているので、利用者は自身の習熟度に応じた手順でＡＴＭの操作(取引)を行うことができる。

【０１１０】図１８には、「振込」の取引における操作手順が示されている。この操作手順は、制御部ＣＰＵが画面作成処理によって生成した取引画面７０をディスプレイ１に表示させることによって、利用者に対して提供される。図１８において、「振込先入力」の手順(図１８参照)は、利用者が振込カードを有していれば、その内容が記録されているので省略可能な手順である。

【０１１１】この「振込先入力」の手順は、振込先の「金融機関の選択」「支店名の入力」及び「口座番号の入力」という３つの手順からなる。ところで、「振込先入力」の手順は、「振込」の取引に慣れた利用者であれば一つの手順として処理することが可能である。

【０１１２】このため、ディスプレイ装置１の取引画面７０には、制御部ＣＰＵによって、省略される手順(「金融機関の選択」「支店名の入力」及び「口座番号の入力」)が表示されるとともに、一度に処理できる手順として「振込先入力」の手順が表示される。さらに、省略される手順と「振込先入力」の手順との一方を選択する旨が表示される。

【０１１３】ここで、「振込先入力」の手順が選択された場合には、利用者が「振込先入力」の手順における操作を行った後、操作手順を次の「振込金入力」の手順へ進めることとなる。これに対し、省略される手順が選択された場合には、利用者は「金融機関の選択」「支店名の入力」及び「口座番号の入力」の各手順における操作(図１８参照)を経て、操作手順を次の「振込金入力」へ進めることとなる。

【０１１４】また、「金融機関選択」の手順が終了すると、次の手順を「支店名入力」の手順で行うか、「支店名頭文字入力」及び「支店名選択」の手順で行うかの選択指示が制御部ＣＰＵの処理によってディスプレイ装置１に表示される。これに対し、利用者は、何れか一方を選択して操作手順を進めていくこととなる。

【０１１５】このように、複数の操作からなる複雑な手順を、単純な複数の手順として処理することが可能となっている。従って、習熟度の高い利用者には最短の手順を提供し、習熟度の低い利用者には詳細な手順を踏んでＡＴＭの操作を行わせることができる。

【０１１６】また、各手順に対応づけて、手順における操作や入力対象の意味を示す「解説」のヘルプ表示１０６(図１８参照)が用意されており、各「解説」のヘルプ表示１０６は、図示せぬ手順選択指示とともにディスプレイ装置１に表示される。これによって、利用者は、手順の選択を慎重且つ適正に行うことができる。

【０１１７】以上説明したように、実施形態１によるＡＴＭによれば、ＡＴＭの利用者は自身の操作の習熟度に応じた操作手順でＡＴＭの操作を行うことができるので、ＡＴＭの操作性が向上する。

〔実施形態２〕次に実施形態２による自動取引装置(ＡＴＭ)を説明する。但し、実施形態２によるＡＴＭは、実施形態１によるＡＴＭとほぼ同様であるので、相違する点についてのみ説明する。

【０１１８】図１９は、実施形態２によるＡＴＭのディスプレイ装置１に表示される取引画面７０の一部を示す説明図である。なお、実施形態１における構成要素と同一の構成要素については同一の符号を付してある。図１９において、背景８１及び手順表示８２の上には、説明表示１８３及び入力パネル表示１８４が表示されている。説明表示１８３は、操作説明を示す文字列を除いて半透明で表示されている。また、入力パネル表示８４は、５０音キー群９４を除いて半透明で表示されている。

【０１１９】このため、ＡＴＭの利用者は、半透明な説明表示１８３及び入力パネル表示１８４を介してこれらの背後に存する手順表示８２の表示内容を見ることができる。従って、各入力データ欄８７に表示された既に入力結果の確認，入力を要求される入力対象の全体像の認識することができる。

【０１２０】実施形態２によれば、ＡＴＭの利用者は、手順表示８２の表示内容を説明表示１８３及び入力パネル表示１８４を介して見ることができる。このため、利用者は、実施形態１に比べて手順表示８２の表示内容をより適正に把握することができる。また、説明表示１８３及び入力パネル表示１８４を半透明とすることで、従来一画面で納まらなかった情報を一画面で表示することが可能となるので、複雑な内容の情報，或いは多量の情報を一画面で表示できる。従って、操作手順の短縮化を図ることができる。

【０１２１】なお、実施形態２では、説明表示１８３及び入力パネル表示１８４を半透明で表示する構成としたが、説明表示１８３又は入力パネル表示１８４の一方のみが半透明で表示される構成となっていても良い。

〔実施形態３〕次に、実施形態３によるＡＴＭを説明する。実施形態３によるＡＴＭは、実施形態１によるＡＴＭとほぼ同様であるので、共通点については説明を省略し、相違点について説明する。

【０１２２】図２０は、実施形態３によるＡＴＭの構成を示すブロック図である。但し、実施形態１と同一の構成要素については、同一の符号を付して説明を省略する。制御部ＣＰＵは、実施形態１にて説明した構成に加え、時間を計測するタイマＡ及びタイマＢを有している。この制御部ＣＰＵは、利用者のＡＴＭの操作の習熟

Petitioner Exhibit 1002-3111

度を判定する処理(習熟度判定処理)を行う。

【０１２３】習熟度判定処理は、利用者によるデータ入力の速さを測ることによって行われる。例えば、利用者が数字(暗証番号，口座番号等)を入力する場合には、利用者が４桁の数字を入力するまでの所用時間によって習熟度の高低を判定する。或いは、任意の数字入力があってからその数字入力を修正する修正キーが押されるまでの時間によって習熟度の高低を判定する(数字入力による習熟度判定処理)。

【０１２４】また、５０音の文字(受取人，依頼人等)入力の場合には、文字の入力時間間隔によって習熟度の高低を判定する。或いは、任意の文字入力があってからその文字入力を修正する修正キーが押されるまでの時間によって習熟度の高低を判定する(文字入力による習熟度判定処理)。

【０１２５】また、習熟度判定処理は、利用者の金融用語の知識度を測ることによって行われる。例えば、特定の金融用語がディスプレイ装置１に表示されてから、入力パネル表示８４の何れかのキーが押されるまでの時間によって習熟度の高低を判定する。特定の金融用語には、例えば、「普通」「当座」「振込カード」「現金振込」「口座振込」等の金融用語が挙げられる(用語による習熟度判定処理)。

【０１２６】図２１は、実施形態３における制御部ＣＰＵによる習熟度判定処理を示すフローチャートである。図２１において、習熟度判定処理は、制御部ＣＰＵがＡＴＭのディスプレイ装置１に取引画面７０が表示されることによってスタートする。但し、ここでは、上述した数字入力による判定処理を行うものとし、取引画面７０として、図示せぬ暗証番号入力画面(暗証番号を入力する操作手順にて表示される取引画面７０)がディスプレイ装置１に表示されたものとする。

【０１２７】ステップＳ１０１では、制御部ＣＰＵは、タイマＡ及びタイマＢをストップし、且つリセット(クリア)した後、処理をステップＳ１０２へ進める。ステップＳ１０２では、制御部ＣＰＵは、図示せぬ暗証番号入力画面に表示されたテンキーの何れかが押されるのを待機する。その後、制御部ＣＰＵは、テンキーの何れかが押されたと判定した場合(ステップＳ０１２；ＹＥＳ)には、処理をステップＳ１０３へ進める。制御部ＣＰＵは、ステップＳ１０３へ処理を進めた場合には、タイマＢをストップした後、処理をステップＳ１０４へ進める。

【０１２８】ステップＳ１０４では、制御部ＣＰＵは、ステップＳ１０２にて押されたキーによって４桁の暗証番号の１桁目の番号が入力されたのか否かを判定する。このとき、制御部ＣＰＵは、１桁目の番号が入力されたと判定した場合(ステップＳ１０４；ＹＥＳ)には、処理をステップＳ１０５へ進め、タイマＡによる計時をスタートさせる。その後、制御部ＣＰＵは、処理をステップＳ１０２へ戻し、再び図示せぬ暗証番号入力画面に表示されたテンキーが押されるのを待機する。これに対し、制御部ＣＰＵは、１桁目の番号が入力されたのではないと判定した場合(ステップＳ１０４；ＮＯ)には、処理をステップＳ１０６へ進める。

【０１２９】制御部ＣＰＵは、ステップＳ１０６へ処理を進めた場合には、ステップＳ１０２にて押されたキーによって４桁の暗証番号の４桁目の番号が入力されたのか否かを判定する。このとき、制御部ＣＰＵは、４桁目の番号が入力されたと判定した場合(ステップＳ１０６；ＹＥＳ)には、処理をステップＳ１１１へ進める。これに対し、制御部ＣＰＵは、４桁目の番号が入力されたのではないと判定した場合(ステップＳ１０６；ＮＯ)には、処理をステップＳ１０７へ進める。

【０１３０】制御部ＣＰＵは、ステップＳ１０７へ処理を進めた場合には、図示せぬ暗証番号入力画面に表示された修正キーが押されたか否かを判定する。このとき、制御部ＣＰＵは、修正キーが押されなかったと判定した場合(ステップＳ１０７；ＮＯ)には、処理をステップＳ１０８へ進め、タイマＢによる計時をスタートさせる。その後、制御部ＣＰＵは、処理をステップＳ１０２へ戻し、再び図示せぬ暗証番号入力画面に表示されたテンキーが押されるのを待機する。これに対し、制御部ＣＰＵは、修正キーが押されたと判定した場合(ステップＳ１０７；ＹＥＳ)には、処理をステップＳ１０９へ進める。

【０１３１】制御部ＣＰＵは、ステップＳ１０９へ処理を進めた場合には、ステップＳ１０３にてストップさせたタイマＢの計時時間(ある数字を入力しその誤りに気付いて修正キーを押すまでの時間)を参照し、その計時時間が規定値以下であるか否かを判定する。このとき、制御部ＣＰＵは、規定値以下でないと判定した場合(ステップ１０９；ＮＯ)には、処理をステップＳ１０８へ進める。これに対し、制御部ＣＰＵは、規定値以下であると判定した場合(ステップＳ１０９；ＹＥＳ)には、処理をステップＳ１１０へ進める。

【０１３２】制御部ＣＰＵは、ステップＳ１１０へ処理を進めた場合には、利用者は操作の熟練者であるものとして、実施形態１にて説明した熟練者フラグをＯＮとする。その後、制御部ＣＰＵは、処理をステップＳ１０８へ進める。一方、制御部ＣＰＵは、ステップＳ１０６にてＹＥＳの判定を行い、処理をステップ１１１へ進めた場合には、タイマＡによる計時をストップする。その後、制御部ＣＰＵは、処理をステップＳ１１２へ進める。

【０１３３】ステップＳ１１２では、制御部ＣＰＵは、ステップＳ１１１にてストップさせたタイマＡの計時時間(４桁の暗証番号入力に要した時間)を参照し、その計時時間が規定値以下であるか否かを判定する。このとき、制御部ＣＰＵは、規定値以下でないと判定した場合

Petitioner Exhibit 1002-3112

(ステップ１０９；NO)には、習熟度判定処理を終了させる。これに対し、制御部ＣＰＵは、規定値以下であると判定した場合(ステップＳ１０９；ＹＥＳ)には、処理をステップＳ１１３へ進める。

【０１３４】制御部ＣＰＵは、ステップＳ１１３へ処理を進めた場合には、利用者は操作の熟練者であるものとして、実施形態１にて説明した熟練者フラグをＯＮとする。その後、制御部ＣＰＵは、習熟度判定処理を終了させる。この習熟度判定処理が終了すると、制御部ＣＰＵ(中央処理部３)は、次の取引画面７０をディスプレイ装置１に表示させる処理を開始する。

【０１３５】熟練者フラグがＯＮとなることによって、実施形態１にて説明したように、快速表示ボタン１０７が押された場合と同じ状態，即ち、画面遷移が高速で行われるとともに、ヘルプ表示１０６の表示回数が低減される。

【０１３６】また、文字入力による習熟度判定処理は、図２１に示したフローチャートと同一の処理によって実現される。但し、文字入力による習熟度判定処理では、５０音の入力パネル表示８４ｃを含む取引画面７０がディスプレイ装置１に表示されることによって処理がスタートする。また、タイマAは、ある文字データが４文字分入力されるまでの時間を計時する。また、タイマＢは、利用者が任意の文字データを入力してからその誤りに気付いて修正キー１０１を押すまでの時間を計時する。そして、ステップＳ１０９及びステップＳ１１２の各処理において用いられる規定値は、数字入力による習熟度判定処理の場合と異なる値で設定される。

【０１３７】図２２は、用語による習熟度判定処理を示すフローチャートである。この判定処理は、特定の用語を入力するためのキーが配置された入力パネル表示８４を含む取引画面７０がディスプレイ装置に表示されることによってスタートする。

【０１３８】処理がスタートすると、制御部ＣＰＵは、タイマAをストップし、且つリセット(クリア)し(ステップＳ２０１)、その後、タイマAによる計時をスタートさせる(ステップＳ２０２)。続いて、制御部ＣＰＵは、特定の用語を入力するためのキーが押されたか否かを判定する(ステップＳ２０３)。このとき、制御部ＣＰＵは、該当するキーが押されたと判定した場合(ステップＳ２０３；ＹＥＳ)には、処理をステップＳ２０４へ進める。これに対し、該当するキーが押されていないと判定した場合(ステップＳ２０３；NO)には、このステップＳ２０３にてＹＥＳの判定がなされるまで、ステップＳ２０３の処理が繰り返し行われる。

【０１３９】制御部ＣＰＵは、ステップＳ２０４へ処理を進めた場合には、タイマAによる計時をストップさせる。続いて、制御部ＣＰＵは、タイマAの計時時間を参照し、その計時時間が規定値以下であるか否かを判定する。このとき、制御部ＣＰＵは、規定値以下でないと判定した場合(ステップ２０５；NO)には、この判定処理を終了させる。これに対し、制御部ＣＰＵは、規定値以下であると判定した場合(ステップＳ２０５；ＹＥＳ)には、処理をステップＳ２０６へ進める。

【０１４０】制御部ＣＰＵは、ステップＳ２０６へ処理を進めた場合には、利用者は操作の熟練者であるものとして、実施形態１にて説明した熟練者フラグをＯＮとする。その後、制御部ＣＰＵは、この判定処理を終了させる。

【０１４１】実施形態３による効果は、実施形態１による効果とほぼ同様である。但し、ＡＴＭの利用者の操作の習熟度を判定し、習熟度が高い場合には、操作手順を省略する。従って、習熟度が高い利用者は、簡略化された操作手順によってＡＴＭを操作でき、習熟度の低い利用者は、詳細な操作手順によってＡＴＭを操作できる。即ち、実施形態３によれば、利用者の習熟度に応じた操作手順を自動的に提供できる。従って、多くの利用者が快適にＡＴＭを操作することが可能となる。

【０１４２】なお、上述した各習熟度判定処理にて用いられた各規定値は、適宜設定可能である。従って、地域差による操作の習熟度の差を吸収できる。例えば、都市部のターミナル駅近傍等では、ＡＴＭの操作に熟練した利用者が多いので、各規定値をローカルな地域に比べて短い時間で設定する。一方、ローカルな地域では、都市部に比べてＡＴＭの操作に熟練した利用者が少ないので、各規定値を都市部に比べて長い時間で設定する。

〔実施形態４〕次に、実施形態４によるＡＴＭを説明する。従来における自動取引装置は、画面遷移させた後、入力が所定時間ない場合には、取引処理全体をキャンセルするタイムアウト時間を定義し、このタイムアウト時間を基づいて、画面遷移後タイムアウト前の適当な時間前(例えば５秒前)にアラームを鳴らして入力を催促していた。その後も入力がない場合には、自動取引装置は、タイムアウト時間がくると同時に取引を強制終了させていた。

【０１４３】このような対応方法は、利用者が自動取引装置の操作を途中で中断して不在になった場合や、利用者が意図的にタイムアウトによる強制終了を実行する場合には有効である。ところが、利用者が何をしてよいか理解できず入力を行うことができない場合等では、催促アラームは利用者を混乱させるのみとなることがあった。この場合には、利用者に催促アラームによって慌てさせられたためできることもできなくなってしまったという不満，或いは、機械に使われているという感覚が与えてしまう場合があった。

【０１４４】実施形態４によるＡＴＭは、上記問題に鑑みなされたものである。但し、実施形態４によるＡＴＭは、実施形態１によるＡＴＭとほぼ同様の構成を有しているので、共通点については説明を省略し、相違点について説明する。図２３は、実施形態４における制御部Ｃ

Petitioner Exhibit 1002-3113

ＰＵによる処理(タイムアウト処理)を示すフローチャートである。

【０１４５】このタイムアウト処理は、取引画面７０の画面遷移が完了することによってスタートする。最初に、制御部ＣＰＵは、自身が保持する図示せぬ入力監視タイマを起動させる(ステップＳ３０１)。続いて、制御部ＣＰＵは、入力装置２ａからキー入力があったか否かを判定する(ステップＳ３０２)。このとき、制御部ＣＰＵは、キー入力があったと判定した場合(ステップＳ３０２；ＹＥＳ)には、タイムアウト処理を終了させ、次の処理を開始する。これに対し、制御部ＣＰＵは、キー入力が無いと判定した場合(ステップＳ３０２；ＮＯ)には、処理をステップＳ３０３へ進める。

【０１４６】制御部ＣＰＵは、処理をステップＳ３０３へ進めた場合には、図示せぬ入力監視タイマが、予め設定されているタイムアウト時間を計時し、タイムアウトが発生したか否かを判定する。このとき、制御部ＣＰＵは、タイムアウトが発生したと判定した場合(ステップＳ３０３；ＹＥＳ)には、取引を強制終了させて、このタイムアウト処理を終了させる。これに対し、制御部ＣＰＵは、タイムアウトが発生していないと判定した場合(ステップＳ３０３；ＮＯ)には、処理をステップＳ３０４へ進める。

【０１４７】制御部ＣＰＵは、処理をステップＳ３０４へ進めた場合には、図示せぬ入力監視タイマを起動させてから１０秒経過していない否かを判定する。このとき、制御部ＣＰＵは、１０秒経過していないと判定した場合(ステップＳ３０４；ＹＥＳ)には、音声出力部６０(図３参照)へ動作命令を与え、注意喚起音を発生させる(ステップＳ３０５)。その後、制御部ＣＰＵは、処理をステップＳ３０２へ戻す。これに対し、制御部ＣＰＵは、１０秒経過していると判定した場合(ステップＳ３０４；ＮＯ)には、処理をステップＳ３０６へ進める。

【０１４８】制御部ＣＰＵは、処理をステップＳ３０６へ進めた場合には、図示せぬ入力監視タイマを起動させてから１５秒経過していないか否かを判定する。このとき、制御部ＣＰＵは、１５秒経過していないと判定した場合(ステップＳ３０６；ＹＥＳ)には、ディスプレイ装置１の取引画面７０上にヘルプ表示１０６を表示させる(ステップＳ３０７)。その後、制御部ＣＰＵは、処理をステップＳ３０２へ戻す。これに対し、制御部ＣＰＵは、１５秒経過していると判定した場合(ステップＳ３０６；ＮＯ)には、処理をステップＳ３０８へ進める。

【０１４９】制御部ＣＰＵは、処理をステップＳ３０８へ進めた場合には、図示せぬ入力監視タイマを起動させてから２０秒経過していないか否かを判定する。このとき、制御部ＣＰＵは、２０秒経過していないと判定した場合(ステップＳ３０８；ＹＥＳ)には、処理をステップＳ３１１へ進める。これに対し、制御部ＣＰＵは、２０秒経過していると判定した場合(ステップＳ３０８；ＮＯ)には、処理をステップＳ３０９へ進める。

【０１５０】制御部ＣＰＵは、処理をステップＳ３０９へ進めた場合には、図示せぬ入力監視タイマがタイムアウト時間を計時する５秒前であるか否かを判定する。このとき、制御部ＣＰＵは、５秒前であると判定した場合(ステップＳ３０９；ＹＥＳ)には、音声出力部６０に動作命令を与え、警告アラームを発生させる。その後、制御部ＣＰＵは、処理をステップＳ３０２へ戻す。これに対し、制御部ＣＰＵは、５秒前でないと判定した場合(ステップＳ３０８；ＮＯ)には、処理をステップＳ３０２へ戻す。

【０１５１】一方、制御部ＣＰＵは、処理ステップＳ３１１へ進めた場合には、ディスプレイ装置１における取引画面７０上にタイムアウト予告(例えば、「あと数秒でタイムアウトとなり取引を強制終了します」の文字列等)を表示させるとともに、音声出力部６０にタイムアウトが発生する旨の音声案内を出力させる。続いて、制御部ＣＰＵは、図示せぬサスペンドボタン(タイムアウト時間を延長するためのボタン)，及び図示せぬ指示表示(例えば、「取引を継続したい場合にはサスペンドボタンを押して下さい」等の文字列)を、取引画面７０上に表示させる。

【０１５２】その後、制御部ＣＰＵは、所定時間図示せぬサスペンドボタンからの入力を受け付ける状態となり、所定時間が経過すると、図示せぬサスペンドボタンが押されたか否かを判定する(ステップＳ３１３)。このとき、制御部ＣＰＵは、図示せぬサスペンドボタンが押されなかったと判定した場合(ステップＳ３１３；ＮＯ)には、処理をステップＳ３０９へ進める。これに対し、制御部ＣＰＵは、図示せぬサスペンドボタンが押されたと判定した場合(ステップＳ３１３；ＹＥＳ)には、処理をステップＳ３０４へ戻す。これによって、制御部ＣＰＵがステップＳ３０３の処理をジャンプする状態となるので、次のステップＳ３０３の処理が行われるまでの間、タイムアウト時間が延長されることとなる。

【０１５３】実施形態４によるＡＴＭによると、画面遷移が行われてから入力装置２ａに対してデータ入力がなされない場合には、ＡＴＭは、第１段階として注意喚起音を発生し、第２段階としてディスプレイ装置１に操作方法説明表示(ヘルプ表示１０６)を表示し、第３段階としてタイムアウト発生予告の表示及び音声案内を行い、第４段階としてタイムアウトの警告アラームを発生する。このように、タイムアウトの情報を段階的にＡＴＭの利用者に対して提供するので、利用者が心理的圧迫感を受けることなく操作を行うことができる。

【０１５４】また、ヘルプ表示１０６を表示することで、操作知識の不足している利用者に対する救済を与えるので、タイムアウトが発生して取引が強制終了してしまう可能性を低減することができる。さらに、図示せぬサスペンドボタンを設け、このボタンを押すことでタイ

Petitioner Exhibit 1002-3114

ムアウトまでの時間が延長される構成としたので、利用者に対しＡＴＭの操作方法の理解に努める猶予を与えることができる。従って、タイムアウト時間となれば必然的に強制終了してしまう従来の自動取引装置に比べ、利用者に対して満足感を与えることができる。

〔実施形態５〕次に、実施形態５によるＡＴＭを説明する。従来における自動取引装置では、取引画面が切り替わる際にシグナル音等の注意喚起音が無かったので、取引画面の切り替わりが終了したことや、データを入力可能な状態となったことにＡＴＭの利用者が気付かない場合があり、取引に時間を要してしまう場合があった。

【０１５５】このことに鑑み、従来における自動取引装置では、取引画面の切り替え完了やデータ入力可能であることを利用者に伝達するため、取引画面の文字を大きく表示したり、文字を点滅させることで利用者の注意を喚起していたが、利用者がディスプレイ装置に注目していない場合には、これらのシグナルを見逃すこととなり、十分ではなかった。

【０１５６】実施形態５によるＡＴＭは、上述した問題に鑑みなされたものである。実施形態５によるＡＴＭは、実施形態１によるＡＴＭとほぼ同様であるので、共通点については説明を省略し、相違点について説明する。図２４は、実施形態５におけるＡＴＭの制御部ＣＰＵによる処理(注意喚起処理)を示すフローチャートである。

【０１５７】この注意喚起処理は、操作手順の何れかが終了することによってスタートする(ステップＳ４０１)。制御部ＣＰＵは、処理をステップＳ４０２へ進めると、取引画面７０の書き換え処理を行う。即ち、ディスプレイ装置１に実施形態１にて説明した画面遷移を表示させるための内部処理(画面表示処理：図４参照)を行う。

【０１５８】続いて、制御部ＣＰＵは、ディスプレイ装置１に対して取引画面７０のデータ(ビデオ信号)を転送し、次の操作手順における取引画面７０を表示させる(ステップＳ４０３)。このステップＳ４０３の処理によって取引画面７０がディスプレイ装置１に表示されると、制御部ＣＰＵは、音声出力部６０に動作命令を与え、シグナル音を発生させる(ステップＳ４０４)。そして、制御部ＣＰＵは、利用者がデータ入力可能な状態，即ち、入力装置２ａからの信号を待機する状態となる(ステップＳ４０５)。

【０１５９】実施形態５によるＡＴＭによると、取引画面７０の画面遷移の際にシグナル音を発生させるので、利用者を取引画面７０に注目させることができる。また、シグナル音発生に続いてデータ入力を可能な状態とするので、利用者は、シグナル音の発生を契機としてＡＴＭに対するデータ入力を開始することができる。このため、利用者によるＡＴＭの操作時間の短縮を図ることができ、ひいては金融機関における顧客の稼働率向上に寄与することもできる。

〔実施形態６〕次に、実施形態６によるＡＴＭを説明する。実施形態６によるＡＴＭは、実施形態１によるＡＴＭとほぼ同様であるので、共通点については省略し、相違点についてのみ説明する。

【０１６０】図２５は、顧客操作部ＵＯＰにおける指の引きずり判定処理が示されたフローチャートである。この判定処理は、ディスプレイ装置１に取引画面７０が表示され、データ入力可能な状態となることによってスタートする。

【０１６１】ステップＳ５０１では、入力装置２ａのタッチパネルと接触する物体が検知されたか否かが判定される。このとき、物体が検知された場合(ステップＳ５０１；ＹＥＳ)には、処理がステップＳ５０２へ進む。これに対し、物体が検知されない場合(ステップＳ５０１；ＮＯ)には、ステップＳ５０１にてＹＥＳの判定がなされるまでステップＳ５０１の処理が繰り返し行われる。

【０１６２】ステップＳ５０２へ処理が進んだ場合には、ステップＳ５０１にて検知した物体が検知されたままの状態であり、且つその物体とタッチパネルとの接触位置座標が、ステップＳ５０１にて検知した際における接触位置座標と異なるか否かを判定する。このとき、物体が検知されたままの状態で、且つ接触位置座標が異なる場合(ステップＳ５０２；ＹＥＳ)には、指の引きずりが発生しているものとして、その旨の信号が制御部ＣＰＵへ転送される(ステップＳ５０３)、そして、この判定処理が終了する。

【０１６３】これに対し、物体が検知されたままの状態でない場合，或いは接触位置座標が異ならない場合(ステップＳ５０２；ＮＯ)には、正常に入力パネル表示８４のキー又はボタンの何れかが押されたものとして、その旨の信号が制御部ＣＰＵへ転送される(ステップＳ５０４)。そして、この判定処理が終了する。

【０１６４】図２６は、制御部ＣＰＵによる引きずり警告音発生処理が示されたフローチャートである。この処理は、ディスプレイ装置１に取引画面７０が表示され、データ入力可能な状態となることによってスタートする。

【０１６５】最初に、制御部ＣＰＵは、キー入力を待つ状態となり(ステップＳ５０５)、キー入力があるか否かを判定する(ステップＳ５０６)。即ち、入力装置２ａから信号が転送されてきたか否かを判定する。このとき、入力装置２ａから信号が転送されてきたと判定した場合には、制御部ＣＰＵは、処理をステップＳ５０７へ進める。

【０１６６】制御部ＣＰＵは、処理をステップＳ５０７へ進めた場合には、入力装置２ａから転送されてきた信号が指の引きずり動作を示す信号であるか否かを判定する。このとき、制御部ＣＰＵは、引きずり動作を示す信

Petitioner Exhibit 1002-3115

号でないと判定した場合には、処理をステップＳ５０８へ進め、他の処理を行い、引きずり警告音発生処理を終了させる。これに対し、引きずり動作を示す信号であると判定した場合には、制御部は処理をステップＳ５０９へ進める。

【０１６７】制御部ＣＰＵは、処理をステップＳ５０９へ進めた場合には、音声出力部６０に動作信号を与え、警告を示すシグナル音を発生させる。続いて、制御部ＣＰＵは、ディスプレイ装置１に、例えば「指を引きずっています。画面からはなして下さい」の文字列を含むウインドウを表示させる(ステップＳ５１０)。その後、制御部ＣＰＵは、処理をステップＳ５０６へ戻す。

【０１６８】実施形態６によれば、指の引きずり動作が行われた場合には、シグナル音がなるので、利用者がディスプレイ装置１に注目する。すると、ディスプレイ装置１には、指の引きずりを警告するメッセージが表示されているので、利用者は、入力データに誤りがないかを確認し、誤りがある場合には、修正キー１０１を押して誤りを修正することとなる。このため、指の引きずりによるデータ入力ミスや装置の誤操作を防止することができる。

〔実施形態７〕次に、実施形態７によるＡＴＭを説明する。従来における自動取引装置では、複数の取引画面の夫々は、取引に必要な操作内容に応じて個別に作成されていた。また、複数の取引画面の表示順序は、自動取引装置に搭載されたプロセッサ装置によって、制御プログラムで規定されるシーケンスに従って決定されていた。このため、複数の取引画面の表示順序を変更したい場合には、プログラムを修正する必要があった。また、自動取引装置に入力される入力対象が変更される場合には、プログラムを変更するとともに、取引画面のデータを変更する必要があった。

【０１６９】ところが、自動取引装置の制御プログラムや取引画面のデータは、通常ハードディスクに格納されるため、その変更作業には時間を要し著しく困難であった。実施形態７は、上述した問題に鑑みなされたものである。

【０１７０】図２７は、実施形態７によるＡＴＭの中央処理装置３(制御部ＣＰＵ)を示すブロック図である。但し、実施形態４によるＡＴＭは、実施形態１によるＡＴＭとほぼ同様であるので、同様の構成要素については、同一の符号を付して説明を省略し、相違する点についてのみ説明する。図２７において、中央処理部３は、ハードディスク２４を有している。ハードディスク２４には、画面作成テーブル２５が保持されている。

【０１７１】図２８は、画面作成テーブル２５の説明図である。図２８において、画面作成テーブル２５には、複数の出力データ(図３に示すＨＤ１０に記録された制御プログラム内に規定されているデータであって、取引画面７０をディスプレイ装置１に表示するためのデータ)の夫々に対応する入力対象，説明表示８３，及び入力パネル表示８４が夫々格納されている。この画面作成テーブル２５は、取引画面７０の画面要素のうち、説明表示８３と入力パネル表示８４とは、入力対象に対して１：１の関係で特定され得ることに着目して作成されたものである。また、背景８１は、取引種別が選択されることによって一意的に決定されるので、固定データとして保有されている。

【０１７２】図２９は、図２７に示した処理制御装置２０による処理を示すフローチャートである。図２９において、ステップＳ６０１～Ｓ６０９の処理のうち、ステップＳ６０１～Ｓ６０４の処理，及びステップＳ６０６～Ｓ６０９の処理は、図１に示したステップＳ０１～Ｓ０４，及びステップＳ０６～Ｓ０９の処理と同様であるので説明を省略し、ステップＳ６０５について説明する。

【０１７３】ステップＳ６０５に処理が進んだ場合には、表示データ処理部２１による画面作成処理のサブルーチンがスタートする。図３０は、画面作成処理を示すフローチャートである。画面作成処理がスタートすると、表示データ処理部２１は、最初に、イメージデータ保持部７から取引種別に対応する背景８１のテクスチャデータを受け取る(ステップＳ７０１)。続いて、表示データ処理部８１は、イメージデータ保持部７から取引種別に対応する手順表示８２のテクスチャデータを受け取る(ステップＳ７０２)。

【０１７４】続いて、表示データ処理部２１は、制御プログラムに規定されている出力データに基づいて画面作成テーブル２５を検索し、対応する入力対象を特定する(ステップＳ７０３)。続いて、表示データ処理部２１は、ステップＳ７０３にて特定した入力対象に対応する説明表示８３を特定し、該当する説明表示８３のテクスチャデータをイメージデータ保持部７から読み出す(ステップＳ７０４)。

【０１７５】続いて、表示データ処理部２１は、ステップＳ７０３にて特定した入力対象に対応する入力パネル表示８４を特定し、該当する入力パネル表示８４のテクスチャデータをイメージデータ保持部７から読み出す(ステップＳ７０５)。そして、表示データ処理部２１は、必要な文字データをＣＧ部６から受け取る。すると、画面作成処理が終了し、メインルーチンにおけるステップＳ６０６へ処理が進む。

【０１７６】実施形態７によるＡＴＭによれば、取引画面７０が画面作成テーブル２５の格納内容に基づいて作成されるので、画面作成テーブル２５の格納内容を変更すれば、取引画面７０の表示内容や取引画面７０の表示順序の変更を行うことができる。従って、ＨＤ１０に記録された制御プログラムの内容変更等の必要がない。

【０１７７】

【発明の効果】本発明による自動取引装置によれば、利

Petitioner Exhibit 1002-3116

用者の操作の習熟度に関係なく従来に比べて操作性の向上を図ることができる

【図面の簡単な説明】

【図１】ＡＴＭの主要部を示すブロック図
【図２】ＡＴＭの外観構成図
【図３】ＡＴＭの具体的構成を示すブロック図
【図４】制御部による処理を示すフローチャート
【図５】取引画面の説明図
【図６】取引画面の画面要素の説明図
【図７】手順表示の説明図
【図８】手順表示の説明図
【図９】手順表示の説明図
【図１０】入力パネル表示の説明図
【図１１】入力パネル表示の説明図
【図１２】入力パネル表示の説明図
【図１３】入力パネル表示の説明図
【図１４】確認画面の説明図
【図１５】戻りボタンの説明図
【図１６】ヘルプ表示の説明図
【図１７】操作手順の概念図
【図１８】操作手順の例を示す図
【図１９】実施形態２による取引画面の説明図
【図２０】実施形態３によるＡＴＭの構成を示すブロック図
【図２１】習熟度判定処理を示すフローチャート
【図２２】習熟度判定処理を示すフローチャート
【図２３】タイムアウト処理を示すフローチャート
【図２４】注意喚起処理を示すフローチャート
【図２５】引きずり判定処理を示すフローチャート
【図２６】引きずり警告音発生処理を示すフローチャート
【図２７】実施形態７によるＡＴＭのブロック図
【図２８】画面作成テーブルの説明図
【図２９】画面作成処理を示すフローチャート
【図３０】画面作成処理を示すフローチャート
【図３１】従来技術の説明図
【図３２】従来技術の説明図
【図３３】従来技術の説明図

【符号の説明】

Ａ，Ｂ　タイマ
ＣＰＵ　制御装置
１　ディスプレイ装置
２ａ　入力装置
３　中央処理装置
６　ＣＧ部
７　イメージデータ保持部
８　ＲＯＭ
９　ＲＡＭ
２０　処理制御装置
２１　表示データ処理部
２２　表示制御部
２３　割り込み処理部
２４　ＥＥＰＲＯＭ
２５　画面作成テーブル
７０　取引画面
７１　取引種別表示領域
７２　操作説明領域
７３　入力対象表示領域
７４　入力データ表示領域
７５　操作領域
８０　注視領域
８１　背景
８１ａ　取引種別表示欄
８１ｂ　取消ボタン
８２　手順表示
８３，１８３　説明表示
８４，１８４　入力パネル表示
８７　入力データ欄
９２　第１確認ボタン
１０１　修正ボタン
１０２　戻りボタン
１０５　第２確認ボタン
１０６　ヘルプ表示
１０７　快速表示ボタン
１０８　丁寧説明ボタン

【図２８】

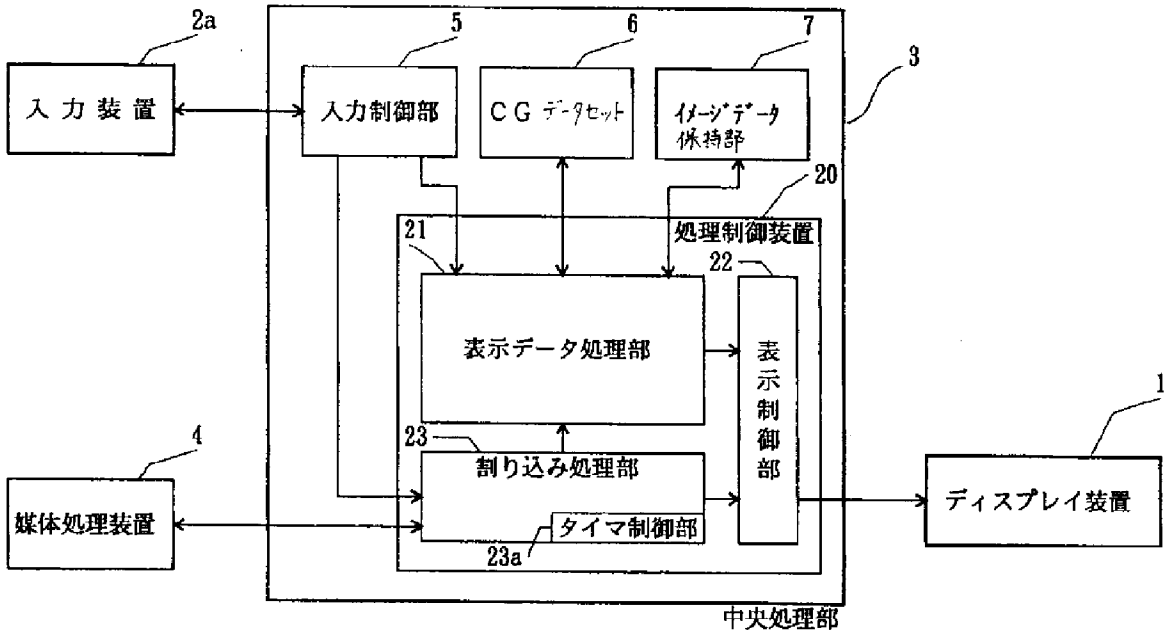
画面作成テーブルの説明図

入力対象種	説明表示種	入力ﾊﾟﾈﾙ表示種	出力データ
振込金額欄			
≈	≈	≈	≈
口座番号	83a	84a	
受取人名	83	84c	
振込金額	83b	84b	

Petitioner Exhibit 1002-3117

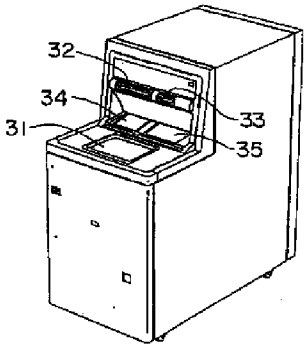
【図１】

ＡＴＭの主要部を示すブロック図



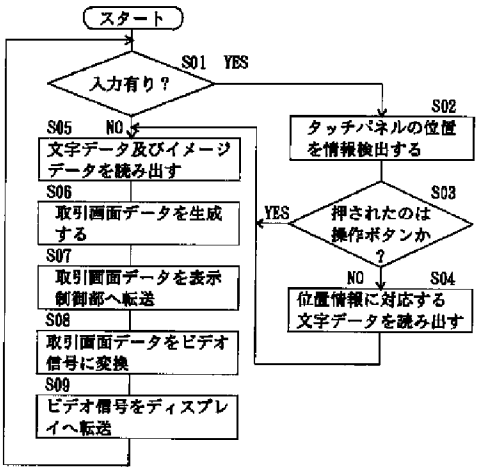
【図２】

ＡＴＭの外観構成図



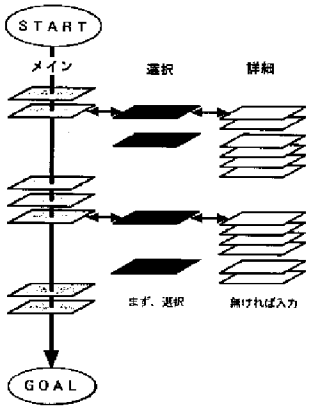
【図４】

制御部による処理を示すフローチャート



【図１７】

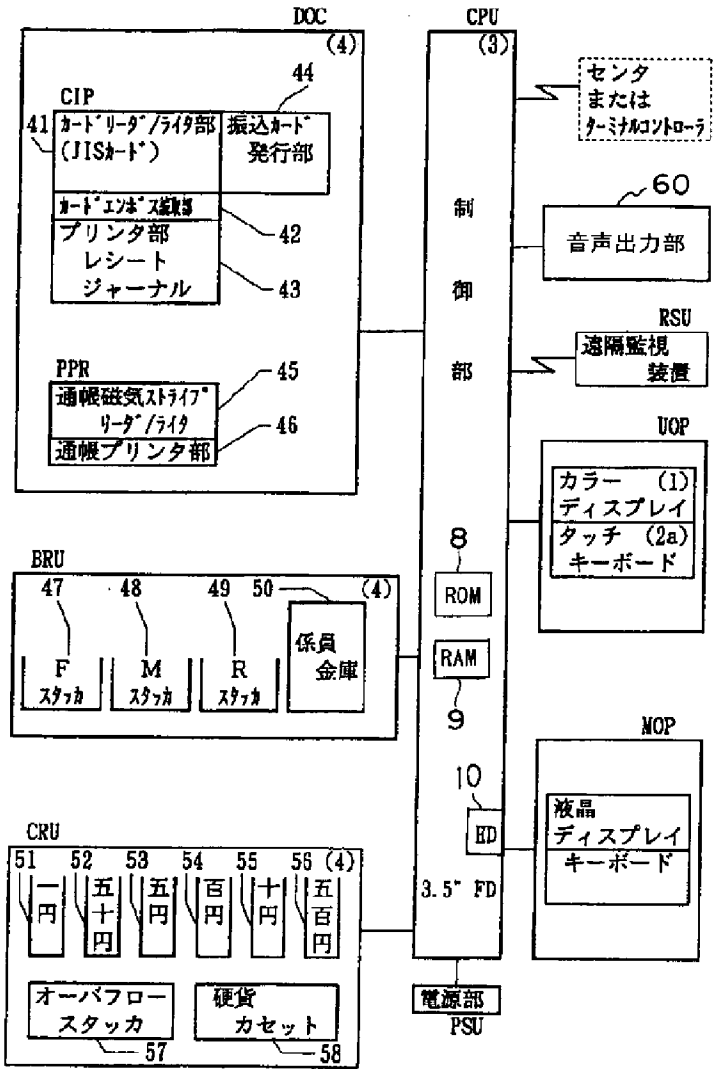
操作手順の概念図



Petitioner Exhibit 1002-3118

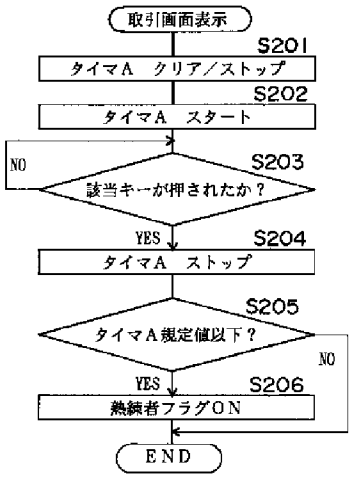
【図３】

ＡＴＭの具体的構成を示すブロック図



【図２２】

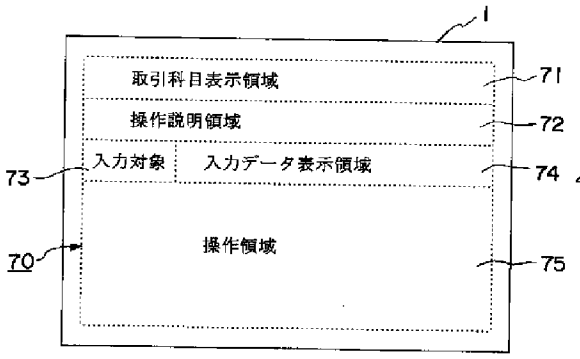
習熟度判定処理を示すフローチャート



Petitioner Exhibit 1002-3119

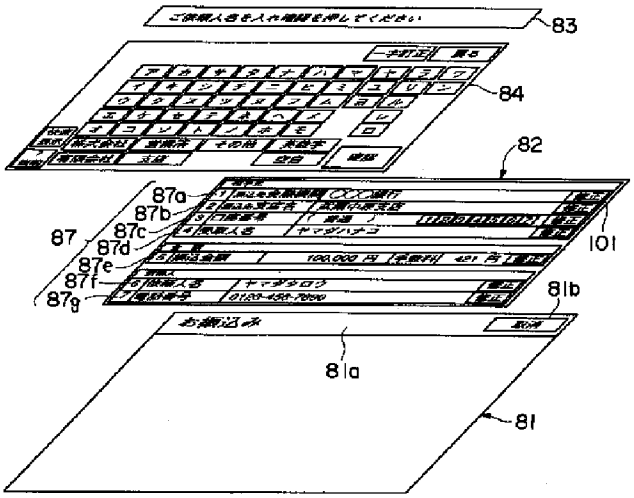
【図５】

取引画面の説明図



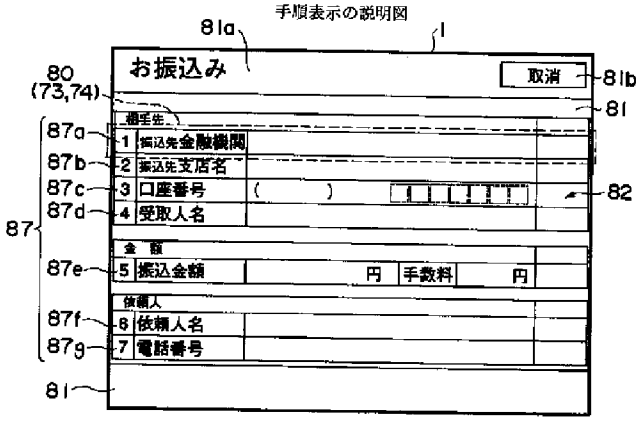
【図６】

取引画面の画面要素の説明図



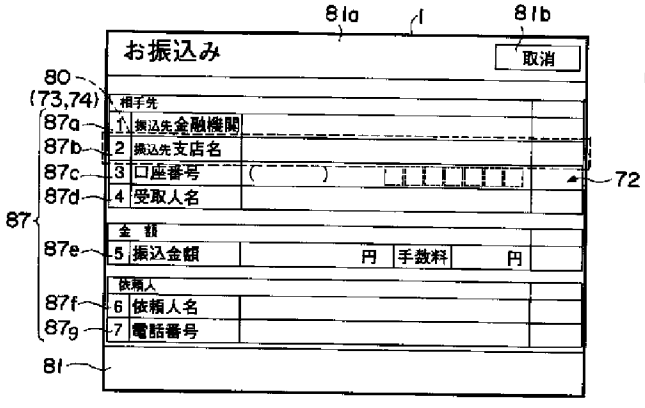
【図７】

手順表示の説明図



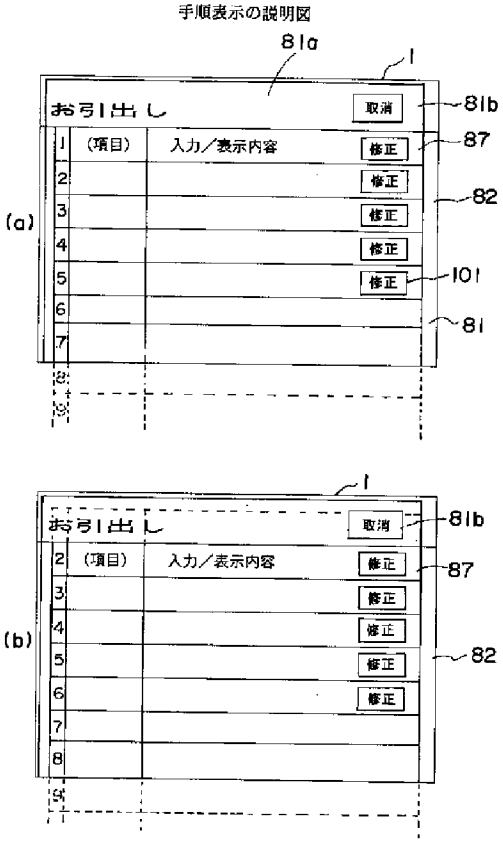
【図８】

手順表示の説明図



【図９】

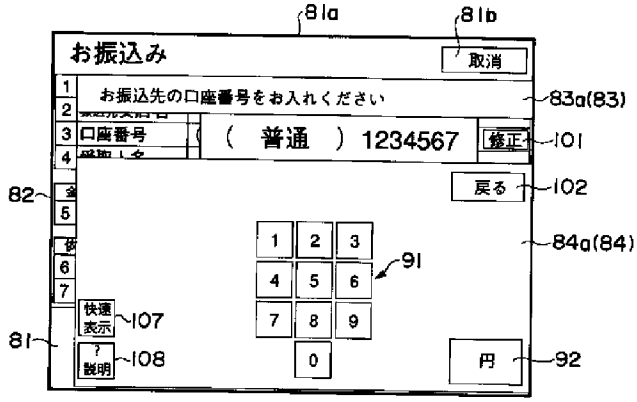
手順表示の説明図



Petitioner Exhibit 1002-3120

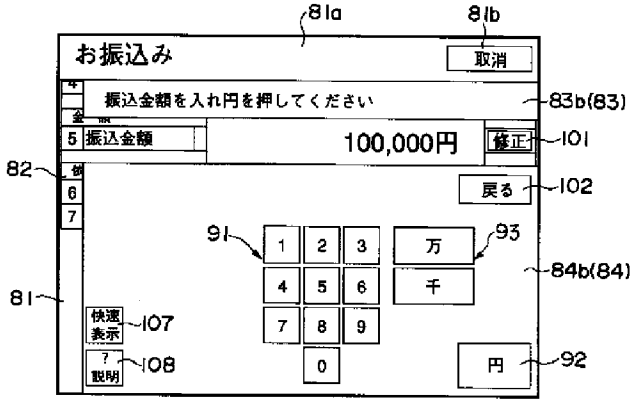
【図１０】

入力パネル表示の説明図



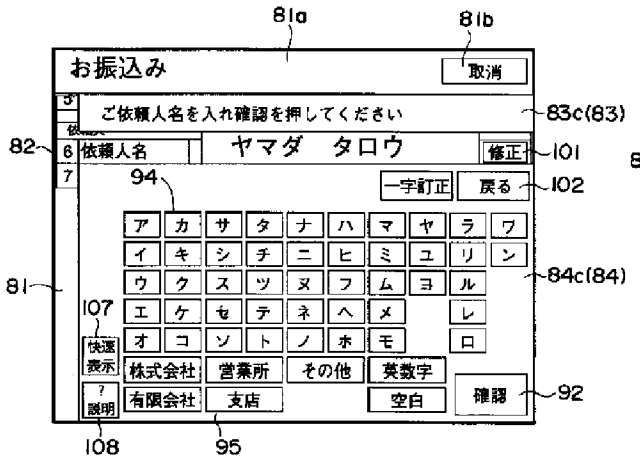
【図１１】

入力パネル表示の説明図



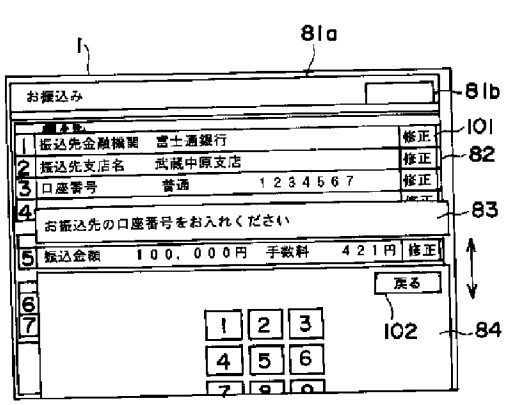
【図１２】

入力パネル表示の説明図



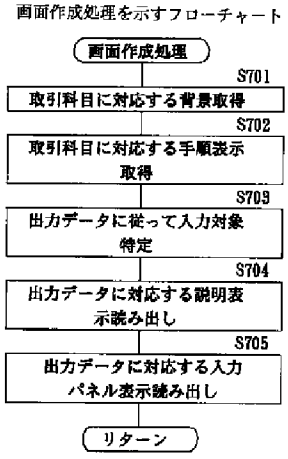
【図１３】

入力パネル表示の説明図



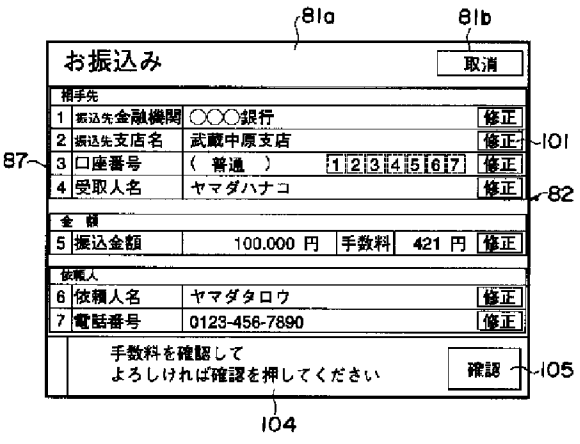
【図３０】

画面作成処理を示すフローチャート



【図１４】

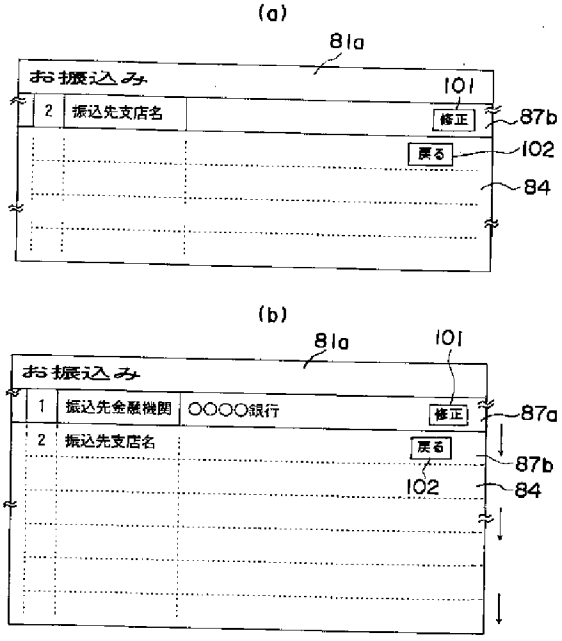
確認画面の説明図



Petitioner Exhibit 1002-3121

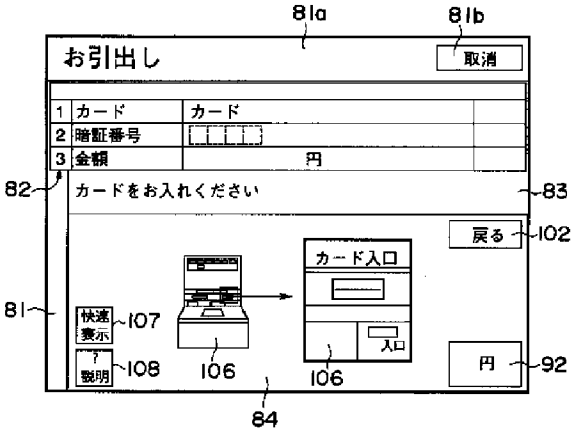
【図１５】

戻りボタンの説明図



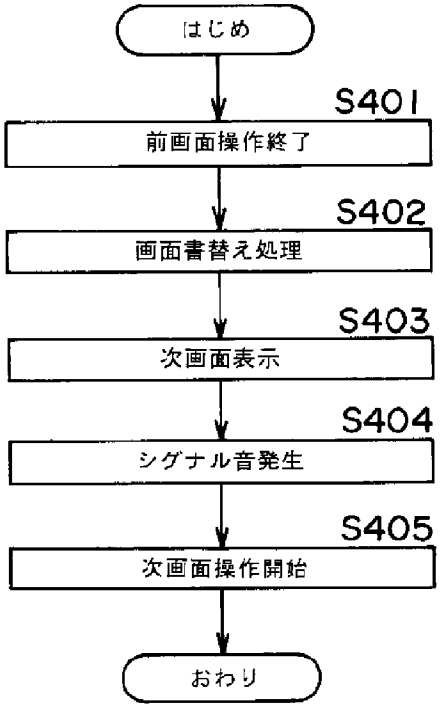
【図１６】

ヘルプ表示の説明図



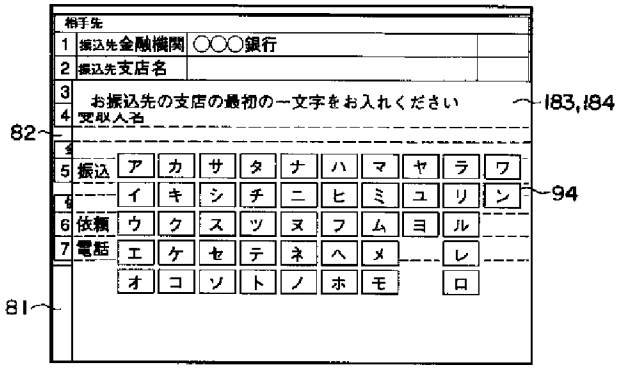
【図２４】

注意喚起処理を示すフローチャート



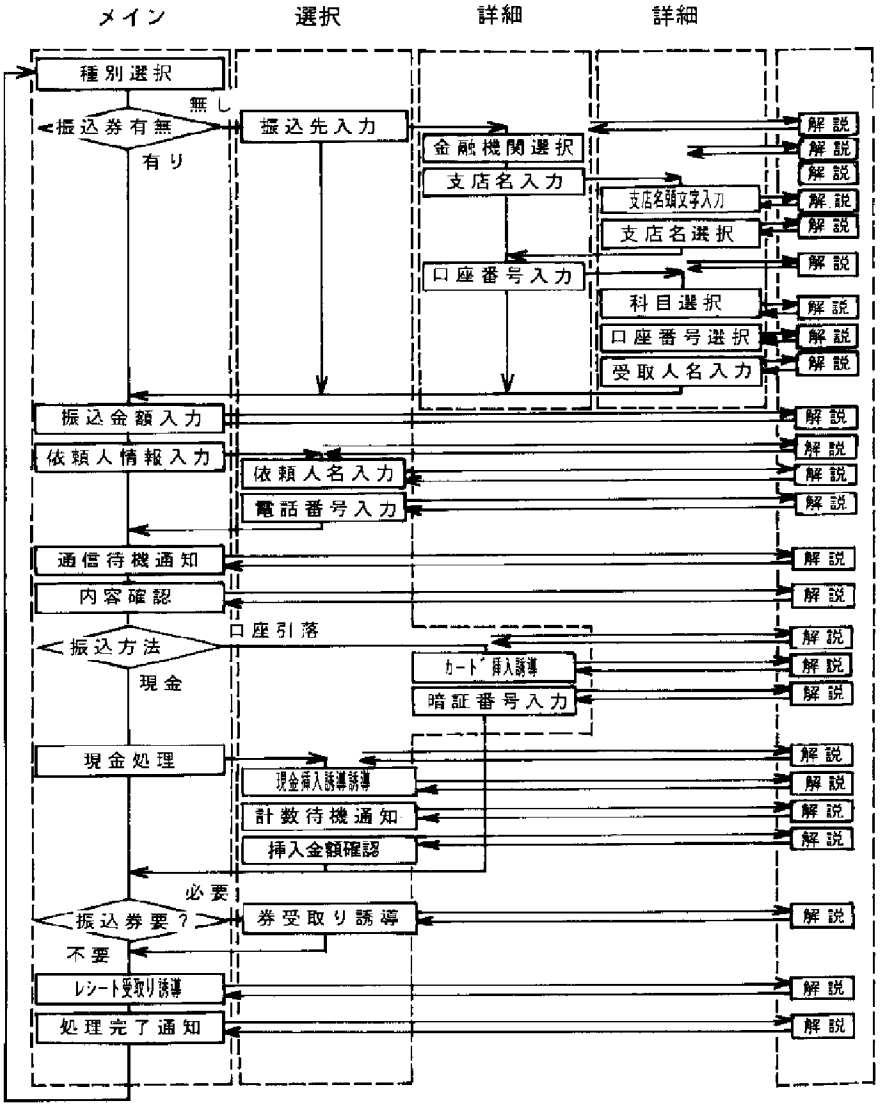
【図１９】

実施形態２による取引画面の説明図



【図18】

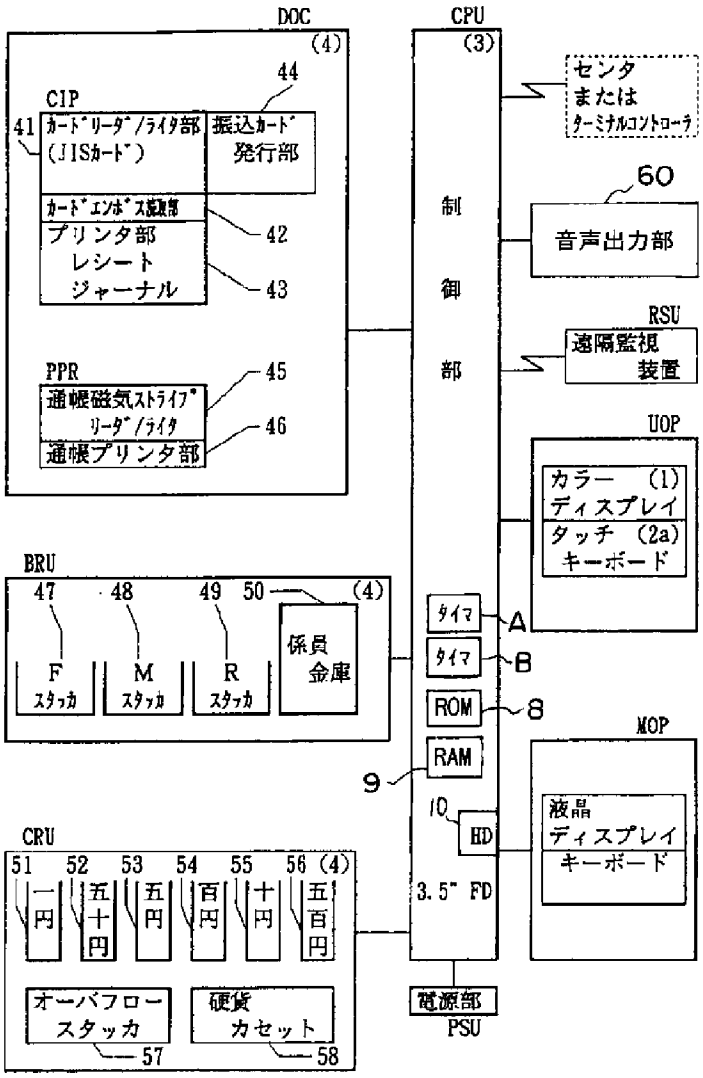
操作手順の例を示す図



Petitioner Exhibit 1002-3123

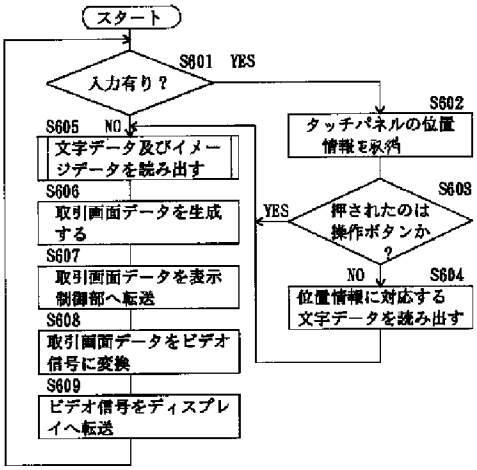
【図２０】

実施形態３によるＡＴＭの構成を示すブロック図



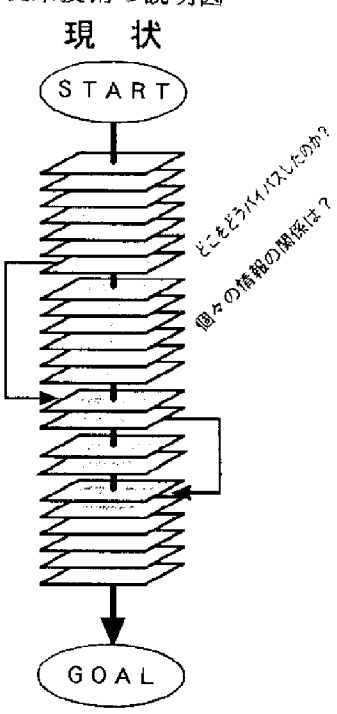
【図２９】

画面作成処理を示すフローチャート



【図３１】

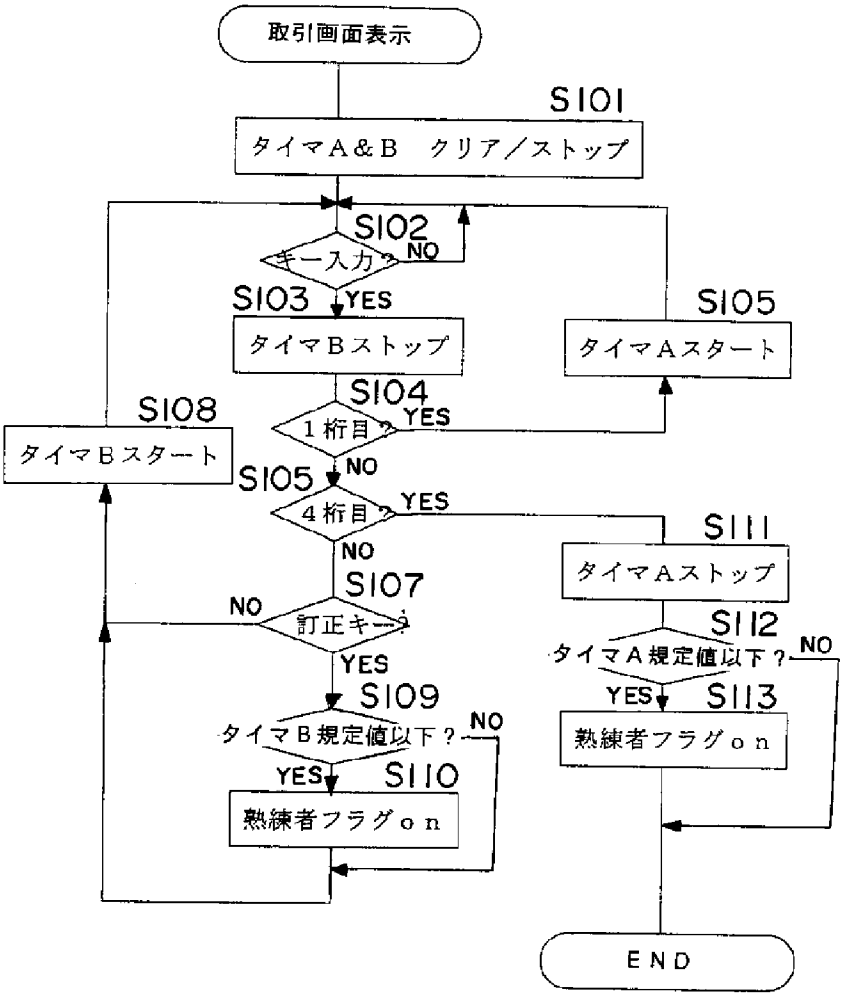
従来技術の説明図



Petitioner Exhibit 1002-3124

【図21】

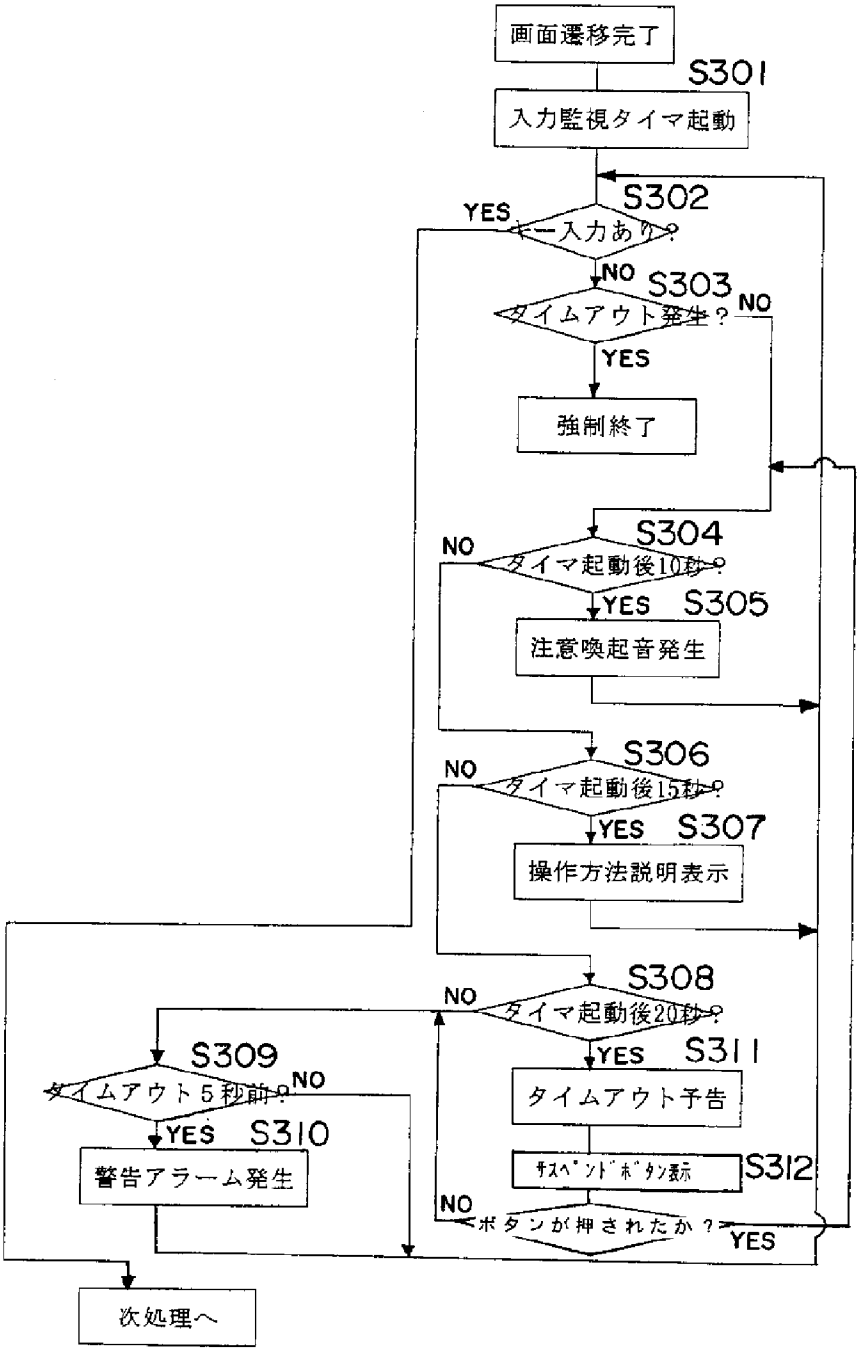
習熟度判定処理を示すフローチャート



Petitioner Exhibit 1002-3125

【図23】

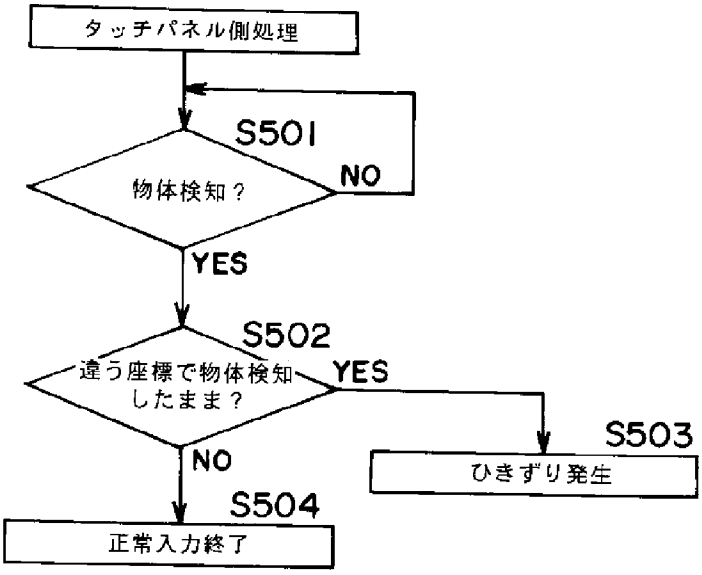
タイムアウト処理を示すフローチャート



Petitioner Exhibit 1002-3126

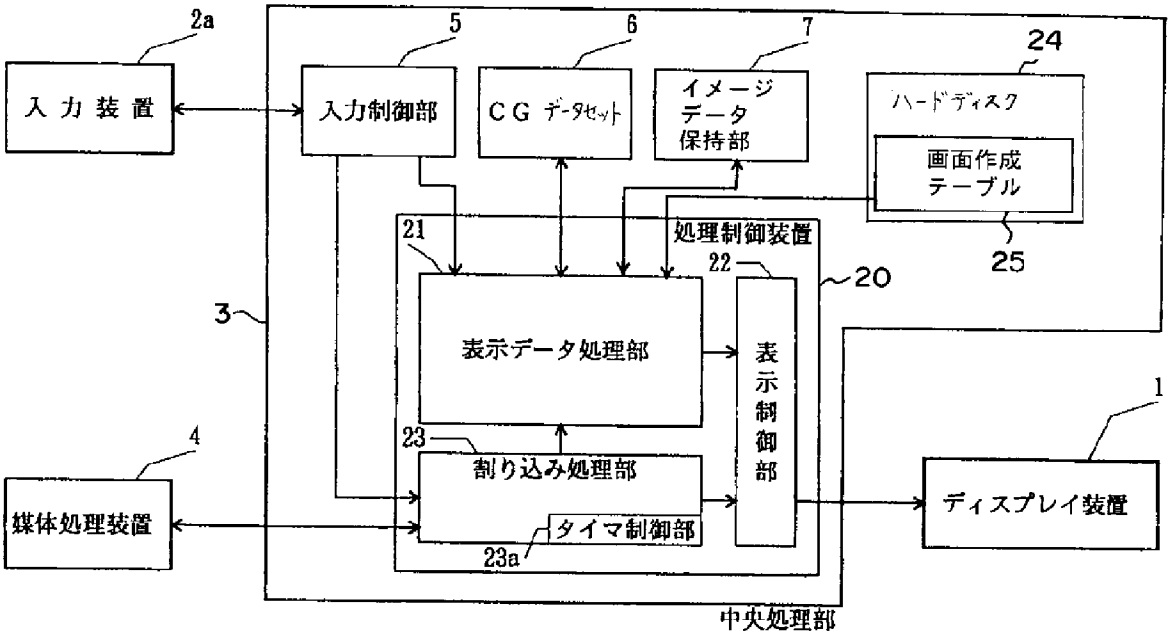
【図２５】

引きずり判定処理を示すフローチャート



【図２７】

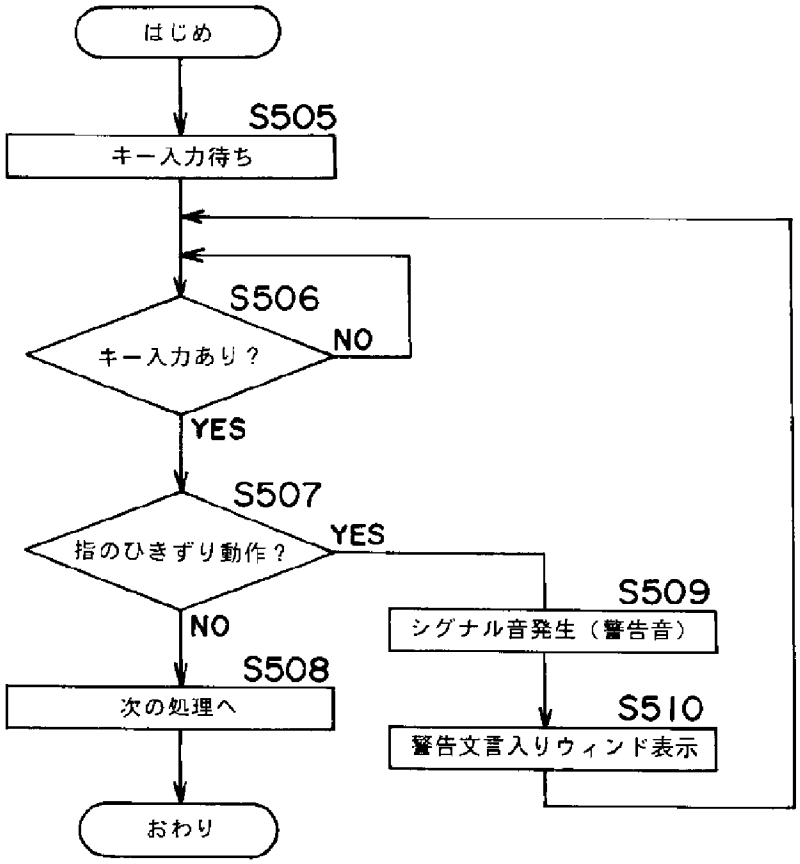
実施形態７によるＡＴＭのブロック図



Petitioner Exhibit 1002-3127

【図２６】

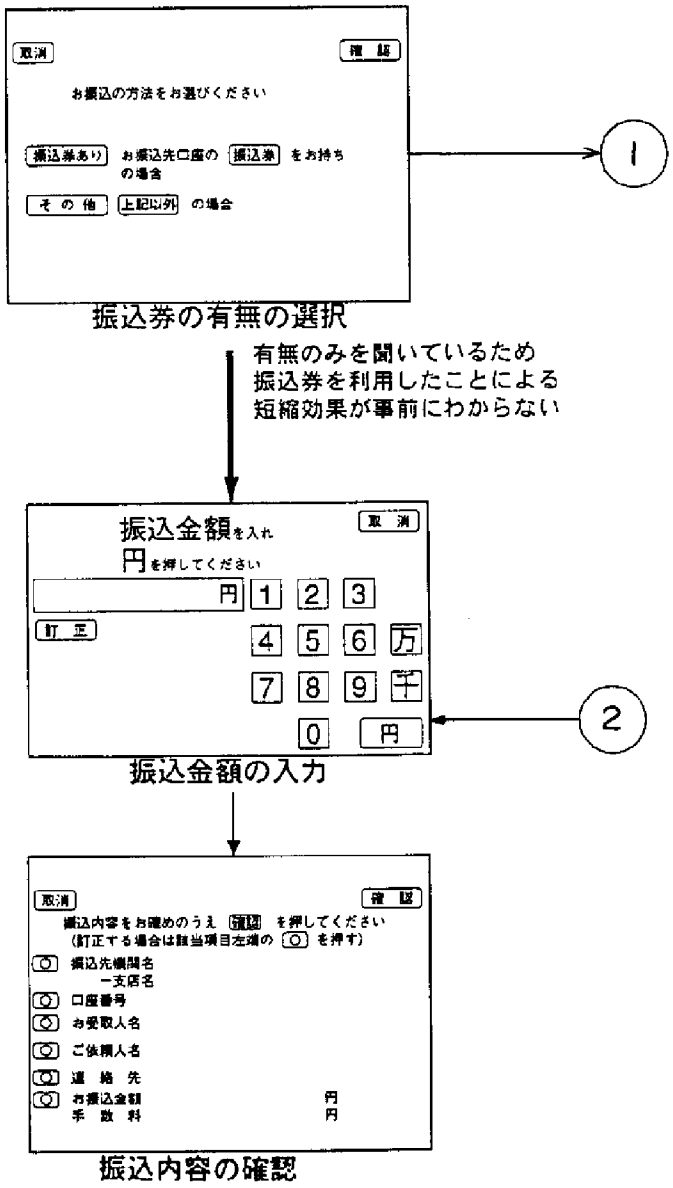
引きずり警告音発生処理を示すフローチャート



Petitioner Exhibit 1002-3128

【図３２】

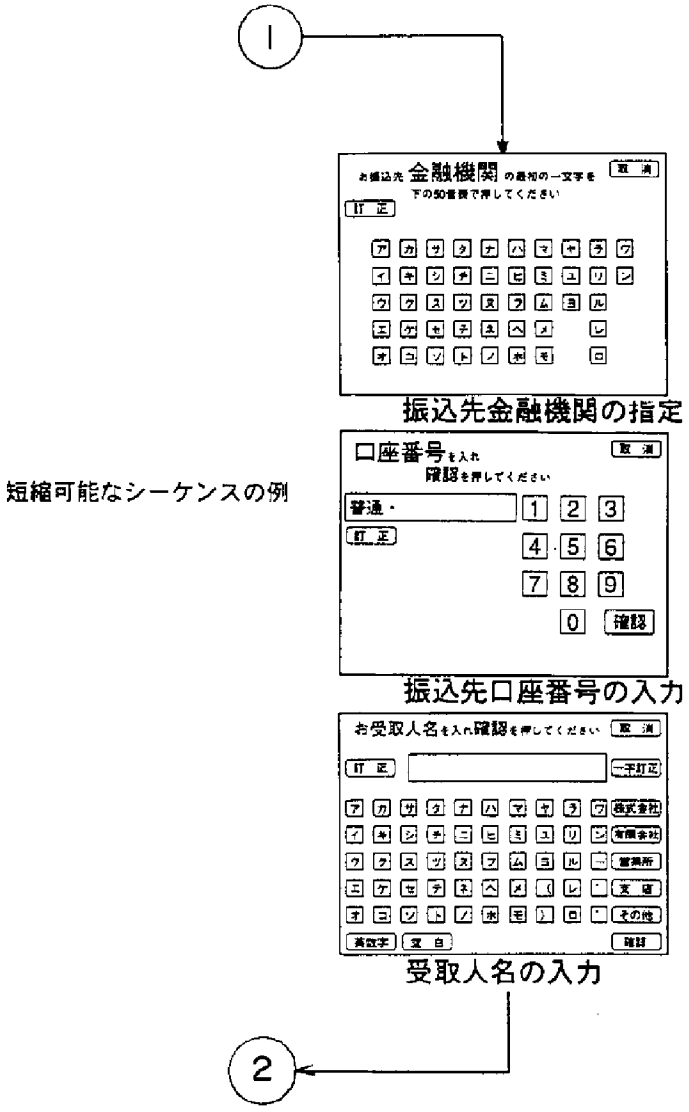
従来技術の説明図



Petitioner Exhibit 1002-3129

【図３３】

従来技術の説明図



フロントページの続き

(72)発明者　浅輪　武生
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72)発明者　岩崎　昭浩
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72)発明者　杉山　睦子
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

Petitioner Exhibit 1002-3130



CSC ServiceWorks – Ex. 1005
Page 1 of 339

Petitioner Exhibit 1002-3131

Payment Technologies for E-Commerce

CSC ServiceWorks – Ex. 1005
Page 2 of 339

Petitioner Exhibit 1002-3132

Springer-Verlag Berlin Heidelberg GmbH

CSC ServiceWorks – Ex. 1005
Page 3 of 339

Petitioner Exhibit 1002-3133

Weidong Kou
Room G05, TIIB
The University of Hong Kong
Pokfulam Road
Hong Kong, P. R. China
and
National Key Laboratory of ISN
Xidian University
Xi'an, 710071, P. R. China
weidong_kou@hotmail.com

Library of Congress Cataloging-in-Publication Data

Payment technologies for E-commerce/Weidong Kou, editor.
p. cm.
Includes bibliographical references and index
ISBN 978-3-642-07887-3 ISBN 978-3-662-05322-5 (eBook)
DOI 10.1007/978-3-662-05322-5
1. Computer security. 2. Electronic funds transfers--Security mesures. 3. Electronic commerce--Security measures. I. Kou, Weidong.

QA76.9.A25P39 2003
005.8--dc21

2002044591

ACM Subject Classification (1998): H.4, K.4.4, J.1

ISBN 978-3-642-07887-3

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilm or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag Berlin Heidelberg GmbH.
Violations are liable for prosecution under the German Copyright Law.

http://www.springer.de

© Springer-Verlag Berlin Heidelberg 2003
Originally published by Springer-Verlag Berlin Heidelberg New York in 2003
Softcover reprint of the hardcover 1st edition 2003
The use of general descriptive names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typesetting: Camera-ready by the editor
Cover Design: KünkelLopka, Heidelberg
Printed on acid-free paper 45/3142SR 5 4 3 2 1 0

Table of Contents

1	**Introduction to E-Payment: An Essential Piece of the E-Commerce Puzzle**	
	Weidong Kou	1
1.1	Introduction	1
1.2	About This Book	3
1.3	References	6
2	**Security Fundamentals**	
	Fangguo Zhang and Yumin Wang	7
2.1	Electronic Commerce Security	7
2.2	Introduction to Cryptography	9
2.3	Symmetric Cryptosystems	13
2.4	Public-Key Cryptography	17
2.5	Digital Signatures	24
2.6	Cryptographic Hash Functions	30
2.7	Cryptographic Random Number Generators	31
2.8	Authentication	32
2.9	Summary	37
2.10	References	38
3	**Public-Key Infrastructure**	
	Hui Li and Yumin Wang	39
3.1	Introduction	39
3.2	X.509	50
3.3	Credential-Based PKI Systems	61
3.4	Summary	67
3.5	References	67
4	**Biometrics for Security in E-Commerce**	
	David Zhang and Li Yu	71
4.1	An Overview of Biometrics	71
4.2	Potential Application Areas	79
4.3	Multiple Authentication Technologies	83

Petitioner Exhibit 1002-3136

4.4 How to Select a Biometrics System ... 86
4.5 Summary ... 92
4.6 References ... 92

5 Smart Cards and Applications
Weidong Kou, Simpson Poon, and Edwin M. Knorr ... 95
5.1 Introduction ... 95
5.2 Fundamentals of Smart Card Systems ... 97
5.3 Java Card ... 106
5.4 Smart Card Standards ... 109
5.5 Smart Cards and Security ... 111
5.6 Smart Card Applications ... 114
5.7 A Case Study in Smart Cards: Hong Kong's Octopus Card ... 118
5.8 Summary ... 125
5.9 References ... 126

6 Wireless Infrastructure
Weidong Kou ... 127
6.1 Introduction ... 127
6.2 Wireless Communications Infrastructure ... 128
6.3 Wireless Computing Infrastructure ... 131
6.4 Wireless Application Protocol ... 134
6.5 Wireless Security ... 144
6.6 Summary ... 145
6.7 Appendix ... 146
6.8 References ... 147

7 Payment Agents
Amitabha Das ... 149
7.1 Introduction ... 149
7.2 Security Implications of Mobile-Agent-Based Systems ... 151
7.3 Security Techniques Protecting Mobile Agents ... 151
7.4 Secure Payment Protocols Using Mobile Agents in an Untrusted Host Environment ... 156
7.5 Summary ... 168
7.6 References ... 169

CSC ServiceWorks – Ex. 1005
Page 7 of 339

Petitioner Exhibit 1002-3137

8 Digital Cash
Yi Mu, Vijay Varadharajan, and Khanh Quoc Nguyen 171
8.1 Introduction 171
8.2 Security Requirements for Digital Cash 172
8.3 Brands' Digital-Cash Scheme 173
8.4 One-Response Digital Cash 175
8.5 Fair Digital Cash 181
8.6 Summary 189
8.7 Appendix 189
8.8 References 192

9 Digital Checks
Bo Yang 195
9.1 Introduction 195
9.2 Digital Check Concept 195
9.3 NetBill 199
9.4 NetCheque System 207
9.5 Summary 209
9.6 References 209

10 Secure Electronic Transactions: Overview, Capabilities, and Current Status
Gordon Agnew 211
10.1 Introduction 211
10.2 Protocol Stack and Capabilities 212
10.3 SET Overview 215
10.4 SET Performance 223
10.5 What Lies Ahead 225
10.6 Summary 225
10.7 References 226

11 Credit Card-Based Secure Online Payment
Johnny Wong, Lev Mirlas, Weidong Kou, and Xiaodong Lin 227
11.1 Introduction 227
11.2 Online Payment by Credit Card 228

Petitioner Exhibit 1002-3138

11.3 Trust Problems in Credit Card Payments ... 230
11.4 Trusted Third Party and a Payment Protocol Using a Trusted Third Party ... 233
11.5 Summary ... 238
11.6 Appendices ... 238
11.7 References ... 243

12 Micropayments
Amir Herzberg ... 245
12.1 Introduction ... 245
12.2 Overview of Micropayment Systems ... 246
12.3 Cost Factors for Online Payments ... 250
12.4 Disputes and Chargebacks ... 252
12.5 Customer Acquiring and Support Costs ... 262
12.6 Equipment, Processing, and Communication Costs ... 273
12.7 Summary ... 279
12.8 References ... 280

13 Industrial E-Payment Systems and Solutions
Zheng Huang, Dong Zheng, Zichen Li, and Weidong Kou ... 283
13.1 Introduction ... 283
13.2 Visa Cash ... 283
13.3 iPIN E-Payment ... 289
13.4 PayPal ... 294
13.5 Summary ... 298
13.6 References ... 299

14 Challenges and Opportunities in E-Payment
Weidong Kou ... 301
14.1 E-Commerce Challenges: E-Payment Security and Privacy ... 301
14.2 E-Payment Systems Supporting Multiple Payment Methods ... 302
14.3 Smart Cards and Digital Cash ... 304
14.4 Micropayment Issues and Solutions ... 305
14.5 Summary ... 306
14.6 References ... 306

Petitioner Exhibit 1002-3139

Glossary 309
About the Editor 323
Contributors 325
Index 331

CSC ServiceWorks – Ex. 1005
Page 10 of 339

Petitioner Exhibit 1002-3140

1 Introduction to E-Payment: An Essential Piece of the E-Commerce Puzzle

Weidong Kou

University of Hong Kong
Pokfulam Road, Hong Kong

1.1 Introduction

When we look at the whole picture of e-commerce, there are many pieces in the puzzle, including the Internet communication infrastructure, various web and e-commerce application servers, client browsers, products/services, databases, security and firewalls, electronic payment (or e-payment), and many other components. To make an e-commerce web storefront work, one needs to put all these pieces of the puzzle together. The first thing that happens in cyberspace is that the customer goes through the web storefront, and looks for a product/service that is interesting to him (or her). It is clear that after the customer has searched web storefront and identified products or services, the immediate next step is making the payment for the purchase of the products/services that the customer has selected. Obviously, e-payment is essential to e-commerce transactions. Without a successful e-payment step, the e-commerce picture is not complete, and very often it will not work.

Currently, the most popular method for e-payment over the Internet is credit card based e-payment. Credit cards have been widely used for mail ordering and telephone ordering. There are regulations on credit cards established by the Federal Reserve Board, the US federal agency charged with oversight of consumer credit card regulations. According to these regulations, merchants who accept credit card information in a transaction in which the credit card is not present are responsible for unauthorized transactions using the credit card information. Although the rule was developed for the mail order and telephone order context, it applies equally to the context of e-commerce over the Internet. The Federal Reserve Board's credit card regulations also limit consumer liability for unauthorized credit card transaction charges to US $50. This limit applies to all kinds of situations whether the card is used in a face-to-face transaction, a mail order transaction, a telephone order transaction, or an e-commerce transaction over the Internet.

Petitioner Exhibit 1002-3141

These federal regulations provide a regulatory framework for credit card based payment transactions over the Internet.

Given the regulatory framework, to make credit card payment work over the Internet, a technical framework has to be developed. The technical framework consists of a number of protocols/schemes to implement online credit card payment. There are two notable credit card based e-payment schemes that have been used in most retail online merchant sites. One is the combination of credit cards with the secure sockets layer (SSL) protocol, and the other is the scheme based on the secure electronic transaction (SET). The SSL protocol provides a secure communication channel between the web browser of an online customer and the e-commerce server at an online merchant site. The SSL is based on public-key infrastructure (PKI). The SET is a standard for online credit card payment. Derived from IBM's internet payment protocol (iKP), the SET was developed jointly by Visa and MasterCard in collaboration with major IT companies such as IBM, GTE, Microsoft, SAIC (Science Applications International Corporation), Terisa Systems, and Verisign. The SET standard offers a much higher level of security than the SSL-based scheme by adding much stronger security protection against fraud and unauthorized use of credit card information. The strong security protection comes with the expense of adding more complex cryptographic operations that may require additional computation resources. The additional cryptographic operations can either make the average end user's system slow to respond to the e-payment transaction, which for the end user is not tolerable, or it simply exceeds the processing capacity of the end user's system. These problems together with business issues have contributed a slow adoption of the SET standard. The SSL-based scheme has, on the other hand, become the de facto standard for online credit card payment despite that it only provides minimal security for credit card payment transaction for this over the Internet. The main reasons are that the SSL is relatively simple, the response time of an SSL-based credit card transaction is acceptable to the average user, and the existing regulatory framework of the credit card system supplements the strong protection in the SET standard to make the SSL-based credit card online payment scheme meet the current minimum requirements of online merchants, online customers, and financial institutions [1.1-1.8].

In addition to credit card based online payment, there are other e-payment methods, including digital check, digital cash, e-payment based on debit cards, smart cards, prepaid cards, pay-by-phone service, and micropayments [1.1-1.8]. Some of these e-payment methods are briefly described as below.

- **Digital check:** Digital check is a paper-check-like payment scheme. With a digital check system in place, funds can be transferred from the payer's bank account to the payee's bank account at the time the transaction takes place. Digital check is based on a bank-account debit system. The requirements for digital check systems include the assurance of a high level of security, the capability of handling different volumes (from large to

CSC ServiceWorks – Ex. 1005
Page 12 of 339

Petitioner Exhibit 1002-3142

small), digital check processing efficiency, low cost of writing a digital check, and the availability to customers through a variety of service providers.

- **Digital cash:** Digital cash is based on credit and cash-payment systems. A digital cash system usually consists of a client, a merchant, and a bank. The client obtains digital cash from the bank and pays the merchant for the goods or services that he (or she) is purchasing. The properties of digital cash include anonymity, transferability, untraceability, infinite duration, portability, and double-spending protection.

- **Smart cards:** Smart cards are plastic cards with an embedded integrated circuit. When smart cards are used as a payment vehicle, they can be used either as a prepaid card with a fixed monetary value, or as a reloadable card (that is, electronic purse) into which people can reload a monetary value from time to time.

- **Micropayment:** Micropayment deals with a very small payment, typically in the range from one cent to a few dollars. Sometimes, the payment can be even a fraction of one cent. Micropayment is perhaps a new payment method born with e-commerce over the Internet. "Pay per click" for a piece of music or video, or pay for a piece of real-time information related to a particular company or company's stock is a new phenomenon in the Internet age. Traditional credit cards or other payment methods will not work, as there is a minimum charge for processing the payment that could exceed the value of a micropayment transaction.

When we look beyond e-commerce applications in web storefronts, nowadays, transferring business services onto the Web has becomes a trend in various industries, particularly given the recent technological developments in the areas of Web Services and Semantic Web. The idea of virtual communities is becoming a reality, as evidenced by many such communities in cyberspace having been built in the last few years, from educational hubs to virtual shopping centers. The latest technological advances in complex online services have required stronger security and more convenience in online payment over the Internet. The challenge is how to meet this increasing demand to produce new e-payment systems/solutions.

1.2 About This Book

This book is meant to respond to the need for a book that can provide readers with comprehensive information on advances in e-payment technology for e-commerce.

CSC ServiceWorks – Ex. 1005
Page 13 of 339

Petitioner Exhibit 1002-3143

We have invited leading experts across the globe, from North America to the Middle East, from Australia and Singapore to Hong Kong and China, to contribute to this book. Starting with fundamental security, the book covers the major subjects related to e-payment, including public key infrastructure, security based on biometrics, smart cards, wireless infrastructure, payment agents, digital cash, digital checks, a secure online payment protocol using a trusted third party, SET, and micropayment.

The target audience of this book includes e-commerce and e-business developers, business managers, academic researchers, university students, professors, and professional consultants. This book can also be used for e-payment classes and training courses.

The book has been divided into roughly two parts. The first part from Chapter 2 to Chapter 7 covers the infrastructure for secure e-payment over the Internet. The second part from Chapter 8 to Chapter 13 covers a variety of e-payment methods and e-payment systems/solutions.

Security is one of the major emphases of this book. The focus of Chapters 2-4 is on security. The security requirements for e-payment or e-commerce in general, such as message privacy, message integrity, authentication, authorization, nonrepudiation, and secure payment, are covered in Chapter 2. In addition, in Chapter 2, the cryptography algorithms and cryptanalysis are also discussed. Chapter 3 is mainly for the discussion of public-key infrastructure (PKI), including certificate authorities (CAs) and the ITU X.509 authentication framework. The authors of Chapter 3 have also covered the recent development of credential-based PKI systems such as simple distributed security infrastructure (SDSI) and simple public-key infrastructure (SPKI). Biometrics, such as fingerprint, retina-scan, facial scan, and voice scan, can be used to strengthen the security. In Chapter 4, a comprehensive overview of biometric technologies is provided. The potential applications of biometrics, including e-commerce applications, are discussed.

Smart cards and applications for security and e-payment are presented in Chapter 5. Smart card topics include fundamentals of smart card systems, Java Card, smart card standards, smart card security, and various smart card applications including e-payment. The Hong Kong Octopus Card, a real-life example of successful smart cards, is presented as a case study of smart cards and related applications.

With the advance of wireless technologies, e-commerce is moving to the wireless world. Wireless payment (or mobile payment) is gaining popularity. Wireless infrastructure is covered in Chapter 6, including wireless communication infrastructure, wireless computing infrastructure, wireless application protocol, and wireless security.

CSC ServiceWorks – Ex. 1005
Page 14 of 339

Petitioner Exhibit 1002-3144

Chapter 7 is devoted to payment agents. A software agent is a software program that acts autonomously on behalf of a person or organization. It is very interesting to know how these software agents can be used for personalization to help us to conduct e-commerce and to make payments online. Chapter 7 covers agent systems for e-commerce and the use of agents for payment. The security implications of mobile-agent-based systems are examined. Various security techniques for protecting mobile agents are also described, followed by a detailed discussion on how to use mobile agents in an untrusted environment to conduct secure payment.

Starting with Chapter 8, the book covers a variety of e-payment methods. The authors of Chapter 8 discuss various digital cash schemes, including Brands' digital cash scheme, one-response digital cash scheme, and fair digital cash scheme. Digital checks are covered in Chapter 9. The subjects include the fundamentals of digital checks and two digital check examples: NetBill and NetCheque. Chapter 10 covers the SET standard with a detailed SET overview. The current status is reported, and the performance issue of the SET standard is discussed. The improvement of the SET standard can be made through the use of alternative PKI systems, such as elliptic curve cryptosystem (ECC). A general introduction to credit-card-based online payment is provided in Chapter 11. In addition, an innovative secure online payment protocol using a trusted third party is also described. This protocol supports privacy protection, as the order information is not released to the third party. A patent application based on this protocol has been filed. Extensive coverage of micro-payment is provided in Chapter 12, including an overview of micro-payment systems, analysis of cost factors for online payments, disputes and charge-backs, customer acquisition and support costs, equipment, and processing and communication costs.

After the discussion of a variety of e-payment methods, in Chapter 13, three systems/solutions of e-payment are introduced, including Visa Cash, iPIN, and PayPal, with descriptions of features, advantages, disadvantages, and security mechanisms.

Finally, the book concludes with Chapter 14, in which challenges and opportunities in e-payment are identified and presented. In particular, we discussed privacy and security issues, multiple payment methods, smart cards and digital cash, and micropayment.

The readers can take advantage of the structure of the book. If they have no background knowledge of security, then they can read chapters of this book sequentially; if they are already familiar with security and PKI, they can escape reading Chapters 2-3; or if they want to focus on payment methods only, they can directly go to Chapter 8, and start their reading from there. Of course, the readers, as they wish, can always select a chapter to read without a particular order.

CSC ServiceWorks – Ex. 1005
Page 15 of 339

Petitioner Exhibit 1002-3145

1.3 References

[1.1] W. Kou, Y. Yesha (2002) Editorial of special issue on technological challenges in electronic commerce. Int J Digit Libr 3: 277–278.
[1.2] W. Kou, Y. Yesha, C. J. Tan (eds.) (2001) Electronic commerce technologies. LNCS 2040. Springer, Berlin Heidelberg New York.
[1.3] W. Kou, Y. Yesha (eds.) (2000) Electronic commerce technology trends: challenges and opportunities. IBM Press, Carlsbad.
[1.4] W. Kou (1997) Networking security and standards. Kluwer, Boston Dordrecht London.
[1.5] M. H. Sherif (2000) Protocols for secure electronic commerce. CRC Press, Boca Raton London New York Washington DC.
[1.6] M. Shaw, R. Blanning, T. Strader, A. Whinston (2000) Handbook on electronic commerce. Springer, Berlin Heidelberg New York.
[1.7] D. O'Mahony, M. Peirce, H. Tewari (1997) Electronic payment systems. Artech House, Boston London.
[1.8] P. Wayner (1997) Digital cash (2nd ed.). AP Professional, Boston New York London.

CSC ServiceWorks – Ex. 1005
Page 16 of 339

Petitioner Exhibit 1002-3146

2 Security Fundamentals

Fangguo Zhang and Yumin Wang

National Key Laboratory of ISN
Xidian University, Xi'an, China

2.1 Electronic Commerce Security

Since the creation of the World Wide Web (WWW), Internet-based electronic commerce has been transformed from a mere idea into reality. The Internet and similar networks provide new infrastructures for communications and commerce. These open networks interconnect computers across many different organizations with dramatically lower communications and distributed-applications development costs. This motivates businesses to transfer commercial activity from closed private networks to open networks like the Internet. Electronic commerce is classified into several forms. Business to business (B2B), business to consumer (B2C), and business to government (B2G) represent the most significant forms in terms of value.

All traditional commercial activities use procedures or occur within contexts designed to generate trust between individuals or between businesses. These trust mechanisms reduce the commercial risks faced by traders and rely on a variety of factors from prior track records, reputations, and the legal context for an exchange. However, unlike discrete face-to-face transactions where some goods are exchanged for cash, electronic commerce creates both opportunities and difficulties for potential traders. Specifically, it opens the opportunity to expand trade at lower costs in a larger marketplace distributed over a wider geographic scope. Indeed, leveraging these new opportunities over an inexpensive global communications infrastructure will be one of the key benefits of electronic commerce.

Open networks like the Internet pose the new requirement of generating trust in an electronic environment. The kernel of electronic commerce is its security, which has been described in many references [2.6-2.8]. We survey the essential requirements for carrying out secure electronic commerce as follows.

Petitioner Exhibit 1002-3147

- Server security

  Internet commerce requires secure-server computers, computers that serve documents, files, or programs to users. Server computers with critical applications should not be vulnerable to many attacks, such as software viruses, Trojan horses (viruses that are hidden programs or documents to be activated at a later time), and unauthorized access to the network by hackers. The basic way to achieve this is to use firewalls and proxy machines. Proxy and firewall servers intermediate all Internet communications between a firm and its external environment. Every packet and/or file transferred to or from the Internet to a firm's internal machine goes through the proxy or firewall server, where the data is checked to assure that there are no known viruses or other problems.

- Message privacy (also known as confidentiality)

  Message privacy is a key requirement for electronic commerce, it assures that communications between trading parties are not revealed to others as the message traverses an open network, thus, an unauthorized party cannot read or understand the message.

- Message integrity

  Message Integrity is another key requirement for electronic commerce. It is important that the communications between trading parties are not altered by a malicious enemy as they traverse an open network.

- Authentication

  In most contexts, the term authentication on its own is often used to mean *authentication of the sender*, which is the assurance the sender of the message was actually the person they claimed to be. Using the paper-letter analogy, authentication of the sender is primarily provided by the signature at the bottom of the page, but the general look of the document, such as the letterhead and/or watermark on the paper, is usually also taken into consideration. Other contexts in which the term *authentication* is commonly used include

  - *User authentication*, which is the assurance that the user of a computer system is really who they claim to be.
  - *Authentication of the receiver*, which allows the sender to be sure that the party they intend to get the message to is the one who receives it, or at least, is the only one who can understand it.

- Authorization

  Authorization ensures that a party has the authority to make a transaction, or is authorized to access specific information or computer resources. Authorization excludes the risk that employees or others may make transac-

CSC ServiceWorks – Ex. 1005
Page 18 of 339

Petitioner Exhibit 1002-3148

tions that create economic damage or access key information or computational resources of the organization.

- Audit mechanisms and non-repudiation

  Like normal commercial transactions, audit mechanisms for electronic commerce enable the exchange parties to maintain and revisit a history or the sequence of events during a prior transaction. In electronic commerce, these audit trails could include time stamps or records by different computers at different stages of a transaction. In addition, there is a need for confirmations and acknowledgments by the various transacting parties that they have accurately received various messages and made specific commitments. Parties should not be able to repudiate their prior commitments.

- Payments and settlements

  Electronic payment and settlements systems lower transaction costs for trading parties. Secure payment and settlement systems also ensure that the commitments to pay for goods or a service over electronic media are met. They are vital to widespread electronic commerce.

In most cases, authentication and non-repudiation are more important to commerce than confidentiality. The majority of business transactions are not sensitive enough to warrant the sender to pay much effort to prevent their contents from being disclosed to third parties. On the other hand, it is usually vital for the receiver of a message to be certain of the identity (or in some cases, the authority) of the sender of the message and that the message has not been altered in transit. In the event of disputes, it is also important that both the sender and the receiver of a message are able to prove later that the message was indeed sent, and thus, hold both parties to the agreement.

There are a number of ways to meet the above security requirements for secure electronic commerce. Other than server security, all the different mechanisms rely on techniques of cryptography. Cryptographic security mechanisms, including data encryption and digital signature schemes, are often used to provide these security services.

2.2 Introduction to Cryptography

Cryptography is the science of writing in secret code and is an ancient art. The history of cryptography dates back to circa 1900 BC where it was mainly used for military purposes. Classical cryptography is used to protect the contents of a message from being viewed by unauthorized parties. It is the art of transforming the contents of a message from its original form to one that cannot be decoded by un-

CSC ServiceWorks – Ex. 1005
Page 19 of 339

Petitioner Exhibit 1002-3149

authorized parties. This ensures that the message remains incomprehensible to unauthorized eyes, even if it is intercepted. Cryptography is a field that is by no means new, but until recently, it has largely remained in the hands of the military. Usage of cryptography for civilian purposes has become more of a mainstream practice only with the advent of ubiquitous computing and public networks. With the widespread development of computer communications, many new forms of cryptography have been proposed. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about *any* network, particularly the Internet.

As we move into an information society, the technological means for global surveillance of millions of individual people are becoming available to major governments. Cryptography has become one of the main tools for privacy, trust, access control, electronic payments, corporate security, and countless other fields.

In the following, we will introduce the basics of modern cryptography. For more about the concepts and techniques of classical cryptography, we refer the reader to [2.11, 2.14, 2.16, 2.17].

2.2.1 Basic Concept

In cryptographic terminology, the message is called *plaintext* or *cleartext*. Encoding the contents of the message in a way that hides its contents from outsiders is called *encryption*. The encrypted message is called the *ciphertext*. The process of retrieving the plaintext from the ciphertext is called *decryption*. Encryption and decryption usually make use of a key, and the coding method is such that decryption can be performed only by knowing the proper key.

Cryptology can be broken into two subfields: cryptography and cryptanalysis. Cryptography is the art or science of keeping messages secret and cryptanalysis is the art of breaking ciphers, i.e., retrieving the plaintext without knowing the proper key.

2.2.2 Basic Cryptographic Algorithms

A method of encryption and decryption is called a cipher. Some cryptographic methods rely on the secrecy of the algorithms; such algorithms are only of historical interest and are not adequate for real-world needs. Modern algorithms use keys to control encryption and decryption; a message can be decrypted only if the key matches the encryption key.

CSC ServiceWorks – Ex. 1005
Page 20 of 339

Petitioner Exhibit 1002-3150

There are two classes of key-based encryption algorithms, symmetric (or secret-key) and asymmetric (or public-key) algorithms. The difference is that symmetric algorithms use the same key for encryption and decryption (or the decryption key is easily derived from the encryption key), whereas asymmetric algorithms use a different key for encryption and decryption, and the decryption key cannot be derived from the encryption key.

Symmetric algorithms can be divided into stream ciphers and block ciphers. Stream ciphers can encrypt a single bit of plaintext at one time, whereas block ciphers take a number of bits and encrypt them as a single unit.

Asymmetric ciphers (also called public-key algorithms or, generally, public-key cryptography) permit the encryption key to be public, allowing anyone to encrypt with the key, whereas only the proper recipient (who knows the decryption key) can decrypt the message. The encryption key is also called the public key and the decryption key is called the private key or secret key.

2.2.3 Cryptanalysis

Cryptanalysis is the art and science of recovering the plaintext of a message without knowing the proper keys. There are many cryptanalytic techniques. Some of the more important ones for a system implementer are described below [2.11, 2.15].

- **Ciphertext-only attack**: This is the situation where an attacker does not know anything about the contents of the message and must work from ciphertext only. In practice, it is quite often possible to make guesses about the plaintext, as many types of messages have fixed format headers. However, this does not work well against modern ciphers.

- **Known-plaintext attack**: The attacker knows or can guess the plaintext for some parts of the ciphertext. The task is to decrypt the rest of the ciphertext blocks using this information. This may be done by determining the key used to encrypt the data, or via some shortcut.

- **Chosen-plaintext attack**: The attacker is able to have any text he likes encrypted with the unknown key. The task is to determine the key used for encryption.

- **Man-in-the-middle attack**: This attack is relevant for cryptographic communication and key exchange protocols. The usual way to prevent the man-in-the-middle attack is to use a public-key cryptosystem capable of providing digital signatures.

CSC ServiceWorks – Ex. 1005
Page 21 of 339

Petitioner Exhibit 1002-3151

- **Correlation**: Correlation between the secret key and the output of the cryptosystem is the main source of information to the cryptanalyst. In the easiest case, the information about the secret key is directly leaked by the cryptosystem. More complicated cases require studying the correlation (basically, any relation that would not be expected on the basis of chance alone) between the observed (or measured) information about the cryptosystem and the guessed key information.

- **Attack against or using the underlying hardware**: In the last few years, as more and more small mobile crypto devices have come into widespread use, a new category of attacks has become relevant which aim directly at the hardware implementation of the cryptosystem.

- **Faults in cryptosystems**: These can lead to cryptanalysis and even to the discovery of the secret key. The interest in cryptographic devices led to the discovery that some algorithms behaved very badly with the introduction of small faults in the internal computation.

- **Quantum computing**: The research on polynomial time factoring and discrete logarithm algorithms with quantum computers has caused growing interest in quantum computing. Quantum computing is a recent field of research that uses quantum mechanics to build computers that are, in theory, more powerful than modern serial computers. The power is derived from the inherent parallelism of quantum mechanics. So instead of doing tasks one at a time, as serial machines do, quantum computers can perform them all at once. Thus, it is hoped that with quantum computers we can solve problems infeasible with serial machines. The recent results of quantum computing research imply that if quantum computers could be implemented effectively, then most of public key cryptography would become history. However, they are much less effective against secret key cryptography. Current states of the art of quantum computing do not appear alarming, as only very small machines have been implemented. The theory of quantum computation show much promise for better performance than serial computers, however, whether it will be realized in practice is an open question.

- **DNA cryptography**: Leonard Adleman, one of the inventors of the well-known RSA Cryptosystem (see Section 2.4), came up with the idea of using DNA as computers. DNA molecules could be viewed as a very large computer capable of parallel execution. This parallel nature could give DNA computers exponential speedup against modern serial computers. There are, unfortunately, problems with DNA computers, one being that the exponential speed-up requires also exponential growth in the volume of the material needed. Thus in practice DNA computers would have limits on their performance. Also, it is not very easy to build one.

CSC ServiceWorks – Ex. 1005
Page 22 of 339

Petitioner Exhibit 1002-3152

There are many other cryptographic attacks and cryptanalysis techniques. However, these are probably the most important ones for an application designer. Anyone contemplating designing a new cryptosystem should have a much deeper understanding of these issues.

2.3 Symmetric Cryptosystems

In *secret key cryptography*, a single key is used for both encryption and decryption. As shown in Fig. 2.1, the sender uses the key to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called *symmetric encryption.*

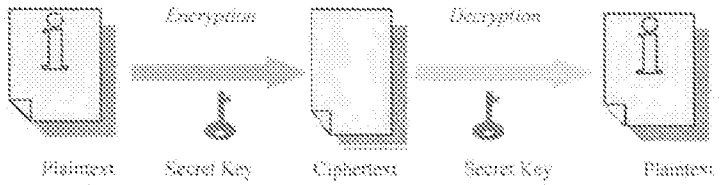


Fig. 2.1 Model of symmetric crytosystems

With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key.

There are several widely used secret key cryptographic schemes, which are generally categorized as being either *block ciphers* or *stream ciphers*. A so called block cipher encrypts more than one block of data at a time; the same plaintext block will always be encrypted into the same ciphertext (when using the same key). Stream ciphers operate on a single bit, byte, or word at a time, and they implement a feedback mechanism so that the same plaintext will yield a different ciphertext every time it is encrypted.

2.3.1 DES and 3DES

The most common secret-key cryptography scheme used is the *data encryption standard* (DES), designed by IBM in the 1970s and adopted by the National Institute for Standards and Technology (NIST) in 1977 for commercial and unclassi-

CSC ServiceWorks – Ex. 1005
Page 23 of 339

Petitioner Exhibit 1002-3153

fied government applications. DES is a block-cipher employing a 56-bit key that operates on 64-bit blocks. DES has a complex set of rules and transformations that were designed specifically to yield fast hardware implementations and slow software implementations, although this latter point is becoming less significant today since the speed of computer processors (and, therefore, programs) is several orders of magnitude faster today than twenty years ago. For many years, the US government has insisted that 56-bit DES is secure and virtually unbreakable if appropriate precautions are taken, although the cryptographic community has disagreed. On July 17, 1998, the Electronic Frontier Foundation[1] (EFF) announced the construction of a hardware device that could break DES in an average of 4.5 days. That device cost only about $220,000, including design (it was erroneously and widely reported that subsequent devices could be built for as little as $50,000). The design is scalable, which suggests that an organization could build a DES cracker that could break 56-bit keys in an average of a day for as little as $1,000,000.

Triple DES (3DES) is a minor variation of DES. It is three times slower than regular DES but can be billions of times more secure if used properly. Triple-DES enjoys much wider use than DES because DES is so easy to break with today's rapidly advancing technology. Triple-DES defines three keys, K1, K2, and K3. Generation of the ciphertext, C, from a block of plaintext, P, is accomplished by:

$$C = E_{K3}(D_{K2}(E_{K1}(P)))$$

where $E_K(P)$ and $D_K(P)$ represent DES encryption and decryption, respectively, of some plaintext *P* using DES key *K*. (For obvious reasons, this is sometimes referred to as an *encryp-decrypt-encryt mode* operation.)

Decryption of the ciphertext is accomplished by

$$P = D_{K1}(E_{K2}(D_{K3}(C))).$$

The use of three, independent 56-bit keys provides 3DES with an effective key length of 168 bits. The specification also defines the use of two keys where, in the operations above, K3 = K1. This provides an effective key length of 112 bits. Finally, a third keying option is to use a single key, so that K3 = K2 = K1. Given the relatively low cost of key storage and the modest increase in processing due to the use of longer keys, the best recommended practices are that 3DES be employed with three keys.

Triple-DES has been adopted by ANSI as standard X9.52 and is a proposed revision to FIPS 46 as draft FIPS 46-3. NIST suggests that use of 3DES replace DES in all but legacy systems and applications.

---

[1] EFF webside: http://www.eff.org

Petitioner Exhibit 1002-3154

2.3.2 AES (Rijndael)

The AES is the Advanced Encryption Standard. The AES is the new US government standard to replace the ageing DES. The algorithm of AES is Rijndael, designed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. To quote from the NIST press release, Rijndael was selected for its "combination of security, performance, efficiency, ease of implementation, and flexibility". With this endorsement Rijndael is quickly finding its way into readily available encryption software. Rijndael has a variable block length and key length. It uses keys with a length of 128, 192, or 256 bits to encrypt blocks with al length of 128, 192 or 256 bits (all nine combinations of key length and block length are possible). Both block length and key length can be extended very easily to multiples of 32 bits. In Daemen and Rijmen's book [2.4], they give a detailed description of the Rijndael algorithm.

Rijndael relies more directly on algebraic constructs than do the other algorithms. Let $GF(2^8)$ be defined by the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$, and then view the 128 bits = 16 bytes as elements of the field. The data are placed in a 4×4 array of elements of $GF(2^8)$. Rijndael has ten rounds, each consisting of four operations: ByteSub, ShiftRow, MixColumn, and AddRoundKey (the last round skips the MixColumn operation). Let elements in the array be indexed beginning with 0. ByteSub has two steps: (i) each array element is replaced by its multiplicative inverse in $GF(2^8)$ (0 is mapped to itself), and (ii) the array undergoes a fixed affine transformation over $GF(2^8)$. Then ShiftRow cyclicly shifts the elements of the ith row of the array i elements to the right. In MixColumn the columns of the array are considered as polynomials over $GF(2^8)$ (the column $A_i = (a_{0;i}\,;\, a_{1;i}\,;\, a_{2;i}\,;\, a_{3;i})$ is viewed as the polynomial $a_{3;i}\,x^3 + a_{2;i}\,x^2 + a_{1;i}\,x + a_{0;i}$, for example) and multiplied modulo $x^4 + 1$ by $03x^3 + 01x^2 + 01x + 02$ to give elements of a new 4×4 array B (thus, $b_{0;i}$ is the zero-th degree term in the product of $a_{3;i}\,x^3 + a_{2;i}\,x^2 + a_{1;i}\,x + a_{0;i}$ with $03x^3 + 01x^2 + 01x + 02$ modulo $x^4 + 1$, $b_{1;i}$ is the coefficient of the "x" term, *etc.*). MixColumn diffuses the bits of each array element through its column. RoundKey is an XOR of the key (given by the key schedule) with the elements of the array.

Rijndael admits many possibilities for parallelism: In the ByteSub and RoundKey operations the bytes can be operated on independently, and in the Shiftrow and MixColumn operations the rows and columns respectively can be independently manipulated.

The S-box (ByteSub) was designed for resistance to differential and linear cryptanalysis. It is invertible, and as it has been shown that it minimizes correlation between linear combinations of input bits and linear combinations of the output bits. MixColumn increases diffusion. Let x be a vector, and let A be a linear transformation. Define the branch number of a linear transformation as:

$$\min_{x \neq 0} \mathrm{hwt}(x) + \mathrm{hwt}(A(x)).$$

CSC ServiceWorks – Ex. 1005
Page 25 of 339

Petitioner Exhibit 1002-3155

Since MixColumn works on columns independently, if a state has a single nonzero byte, the output can have at most four nonzero bytes. Hence the maximum branch number is 5. The polynomial $03x^3+01x^2 + 01x + 02$ achieves this maximum.

The key schedule for Rijndael is a simple expansion using XOR and cyclic shift.

2.3.3 IDEA

IDEA is a 64-bit block cipher with a 128-bit key, and has an excellent reputation for quality and strength. It was originally developed in Zurich by Massey and Xuejia Lai in 1990. It was strengthened against Biham and Shamir's differential cryptanalysis attack to become IDEA in 1992.

The same algorithm is used for both encryption and decryption and consists of eight main iterations. It is based on the design concept of "mixing operations from different algebraic groups." The three algebraic groups whose operations are being mixed are: (1) XOR; (2) Addition, ignoring any overflow (addition modulo 2^{16}); and (3) Multiplication, ignoring any overflow (multiplication modulo $2^{16}+1$). IDEA runs much faster in software than DES.

The main drawback of IDEA is that it is patented and requires a license for all but personal non-commercial use, specifically including internal use for normal institutional business.

2.3.4 Other Secret-Key Cryptography Algorithms

There are a number of other secret-key cryptography algorithms that are also in use today.

- *CAST-128* (described in Request for Comments, or RFC, 2144; CAST is not an acronym, rather, its name is derived from the initials of its inventors, Carlisle Adams and Stafford Tavares of Nortel), conceptually similar to DES, a 64-bit block cipher using 128-bit keys. A 256-bit key version has also been described, called CAST-256.

- *RC2 (RC2),* a cipher is named for its inventor Ron Rivest (thus, "RC" is also sometimes expanded as "Ron's Code"). In addition to RC2, there are also RC4, RC5 and RC6. They all are invented by Ron Rivest. RC2 is a 64-bit block cipher using variable-sized keys designed to replace DES. Its code has not been made public although many companies have licensed RC2 for use in their products.

CSC ServiceWorks – Ex. 1005
Page 26 of 339

Petitioner Exhibit 1002-3156

- *RC4*, a stream cipher uses variable-sized keys. It is widely used in commercial cryptography products, although it can only be exported using keys that are 40 bits or less in length.

- *RC5*, a block-cipher supporting a variety of block sizes, key sizes, and number of encryption passes over the data.

- *RC6*, RC6 is based on Feistel rounds but not rounds Feistel operating between the two halves of the block. Instead, the Feistel rounds operate between pairs of quarters of the block, and they are interlocked by the exchange of some data. Circular shifts the extent of which is controlled by data, and a quadratic function applied to 32-bit integers are the nonlinear elements that provide the security of this block cipher.

- *Twofish*, a 128-bit block cipher using 128-, 192-, or 256-bit keys, invented by Bruce Schneier. Designed to be highly secure and highly flexible, well-suited for large microprocessors, 8-bit smart card microprocessors, and dedicated hardware.

2.4 Public-Key Cryptography

In contrast to secret-key cryptography, public-key cryptography is very new. It was first conceived of in 1976 by Diffie and Hellman [2.5], then in 1977 Rivest, Shamir and Adleman invented the RSA Cryptosystem, the first realization of a public-key system. There have since been several proposals for public-key schemes, including the ElGamal Cryptosystem and elliptic-curve cryptosystems.

Each public-key cryptosystem has its own technical nuances, however they all share the same basic property that, given an encryption key, it is computationally infeasible to determine the decryption key (and vice versa). This property lets a user, say Alice, publish her encryption key. Anyone can use that public key to encrypt a message, but only Alice can decipher the ciphertext with her private key.

In practice, computing a public-key cipher takes much longer than encoding the same message with a secret-key system. This has lead to the practice of encrypting messages with a secret-key system such as DES or AES, then encoding the secret key itself with a public-key system such as RSA. We say that the public-key system "transports" the secret key. Since the secret key is usually much shorter than the message, this technique results in significantly faster processing than if public-key cryptography alone were used.

Thus, each securely transmitted message has two components: the message proper (encoded with a secret-key system) and the key used to encode the message

CSC ServiceWorks – Ex. 1005
Page 27 of 339

Petitioner Exhibit 1002-3157

(itself encoded using a public-key system). Reading the message is, hence, a two-step process: first decode the secret key, then decode the message. In this chapter, when we say that a person used a public (or private) key to encrypt a message or that a message is encrypted, we are referring to this combined technique. The model of Public-key Cryptosystems (PKC) is shown in Fig 2.2.

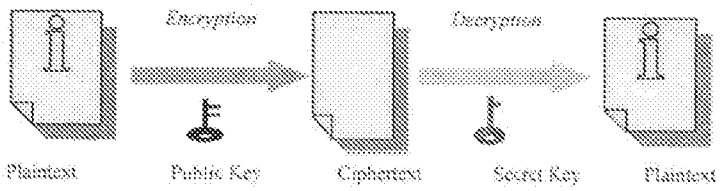


Fig. 2.2 Model of public-key cryptosystems

In a public-key cryptogsystem (PKC), one of the keys is designated the *public key* and may be advertised as widely as the owner wants. The other key is designated the *private key* and is never revealed to another party. It is straight-forward to send messages under this scheme. The sender, for example, encrypts some information using the intended receiver's public key; the receiver decrypts the ciphertext using his own private key. This method could be also used in both directions at the same time. For example, the sender could encrypt the plaintext first with his own private key and then encrypt again with the receiver's public key; this latter scheme might be used where it is important that the sender cannot deny sending the message (*non-repudiation*).

Over the years, many of the proposed public-key cryptographic systems have been broken (that is, proved to be based on an easier problem than first thought), and many others have proved impractical. Today, only three types of systems should be considered both secure and efficient. The systems, classified according to the mathematical problem on which they are based, are: the *integer factorization systems* (of which RSA is the best known example), the *discrete logarithm systems* (such as the U.S. government's DSA), and the *elliptic curve cryptosystem* (also defined as the elliptic curve discrete logarithm system).

2.4.1 RSA

The first, and still most common, PKC implementation is RSA, named for the three MIT mathematicians who developed it, Ronald Rivest, Adi Shamir, and Leonard Adleman [2.13]. RSA is used today in hundreds of software products and

CSC ServiceWorks – Ex. 1005
Page 28 of 339

Petitioner Exhibit 1002-3158

can be used for key exchange or encryption (although the latter is relatively rare). RSA uses a variable size encryption block and a variable-size key.

When an entity, say Bob, wants to use RSA cryptosystem. He first chooses two large unique primes, p and q, of roughly equal length. Then, he computes their product $n = pq$, which is called the modulus. The next step is to choose a number, e, less than n and relatively prime to $\phi(n) = (p\text{-}1)(q\text{-}1)$, which means e and $\phi(n)$ have no common factors except 1. In other words, $\text{GCD}(e, \phi(n)) = 1$. Then he finds a number d such that $ed = 1 \bmod \phi(n)$. e and d are called the public and private exponents, respectively. He publishes the public exponent and the modulus, (n, e), and keeps d, p, q private.

Now Alice wants to send a message m to Bob. Alice computes $c = m^e \bmod n$, where e and n are Bob's public key. She sends c to Bob.

To decrypt the message c Alice has sent, Bob computes m by $m = c^d \bmod n$. The relationship between e and d ensures that Bob correctly recovers m. Because only Bob knows d, only Bob can decrypt c.

The theory behind RSA cryptosystem is that currently there are no efficient algorithms for factoring large numbers. If such algorithms are found, RSA cryptosystem will become useless.

The recommended key size for RSA cryptosystem is 1024 for normal use and 2048 for extreme security.

2.4.2 Diffie-Hellman Public-Key Distribution Scheme

The Diffie - Hellman key agreement protocol was developed by Whitfield Diffie and Martin Hellman in 1976 and published in the ground-breaking paper "New Directions in Cryptography" [2.5]. The protocol allows two users to exchange a secret key over an insecure medium without any prior secrets.

The protocol has two system parameters, p and g. They are both public and may be used by all the users in a system. Parameter p is a prime number and parameter g (usually called a generator) is an integer less than p, with the following property: for every number h between 1 and p - 1 inclusive, there is a power k of g such that $h = g^k \bmod p$.

Suppose Alice and Bob want to agree on a shared secret key using the Diffie-Hellman key agreement protocol. They proceed as follows: First, Alice generates a random private value a and Bob generates a random private value b. Both a and b are drawn from the set of integers $\{1, \ldots, p - 2\}$. Then they derive their public values using parameters p and g and their private values. Alice's public value is g^a

CSC ServiceWorks – Ex. 1005
Page 29 of 339

Petitioner Exhibit 1002-3159

mod p and Bob's public value is g^b mod p. They then exchange their public values. Finally, Alice computes $g^{ab} = (g^b)^a$ mod p, and Bob computes $g^{ba} = (g^a)^b$ mod p. Since $g^{ab} = g^{ba} = k$, Alice and Bob now have a shared secret key k.

The protocol depends on the discrete logarithm problem (all of the fast algorithms known for computing discrete logarithms modulo p, where p is a large prime, are forms of the index-calculus algorithm) for its security. It assumes that it is computationally infeasible to calculate the shared secret key $k = g^{ab}$ mod p given the two public values g^a mod p and g^b mod p when the prime p is sufficiently large. Maurer has shown that breaking the Diffie-Hellman protocol is equivalent to computing discrete logarithms under certain assumptions.

2.4.3 ECC

In 1985, Neil Koblitz [2.9] from the University of Washington and Victor Miller [2.12], who was working at IBM at that time, independently proposed the elliptic-curve cryptosystem (ECC), whose security rests on the discrete logarithm problem over the points on an elliptic curve. ECC can be used to provide both a digital signature scheme and an encryption scheme. ECC represents an alternative to older forms of public-key cryptography and offers certain advantages.

To understand what ECC entails, one must understand the arithmetic involved with elliptic curves. Elliptic curves as algebraic/geometric entities have been studied extensively for the past 150 years.

A finite field consists of a finite set of elements together with two operations, addition and multiplication, that satisfy certain arithmetic properties. Finite fields often used in cryptography are F_p; where p is a prime number, and the field F_{2^m}.

An elliptic curve over finite field F_q consists of elements (x, y) satisfying the Weierstrass equation:

$$y^2+a_1xy+ a_3y = x^3 + a_2x^2+a_4x + a_6$$

When the character of F_q is not equal to 2 and 3, the equation can be simplified into

$$y^2 = x^3 + ax + b$$

If (x, y) satisfies the above equation then $P=(x, y)$ is a point on the elliptic curve. The elliptic curve formula is slightly different for some fields.

CSC ServiceWorks – Ex. 1005
Page 30 of 339

Petitioner Exhibit 1002-3160

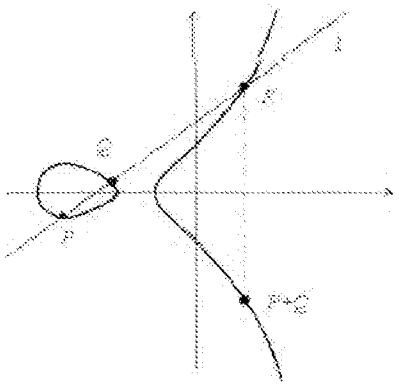


Fig. 2.3 The addition of two points on an elliptic curve

The set of points on an elliptic curve forms a group under addition, where the addition of two points on an elliptic curve is defined according to a set of simple rules. For example, consider the two points P and Q in Fig. 2.3. Point P plus point Q is equal to point $P+Q = (x, -y)$, where $(x, y) = R$ is the third point on the intersection of the elliptic curve and the line l through P and Q.

The *elliptic curve discrete logarithm problem* (ECDLP) can be stated as follows. Given an elliptic curve E defined over $\mathbb{F}_q$, a point $P \in E(\mathbb{F}_q)$ of order n, and a point $Q \in E(\mathbb{F}_q)$, determine the integer l, $0 \le l \le n - 1$, such that $Q = lP$, provided that such an integer exists.

The general conclusion of leading cryptographers is that the ECDLP requires fully exponential time to solve. The security of ECC is dependent on the difficulty of solving the ECDLP.

There are several advantages to ECC [2.10]:

- ECC leads to more efficient implementations than other public-key systems due to its extra strength provided by the difficulty in solving the ECDLP.

- The biggest advantage of ECC is key size. For example, a typical key size for the RSA algorithm is 1024 bits, which would take approximately 10^{11} MIPS years to break. In comparison, an ECC key size is 160 bits and offers the same level of security.

- Computational efficiencies are achieved with ECC. ECC does not require processing of prime numbers to achieve encryption, unlike other public-key cryptosystems. ECC is roughly 10 times faster than either RSA or DSA.

CSC ServiceWorks – Ex. 1005
Page 31 of 339

Petitioner Exhibit 1002-3161

- ECC offers considerable bandwidth savings over the other types of public-key cryptosystems when being used to transform short messages, such as the typical implementation of ECDSA. Bandwidth savings are about the same as other public-key cryptosystems when transforming long messages.

- These advantages lead to higher speeds, lower power consumption, and code-size reductions. Implementations of ECC are particularly beneficial in applications where bandwidth, processing capacity, power availability, or storage is constrained. Such applications include wireless transactions, handheld computing, broadcast, and smart card applications.

2.4.4 Other Public-Key Algorithms

Knapsack Cryptosystem

The Chor-Rivest knapsack cryptosystem was first published in 1984, followed by a revised version in 1988 [2.3]. It was the only knapsack-like cryptosystem that did not use modular multiplication. It was also the only knapsack-like cryptosystem that was secure for any extended period of time. Eventually, Schnorr and Hörner developed an attack on the Chor-Rivest cryptosystem using improved lattice reduction which reduced to hours the amount of time needed to crack the cryptosystem for certain parameter values (though not for those recommended by Chor and Rivest). They also showed how the attack could be extended to attack Damgård's knapsack hash function.

McEliece Cryptosystem

The McEliece cryptosystem is based on a class of error-correcting codes, known as Goppa codes. It was developed by R.J. McEliece in 1978. The idea behind this algorithm is to first select a particular code for which an efficient decoding algorithm is known, and then to disguise the code as a general linear code, using the fact that the problem of decoding an arbitrary linear code is NP-hard. There were no successful cryptanalytic results against the system. The system was the first public-key encryption scheme to use randomization in the encryption process. Also, the system is very efficient. But it has received little attention in practice because of some problems: the public key is enormous. The data expansion is large, and the ciphertext is twice as long as the plaintext.

CSC ServiceWorks – Ex. 1005
Page 32 of 339

Petitioner Exhibit 1002-3162

NTRU

The NTRU is a public-key cryptosystem based on the hard mathematical problem of finding very short vectors in lattices of very high dimension. It was developed by J. Hoffstein and J.H. Silverman in 1996. The process of solving this problem is called "lattice reduction", and the general study of small vectors in lattices goes by the name "geometry of numbers". The NTRU Cryptosystem is parameterized by three values, N, p, and q. All objects are univariate polynomials of degree N, which are multiplied using the convolution product rule. p and q are moduli, i.e., multiplications and additions are generally followed by reduction mod p or mod q. The most time-consuming operations in the NTRU cryptosystem are the convolution multiplications. This tutorial describes ways to speed up those multiplications.

Braid Groups Cryptosystem

The braid groups are infinite noncommutative groups naturally arisen from geometric braids. The word problem of braid groups is easy, but the generalized conjugacy search problem of braid groups is difficult. It was developed by six inventors: K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.S. Kang , C.S. Park in 2000. The underlying problem of this public key cryptosystem is the generalized conjugacy search problem in the braid group and the underlying mathematical structure is the infinite noncommutative braid group B_n.

Lucas Cryptosystem

Lucas sequences can be used for encryption and signature systems in a manner similar to RSA, but using Lucas sequences modulo a composite number instead of exponentiation. It was developed by P.J. Smith of New Zealand in 1993. It has roughly the same security as RSA for the same size key but is about twice as slow. It also has message-dependent keys. Its underlying mathematical structure is the ring of integers of the quadratic field modulo a prime p.

Hyperelliptic Curve Cryptosystems (HCC)

Hyperelliptic curves are a special class of algebraic curves and can be viewed as generalizations of elliptic curves. A hyperelliptic curve of genus g = 1 is an elliptic curve. Since 1989, the theory of hyperelliptic curves over finite fields has been applied to construction of cryptosystems. One of the main reasons for researchers interesting in cryptosystems based on elliptic and hyperelliptic curves is that these curves are a source of a tremendous number of finite abelian groups (its Jacobian) having a rich algebraic structure. Again the security depends on our inability to efficiently solve the discrete log problem, the HCDLP. The fact that this simple de-

CSC ServiceWorks – Ex. 1005
Page 33 of 339

Petitioner Exhibit 1002-3163

scription of the Jacobian does not hold for curves of genus g>1 has apparently led people to shrink back from HCC. But there are compact ways to represent elements in the Jacobians and efficient algorithms to add and double in these groups.

2.5 Digital Signatures

Digital signatures are one of the most important applications of asymmetric public-key cryptography. They are essentially electronic signatures that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time stamped. It prevents the original signer repudiate his signature later.

A *digital signature* is a cryptographic technique that enables the user to protect digital information (represented as a bit string) from undesirable modification. Since signature cannot just be appended to a digital bit string, more sophisticated methods (also known as signatures schemes) for signing have been developed.

A signature scheme is a pair of efficient functions (Sig,Ver) of a key pair (S_A,V_A) and a bit string M, such that

- Anyone who knows the secret key S_A can efficiently compute the signature $C=Sig(P_A,M)$ of any bit string M.
- If $C=Sig(S_A,M)$, then $Ver_{VA}(M,C)$=true.
- For a randomly chosen C, it is intractable for anyone who does *not* know S_A to find a value M such that $Ver_{VA}(M,C)$=true.

Some public-key algorithms can be used to generate digital signatures. A digital signature is a small amount of data that was created using some secret key, and there is a public key that can be used to verify that the signature was really generated using the corresponding private key. The algorithm used to generate the signature must be such that without knowing the secret key, it is not possible to create a signature that would be verified as valid.

Digital signatures are used to verify that a message really comes from the claimed sender (assuming only the sender knows the secret key corresponding to their public key). They can also be used to time stamp documents: a trusted party signs the document and its timestamp with their secret key, thus testifying that the document existed at the stated time.

CSC ServiceWorks – Ex. 1005
Page 34 of 339

Petitioner Exhibit 1002-3164

2.5.1 Some Main Digital Signature Schemes

The RSA Signature Scheme

The RSA cryptosystem can perform authentication, which means it can make sure the message received is authentic, has not been tampered with, and is from the sender claimed in the message. To do that, Alice, the sender, first creates a digital signature s by $s = m^d \bmod n$, where d and n are Alice's private key. She then sends m and s to Bob. Upon receiving m and s, Bob can check that the message m is indeed recovered by $m = s^e \bmod n$, where e and n are Alice's public key.

The RSA signature scheme is a deterministic digital-signature scheme which provides message recovery. The security of the schemes presented here relies to a large degree on the intractability of the integer-factorization problem.

The Rabin Public-Key Signature Scheme

The Rabin signature scheme is a variant of the RSA signature scheme. It has the advantage over RSA that finding the private key and forgery are both provably as hard as factoring. Verification is faster than signing, as with RSA signatures. In the Rabin scheme, the public key is an integer n where $n= pq$, and p and q are prime numbers that form the private key. The message to be signed must have a square root mod n; otherwise, it has to be modified slightly. Only about 1/4 of all possible messages have square roots mod n.

Signature: $s=m^{1/2} \bmod n$, where s is the signature
Verification: $m=s^2 \bmod$ n

The provable security has the side-effect that the prime factors can be recovered under a chosen message attack. This attack can be countered by padding a given message with random bits or by modifying the message randomly, at the loss of provable security.

DSA

In August of 1991, the NIST proposed a digital signature algorithm (DSA). The DSA has become a US Federal Information Processing Standard (FIPS 186), called the *digital signature standard* (DSS). It is the first digital signature scheme recognized by any government. The algorithm is a variant of the ElGamal scheme and is a digital signature scheme with appendix.

CSC ServiceWorks – Ex. 1005
Page 35 of 339

Petitioner Exhibit 1002-3165

The signature mechanism requires a hash function h: $\{0, 1\}^* \rightarrow Z_q$ for some integer q. The DSS explicitly requires use of the secure hash algorithm (SHA-1), which we will describe in Section 2.6.1.

Key generation for the DSA [2.11]. Each entity creates a public key and corresponding private key. Each entity A should do the following:

1. Select a prime number q such that $2^{159} < q < 2^{160}$.
2. Choose t so that $0 \leq t \leq 8$, and select a prime number p where $2^{511+64t} < p < 2^{512+64t}$, with the property that q divides $(p - 1)$.
3. (Select a generator α of the unique cyclic group of order q in Z^*_p.)
3.1 Select an element $g \in Z^*_p$ and compute $\alpha = g^{(p-1)/q} \bmod p$.
3.2 If $\alpha = 1$ then go to step 3.1.
4. Select a random integer a such that $1 \leq a \leq q - 1$.
5. Compute $y = \alpha^a \bmod p$.
6. A's public key is $(p; q; \alpha; y)$; A's private key is a.

DSA signature generation and verification. In *signature generation*, entity A should do the following:

1. Select a random secret integer k; $0 < k < q$.
2. Compute $r = (\alpha^k \bmod p) \bmod q$.
3. Compute $k^{-1} \bmod q$.
4. Compute $s = k^{-1}\{h(m) + ar\} \bmod q$.
5. A's signature for m is the pair $(r; s)$.

To verify A's signature $(r; s)$ on m, B should do the following:

1. Obtain A's authentic public key $(p; q; \alpha; y)$.
2. Verify that $0 < r < q$ and $0 < s < q$; if not, then reject the signature.
3. Compute $w = s^{-1} \bmod q$ and $h(m)$.
4. Compute $u_1 = wh(m) \bmod q$ and $u_2 = rw \bmod q$.
5. Compute $v = (\alpha^{u1} y^{u2} \bmod p) \bmod q$.
6. Accept the signature if and only if $v = r$.

The security of the DSA relies on two distinct but related discrete logarithm problems. One is the logarithm problem in Z_p, where the powerful index-calculus methods apply; the other is the logarithm problem in the cyclic subgroup of order q, where the best current methods run in "square-root" time.

ECDSA

A major application of ECC is ECDSA. ECC applications work extremely well with small amounts of data such as digital signatures. The ECDSA is the elliptic-curve analog of the digital signature algorithm (DSA).

CSC ServiceWorks – Ex. 1005
Page 36 of 339

Petitioner Exhibit 1002-3166

The key generation procedures for ECDSA are as follows [2.9-2.10]:

1. Entity A selects an elliptic curve E defined over F_q. The number of points in $E(F_q)$ should be divisible by a large prime n.
2. Select a point $P = E(F_q)$ of order n.
3. Select a statistically unique and unpredictable integer d in the interval $[1, n - 1]$.
4. Compute $Q = dP$.
5. A's public key is (E, P, n, Q). A's private key is d.

ECDSA signature generation:

1. Entity A selects a statistically unique and unpredictable integer k in $[1, n - 1]$.
2. Compute $kP = (x_1, y_1)$ and $r = x_1 \bmod n$. To avoid a security condition, x_1 should not equal 0.
3. Compute $k^{-1} \bmod n$.
4. Compute $s = k^{-1}(h(m) + dr) \bmod n$. h is the SHA-1.
5. If $s = 0$, then go to Step 1. If $s = 0$, then $s^{-1} \bmod n$ does not exist and s^{-1} is required in the signature verification process.
6. The signature for the message m is the pair of integers (r, s).

ECDSA signature verification:

1. Entity B obtains an authentic copy of entity A's public key (E, P, n, Q).
2. Verify that r and s are integers in the interval $[1, n - 1]$.
3. Compute $w = s^{-1} \bmod n$ and $h(m)$.
4. Compute $u_1 = h(m)w \bmod n$ and $u_2 = rw \bmod n$.
5. Compute $u_1P + u_2Q = (x_0, y_0)$ and $v = x_0 \bmod n$.
6. Entity B accepts the signature if and only if $v = r$.

Instead of choosing to generate his own elliptic curve, the entities can use the same curve E over F_q and point P of order n. In this situation, an entity's public key consists of just one point Q. This results in smaller public key sizes.

2.5.2 Some types of digital signatures

Blind Digital Signature Schemes

The concept of blind signatures was introduced by Chaum [2.18] to protect the privacy of users in applications such as electronic payment systems. In contrast to regular signature schemes, a blind signature scheme is an interactive two-party protocol between a recipient and a signer. It allows the recipient to obtain a signature of a message in a way that the signer learns neither the message nor the resulting signature. A blind signature should have two requirements: *blindness* (i.e., the

CSC ServiceWorks – Ex. 1005
Page 37 of 339

Petitioner Exhibit 1002-3167

signer does not know the content of the message) and *untraceability* (i.e., the signer can not link the message-signature pair after the blind signature has been revealed to the public).

Undeniable Signature Schemes

Undeniable signature schemes are distinct from general digital signatures in that the signature verification protocol requires the cooperation of the signer. It is devised by Chaum and van Antwerpen [2.2], are non-self-authenticating signature schemes, where signatures can only be verified with the signer's consent. However, if a signature is only verifiable with the aid of a signer, a dishonest signer may refuse to authenticate a genuine document. Undeniable signatures solve this problem by adding a new component called the disavowal protocol in addition to the normal components of signature and verification.

Fail-stop Signature Schemes

Fail-stop digital signatures are digital signatures which permit an entity A to prove that a signature purportedly (but not actually) signed by A is a forgery. This is done by showing that the underlying assumption on which the signature mechanism is based has been compromised.

The ability to prove a forgery does not rely on any cryptographic assumption, but may fail with some small probability; this failure probability is independent of the computing power of the forger. Fail-stop signature schemes have the advantage that even if a very powerful adversary can forge a single signature, the forgery can be detected and the signing mechanism no longer used. Hence, the term *fail-then-stop* is also appropriate. A fail-stop signature scheme should have the following properties:

1. If a signer signs a message according to the mechanism, then a verifier upon checking the signature should accept it.
2. A forger cannot construct signatures that pass the verification algorithm without doing an exponential amount of work.
3. If a forger succeeds in constructing a signature that passes the verification test, then with high probability, the true signer can produce a proof of forgery.
4. A signer cannot construct signatures that are at some later time claimed to be forgeries.

CSC ServiceWorks – Ex. 1005
Page 38 of 339

Petitioner Exhibit 1002-3168

2.5.2.4 Group Signature Schemes

In 1991 Chaum and van Heyst [2.1] put forth the concept of a group-signature scheme. Participants are group members, a membership manager, and a revocation manager. A group signature scheme allows a group member to sign messages anonymously on behalf of the group. More precisely, signatures can be verified with respect to a single public key of the group and do not reveal the identity of the signer.

The membership manager is responsible for the system setup and for adding group members, while the revocation manager has the ability to revoke the anonymity of signatures. A group signature scheme could, for instance, be used by an employee of a large company to sign documents on behalf of the company. In this scenario, it is sufficient for a verifier to know that some representative of the company has signed. Moreover, in contrast to the case when an ordinary signature scheme would be used, the verifier does not need to check whether a particular employee is allowed to sign contracts on behalf of the company, i.e., the verifier needs only to know a single company's public key.

The following informally stated security requirements must hold:

1. *Unforgeability of signatures:* Only group members are able to sign messages. Furthermore, they must only be able to sign in such a way that, when the signature is (later) presented to the revocation manager, he will be able to reveal the identity of the signer.

2. *Anonymity of signatures:* It is not feasible to find out the group member who signed a message without knowing the revocation manager's secret key.

3. *Unlinkability of signatures:* It is infeasible to decide whether two signatures have been issued by the same group member or not.

4. *No framing:* Even if the membership manager, the revocation manager, and some of the group members collude, they cannot sign on behalf of noninvolved group members.

5. *Unforgeability of tracing verification:* The revocation manager cannot falsely accuse a signer of having originated a given signature.

Proxy Signature Schemes

A digital signature protocol allows the signer to give the authority to sign a message to someone else without disclosing their private key.

CSC ServiceWorks – Ex. 1005
Page 39 of 339

Petitioner Exhibit 1002-3169

Proxy signatures allow the signer to designate someone else to verify their signatures. In the absence of a participant, a proxy of the participant can be authorized to sign (analogous to the power of attorney concept) without even disclosing the participant's private key. This is a very strong concept for achieving privacy in a collaborative environment.

The following properties hold for proxy signatures:

- Distinguishability: Proxy signatures are distinguishable from normal signatures by everyone.
- Unforgeabililty: Only the signer and the authorized proxy should be able to sign.
- Verifiability: The verifier should be convinced of the proxy relationship between the participant and proxy.
- Identifiability: The original signer should be able to determine the proxy signer's identity from a proxy signature.
- Undeniability: A proxy/participant cannot deny a message.

2.6 Cryptographic Hash Functions

Cryptographic hash functions are used in various contexts, for example, to compute the message digest when making a digital signature. A hash function compresses the bits of a message to a fixed-size *hash value* in a way that distributes the possible messages evenly among the possible hash values. A cryptographic hash function does this in a way that makes it extremely difficult to come up with a message that would hash to a particular hash value.

Cryptographic hash functions typically produce hash values of *128* or more bits. This number (2^{128}) is vastly larger than the number of different messages likely to ever be exchanged in the world. The reason for requiring more than *128* bits is based on the *birthday paradox*. The birthday paradox roughly states that given a hash function mapping any message to a *128*-bit hash digest, we can expect that the same digest will be computed twice when 2^{64} randomly selected messages have been hashed. As cheaper memory chips for computers become available, it may become necessary to require larger than *128*-bit message digests (such as *160* bits, which has become standard recently).

Hash algorithms are typically used to provide a *digital fingerprint* of a file's contents, and are often used to ensure that the file has not been altered by an intruder or a virus. Hash functions are also commonly employed by many operating systems to encrypt passwords.

CSC ServiceWorks – Ex. 1005
Page 40 of 339

Petitioner Exhibit 1002-3170

2.6.1 SHA-1

The secure hash algorithm also called the *secure hash standard* (SHS) is a cryptographic hash algorithm published by the United States Government. It produces a 160-bit hash value from a message of an arbitrary length. It is considered to be very good. The length of the padded message is a multiple of 512 bits. This standard specifies a *secure hash algorithm*, SHA-1, for computing a condensed representation of a message or a data file. When a message of any length $< 2^{64}$ bits is input, the SHA-1 produces a 160-bit output called a message digest. The message digest can then be input to the *digital signature algorithm* (DSA), which generates or verifies the signature for the message. Signing the message digest rather than the message itself often improves the efficiency of the process because the message digest is usually much smaller in size than the message. The same hash algorithm must be used by the verifier of a digital signature as was used by the creator of the digital signature.

SHA-1 is probably the preferred hash function for new applications. Currently, no problems are found from it.

2.6.2 MD5

The *message digest algorithm 5* (MD5) is one of message-digest algorithms developed by Rivest. The other algorithms are MD2 and MD4. MD5 is basically MD4 with "safety-belts". While it is slightly slower than MD4, it is more secure. The algorithm consists of four distinct rounds, with a slightly different design from that of MD4. It can be used to hash an arbitrary length byte string into a 128-bit value.

MD5's ancestor, MD4, has been broken, and there are some concerns about the safety of MD5 as well. In 1996 a collision of the MD5 compression function was found by Hans Dobbertin. Although this result does not directly compromise its security, as a precaution the use of MD5 is not recommended in new applications.

2.7 Cryptographic Random Number Generators

Cryptographic random number generators generate random numbers for cryptographic applications, such as keys. Conventional random number generators available in most programming languages or programming environments are not suitable for use in cryptographic applications (they are designed for statistical randomness, not to resist prediction by cryptanalysts).

CSC ServiceWorks – Ex. 1005
Page 41 of 339

Petitioner Exhibit 1002-3171

In the optimal case, random numbers are based on true physical sources of randomness that cannot be predicted. Such sources may include the noise from a semiconductor device, the least significant bits of an audio input, or the intervals between device interrupts or user keystrokes. The noise obtained from a physical source is then "distilled" by a cryptographic hash function to make every bit depend on every other bit. Quite often, a large pool (several thousand bits) is used to contain randomness, and every bit of the pool is made to depend on every bit of the input noise and every other bit of the pool in a cryptographically strong way.

When true physical randomness is not available, pseudo-random numbers must be used. This situation is undesirable, but often arises on general-purposed computers. It is always desirable to obtain some environmental noise, even from device latencies, resource utilization statistics, network statistics, keyboard interrupts, or whatever. The point is that the data must be unpredictable for any external observer; to achieve this, the random pool must contain at least 128 bits of true entropy.

Cryptographic pseudo-random number generators typically have a large pool ("seed value") containing randomness. Bits are returned from this pool by taking data from the pool, optionally running the data through a cryptographic hash function to avoid revealing the contents of the pool. When more bits are needed, the pool is stirred by encrypting its contents by a suitable cipher with a random key (that may be taken from an unreturned part of the pool) in a mode that makes every bit of the pool depend on every other bit of the pool. New environmental noise should be mixed into the pool before stirring to make prediction of previous or future values even more impossible.

Even though cryptographically strong random number generators are not very difficult to build if designed properly, they are often overlooked. The importance of the random number generator must thus be emphasized, that is, if done badly, it will easily become the weakest point of the system.

2.8 Authentication

In the real world of full competition, those fraudulent of identities are inevitable. One is often asked to prove one's identity. The security of communication and data systems depend to a great extent on whether or not the identities of users can be properly verified. For instance, the *automatic teller machine* (ATM) in a bank can give cash to authorized cardholders, which improves the efficiency of the bank greatly. Access to and use of a computer and confidential data are based on the accurate verification of users' identities. Authentication refers to a process of confirming whether or not the object to be authenticated is exactly what it is claimed to be. The object to be authenticated can be a password, a digital signa-

CSC ServiceWorks – Ex. 1005
Page 42 of 339

Petitioner Exhibit 1002-3172

ture, or some physiological characteristic such as a fingerprint, voice, or retina. Authentication is often used in communication to mutually confirm the identities of users so as to guarantee to both sides that the identity of the other side is real and valid. There are many methods to realize authentication.

2.8.1 Authentication Based on Password

Conventional password authentication schemes involve time-invariant passwords, which provide so-called *weak authentication*. The basic idea is as follows. Each user (entity) is associated with a *password*. The user is capable of committing their password to memory. The password is then used as a shared secret between the user and the system. For the user to gain access to a system resource, he inputs a (*user-ID*, *password*) pair, and explicitly or implicitly specifies a resource. Here *user-ID* is a claim of identity, and *password* is the evidence supporting the claim. The system then authenticates the user by checking the password. The user is authentic and is authorized to access the resource if the password matches the corresponding data held for that *user-ID*.

Password schemes can be divided into many classes according to the means by which information allowing password verification is stored within the system along with the method of verification. Fixed password schemes and one-time password schemes are typical examples.

Authentication schemes based on passwords have some advantages. Many systems, such as UNIX, Windows NT, and NetWare, all support this kind of authentication. They are simple and practical for closed small systems; however, they also have disadvantages [2.11].

Password schemes are only suitable for one-way authentication. That is, the system can authenticate the user, but the user cannot authenticate the system. Hence, the adversary may disguise itself as the system to get a user's password.

To overcome these drawbacks, the system can take measures, such as enciphering the user's password when transmitting, and applying uninvertible encryption to users' password files. However, there are still some ways for the adversary to decipher a user's password or decrypt users' password files.

2.8.2 Double Factor Authentication

In double-factor authentication systems, a user possesses not only a password but also a device-of-access token. When a user enters the system, in addition to a password they need to also input the number showed on their device-of-access to-

CSC ServiceWorks – Ex. 1005
Page 43 of 339

Petitioner Exhibit 1002-3173

ken. This number on their device-of-access token changes from time to time and is inherent with the authentication sever.

A double-factor authentication scheme is more difficult for the adversary to attack than a password-based authentication scheme. The adversary cannot pass authentication with only a user's password or access token-device. Changing numbers on the access-token device makes it even harder for the adversary to attack the system. So double-factor authentication is more secure than password-based authentication.

2.8.3 Two-Stage Authentication and Password-Derived Keys

Human users have difficulty remembering secret keys that have sufficient entropy to provide adequate security. Two techniques that address this issue are now described. When tokens are used with offline PIN verification, a common technique is for the PIN to serve to verify the user to the token, while the token contains additional independent information allowing the token to authenticate itself to the system (as a valid token representing a legitimate user). The user is thereby indirectly authenticated to the system by a two-stage process. This requires the users to have possession of the token but only remember a short PIN, while a longer key (containing adequate entropy) provides cryptographic security for authentication over an unsecured link.

The second technique is to map a user's password into a cryptographic key (e.g., a 56-bit DES key) by a one-way hash function. Such password-derived keys are called *passkeys*. The passkey is then used to secure a communication link between the user and a system that also knows the user password. It should be ensured that the entropy of the user's password is sufficiently large that an exhaustive search of the password space is not more efficient than an exhaustive search of the passkey space (i.e., guessing passwords is not easier than guessing 56-bit DES keys).

2.8.4 Challenge-Response Identification (Strong Authentication)

Challenge-response identification is also an important kind of authentication. The idea of cryptographic challenge-response protocols is that one entity (the claimant, or prover) "proves" its identity to another entity (the verifier) by demonstrating knowledge of a secret known to be associated with that entity, without revealing the secret itself to the verifier during the protocol. This is accomplished by answering a time-variant challenge, where the answer is determined by both the prover's secret and the challenge. The *challenge* is typically a random number chosen by one entity secretly at the outset of the protocol. Even if the communica-

CSC ServiceWorks – Ex. 1005
Page 44 of 339

Petitioner Exhibit 1002-3174

tion line is monitored, the response from one execution of the identification protocol should not provide an adversary with useful information for a later authentication, as a later challenge will be different.

The protocols of challenge-response identification fall into three major classes. They are based on symmetric-key cryptosystems, public-key cryptosystems, and zero-knowledge proof systems [2.11], respectively.

Challenge-Response by Symmetric-Key Techniques

Challenge-response mechanisms based on symmetric-key techniques require the claimant and the verifier to share a symmetric key. For closed systems with a small number of users, each pair of users may share a key in advance. In larger systems employing symmetric-key techniques, identification protocols often involve the use of a trusted online server. Each party shares a key with the trusted sever. The trusted sever effectively provides a common session key to two parties each time one requests authentication with the other.

The Kerberos protocol [2.11] and the Needham-Schroeder shared-key protocol [2.11] are good examples of authentication protocols that provide entity authentication based on symmetric encryption and involve the use of an online trusted third party. Kerberos protocol employs a client/server architecture and provides user-to-server authentication rather than host-to-host authentication. In this model, security and authentication are based on secret-key technology where every host on the network has its own secret key. It would clearly be unmanageable if every host had to know the keys of all other hosts, so a secure, trusted host somewhere on the network, known as a *key distribution center* (KDC), knows the keys for all of the hosts (or at least some of the hosts within a portion of the network, called a *realm*). In this way, when a new node is brought online, only the KDC and the new node need to be configured with the node's key (keys can be distributed physically or by some other secure means).

Challenge-Response by Public-Key Techniques

In such identification protocols, a claimant demonstrates knowledge of its private key in one of the following two ways:

1. The claimant decrypts a challenge encrypted under its public key.
2. The claimant digitally signs a challenge.

Ideally, the public-key pair used in such mechanisms should not be used for other purposes, since combined usage may compromise security. A second caution is that the public-key system used should not be susceptible to chosen ciphertext

CSC ServiceWorks – Ex. 1005
Page 45 of 339

Petitioner Exhibit 1002-3175

attacks, as an adversary may attempt to extract information by impersonating a verifier and choosing strategic rather than random challenges.

Challenge-Response by Zero-Knowledge Proof

The verifier learns nothing about the fact being proved (except that it is correct) from the prover that the verifier could not already learn without the prover, even if the verifier does not follow the protocol (as long as the prover does). In a zero-knowledge proof, the verifier cannot even later prove the fact to anyone else. (Not all interactive proofs have this property.)

A typical round in a zero-knowledge proof consists of a "commitment" message from the prover, followed by a challenge from the verifier, and then a response to the challenge from the prover. The protocol may be repeated for many rounds. Based on the prover's responses in all the rounds, the verifier decides whether to accept or reject the proof.

There are few zero-knowledge and interactive proof protocols [2.17] used today as identification schemes. The *Fiat-Shamir protocol* is the first practical zero-knowledge protocol with cryptographic applications and is based on the difficulty of factoring. A more common variation of the Fiat-Shamir protocol is the Feige-Fiat-Shamir scheme. Guillou and Quisquater further improved Fiat-Shamir's protocol in terms of memory requirements and interaction (the number of rounds in the protocol).

2.8.5 Authentication Based on Certificate Authority

The authentication technique based on *certificate authority* (CA) is similar to that of Kerberos. It realizes authentication using a mutually trusted third party. It employs public-key cryptosystems, and its realization is much simpler. The trusted third party here is the so-called CA. The CA is responsible for user identification and issues signed digital certificates for users. The digital certificate is called an X.509 certificate since it follows the format of the X.509 standard. A user possessing such a certificate can access those severs trusting CA. We will describe CA and X.509, in detail in the next Chapter.

When a user asks to access a sever, they are asked to submit their digital certificate. The sever decrypts and verifies the user's certificate. If the certificate is valid, the sever then gets the user's public key. In subsequent communication with the user, the sever can encrypt messages with the user's public key. The authentication mechanism based on an X.509 certificate is applicable to identification in an open-network environment. It has gained wide acceptance. Many network se-

CSC ServiceWorks – Ex. 1005
Page 46 of 339

Petitioner Exhibit 1002-3176

curity programs, such as IPSec, SSL, SET, and S/MIME, all use this identification mechanism.

This authentication mechanism employs asymmetric cryptosystem so that the user's certificate and their private key are not transmitted in the network. Hence the security drawbacks of password-based authentication are effectively overcome. Even if the adversary intercepts a user's certificate, they still cannot decrypt the message delivered to the user since they do not know the user's private key.

There are already some authentication organizations on the Internet using the X.509 certificate mechanism. Verisign, US Postal Service, and CommerceNet are examples.

The certificate associates the unique user name with its public key. Whether or not this association is legal is beyond the X.509 standard. X.509 claims that whatever is concerned with semantics and trust relies on the *certification practice statement* (CPS) of CA. This will obviously result in differences in the methods and degree of strictness of identification. Thus, it is necessary to establish a uniform authentication system and related rules all over the world.

2.9 Summary

The promise of electronic commerce is one of the major factors that are contributing to the rapid growth of the Internet as a communications medium. With any commercial activity, it is important to consider the security implications of doing business. It will be especially important to support the use of cryptographic mechanisms for data protection, authentication, and privacy protection in electronic commerce. This chapter introduced the security of electronic commerce and the basics of cryptography. Particularly, it deals with the following themes:

- The essential requirements for carrying out secure electronic commerce.
- A basic introduction to cryptography, include secret-key cryptography, public-key cryptography, digital signature, Hash function, random number generators and authentication techniques.

CSC ServiceWorks – Ex. 1005
Page 47 of 339

Petitioner Exhibit 1002-3177

2.10 References

[2.1] D. Chaum, E. Heijst (1991) Group signatures. In: Advances in cryptology – EUROCRYPT 91, LNCS 547. Springer, Berlin Heidelberg New York, pp. 257–265.

[2.2] D. Chaum, H. Antwerpen (1990) Undeniable signatures. In: Advances in cryptology – CRYPTO 89, LNCS 434. Springer, Berlin Heidelberg New York, pp. 212–216.

[2.3] B. Chor, R.L. Rivest (1988) A knapsack-type public-key cryptosystem based on arithmetic in finite fields. IEEE Trans Infor Theory 34: 901–909.

[2.4] J. Daemen, V. Rijmen (2002) The design of Rijndael. Springer, Berlin Heidelberg New York.

[2.5] W. Diffie, M. Hellman (1976) New directions in cryptography. IEEE Trans Infor Theory 22: 644–654.

[2.6] W. Ford, M. Baum (1997) Secure electronic commerce: building the infrastructure for digital signatures encryption. Prentice-Hall, Englewood Cliffs New York.

[2.7] S. Garfinkel (1995) PGP: pretty good privacy. O'Reilly, Beijing Cambridge Farnham Koln Tokyo.

[2.8] A. Kambil (draft) Trends in electronic commerce security background material for discussion on payments and settlements. http://www.stern.nyu.edu/~akambil/teaching/cases/secure.pdf.

[2.9] N. Koblitz (1987) Elliptic curve cryptosystems. Math Comput 48: 203–209.

[2.10] A. J. Menezes (1993) Elliptic curve public key cryptography. Kluwer, Boston Dordrecht London.

[2.11] A. J. Menezes, P.C. Oorschot, S. A. Vanstone (1997) Handbook of applied cryptography. CRC Press, Boca Raton.

[2.12] V. S. Miller (1986) Use of elliptic curves in cryptography. In: Advances in cryptology – CRYPTO 85, LNCS 218. Springer, Berlin Heidelberg New York, pp. 417–426.

[2.13] R. L. Rivest, A. Shamir, L. M. Adleman (1978) A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 21(2): 120–126.

[2.14] G. J. Simmons (ed.) (1992) Contemporary cryptology: the science of information integrity. IEEE Press, New York.

[2.15] SSH - tech corner - introduction to cryptography. http://www.ssh.fi/tech/crypto/intro.html.

[2.16] D. R. Stinson (1995) Cryptography: theory and practice. CRC Press, Boca Raton.

[2.17] W. Stallings (1999) Cryptography and network security: principles and practice (2nd ed.). Prentice-Hall, Upper Saddle River.

[2.18] D. Chaum (1983): Blind signature for untraceable payments. In: Advance in cryptology. Plenum Press, New York, pp. 199–203.

CSC ServiceWorks – Ex. 1005
Page 48 of 339

Petitioner Exhibit 1002-3178

3 Public-Key Infrastructure

Hui Li and Yumin Wang

National Key Laboratory of ISN
Xidian University, Xi'an, China

3.1 Introduction

3.1.1 What Is a PKI?

In its most simple form, a *Public-key infrastructure* (PKI) is a system for publishing the public-key values used in public-key cryptography. PKI is the combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on the Internet.

A PKI integrates digital certificates, public-key cryptography, and certificate authorities into a total, enterprise-wide network security architecture. A typical enterprise's PKI encompasses the issuance of digital certificates to individual users and servers; end-user enrollment software; integration with corporate certificate directories; tools for managing, renewing, and revoking certificates; and related services and support.

3.1.2 Why Do You Need PKI

PKI protects your information assets in several essential ways:

- **Authenticate identity.** Digital certificates issued as part of your PKI allow individual users, organizations, and web site operators to confidently validate the identity of each party in an Internet transaction.
- **Verify integrity.** A digital certificate ensures that the message or document the certificate "signs" has not been changed or corrupted in transit online.
- **Ensure privacy.** Digital certificates protect information from interception during Internet transmission.

Petitioner Exhibit 1002-3179

- **Authorize access.** PKI digital certificates replace easily guessed and frequently lost user IDs and passwords to streamline intranet log-in security and reduce the MIS overhead.
- **Authorize transactions.** With PKI solutions, your enterprises can control access privileges for specified online transactions.
- **Support for non-repudiation.** Digital certificates validate their users' identities, making it nearly impossible to later repudiate a digitally "signed" transaction, such as a purchase made on a web site.

3.1.3 Certificates and Certificate Authorities (CAs)

A *certificate* is a collection of information that has been digitally signed by its issuer (see Fig. 3.1). Such certificates are distinguished by the kind of information they contain. An *identity certificate* is an electronic document used to identify an individual, a server, a company, or some other entity called the certificate *subject* and to associate that subject with a public key. A *credential certificate* describes non-entities, such as a permission or credential. Like a driver's license, a passport, or other commonly used personal IDs, a certificate provides generally recognized proof of a person's identity. Public-key cryptography uses certificates to address the problem of impersonation.

To get a driver's license, you typically apply to a government agency, such as the Department of Motor Vehicles, which verifies your identity, your ability to drive, your address, and other information before issuing the license. To get a student ID, you apply to a school or college, which performs different checks (such as whether you have paid your tuition) before issuing the ID. To get a library card, you may need to provide only your name and a utility bill with your address on it.

Certificates work much the same way as any of these familiar forms of identification. *Certificate authorities* (CAs) are entities that validate identities and issue certificates. They can be either independent third parties or organizations running their own certificate-issuing server software (such as Netscape Certificate Server). The methods used to validate an identity vary depending on the policies of a given CA, that is, just as the methods to validate other forms of identification vary depending on who is issuing the ID and the purpose for which it will be used. In general, before issuing a certificate, the CA must use its published verification procedures for that type of certificate to ensure that an entity requesting a certificate is in fact who it claims to be.

The certificate issued by the CA binds a particular public key to the name of the entity the certificate identifies (such as the name of an employee or a server). Certificates help prevent the use of fake public keys for impersonation. Only the public key certified by the certificate will work with the corresponding private key possessed by the entity identified by the certificate.

CSC ServiceWorks – Ex. 1005
Page 50 of 339

Petitioner Exhibit 1002-3180

In addition to a public key, a certificate always includes the name of the entity it identifies, an expiration date, the name of the CA that issued the certificate, a serial number, and other information. Most importantly, a certificate always includes the digital signature of the issuing CA. The CA's digital signature allows the certificate to function as a "letter of introduction" for users who know and trust the CA but don't know the entity identified by the certificate.

A certificate *user* is an entity who relies upon the information contained in a certificate. The certificate user trusts the issuing authority to issue true certificates, that is, certificates that truly identify the subject and its public key (in the case of identity certificates), or that truly describe a subject's credentials (in the case of credential certificates).

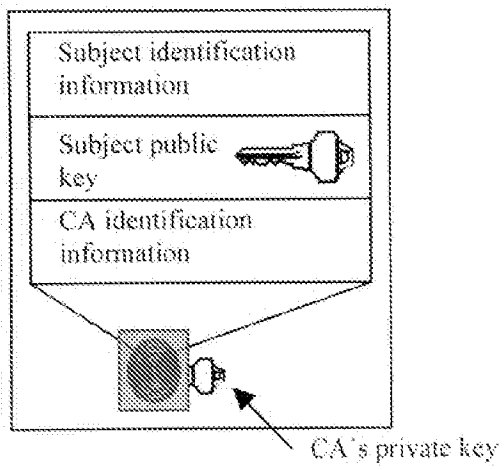


Fig. 3.1 A basic certificate

To help illustrate these concepts, we present an example using identity certificates. Imagine that Alice wishes to securely communicate with Bob using a public key cryptosystem. Alice needs to know the value of Bob's public encrypting key. Without a PKI, Alice must have direct knowledge of that key, i.e., Bob must communicate it to her via a secure channel.

With a PKI, Alice only needs to have direct knowledge of a CA's public signing key. The CA would issue an identity certificate for each of Bob's public encrypting keys. Then if Alice wishes to communicate with Bob, she can use the appropriate certificate to obtain the correct public key value. In this case, Alice is the certificate user while Bob is the subjects of certificate. See Fig. 3.2.

CSC ServiceWorks – Ex. 1005
Page 51 of 339

Petitioner Exhibit 1002-3181

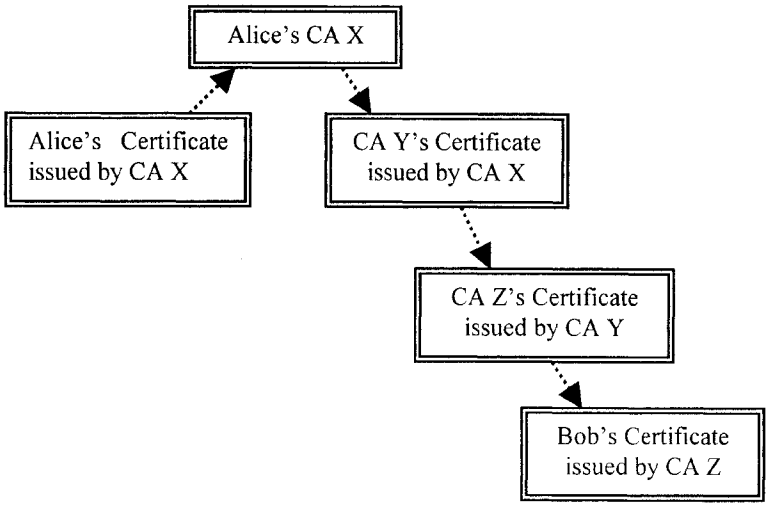


Fig. 3.2 A certification path from Alice to Bob

3.1.4 CA Arrangements

Certificate Hierarchies

In large organizations, it may be appropriate to delegate the responsibility for issuing certificates to several different certificate authorities. For example, the number of certificates required may be too large for a single CA to maintain; different organizational units may have different policy requirements; or it may be important for a CA to be physically located in the same geographic area as the people to whom it is issuing certificates.

It's possible to delegate certificate-issuing responsibilities to subordinate CAs. The X.509 standard includes a model for setting up a hierarchy of CAs like that shown in Fig. 3.3.

CSC ServiceWorks – Ex. 1005
Page 52 of 339

Petitioner Exhibit 1002-3182

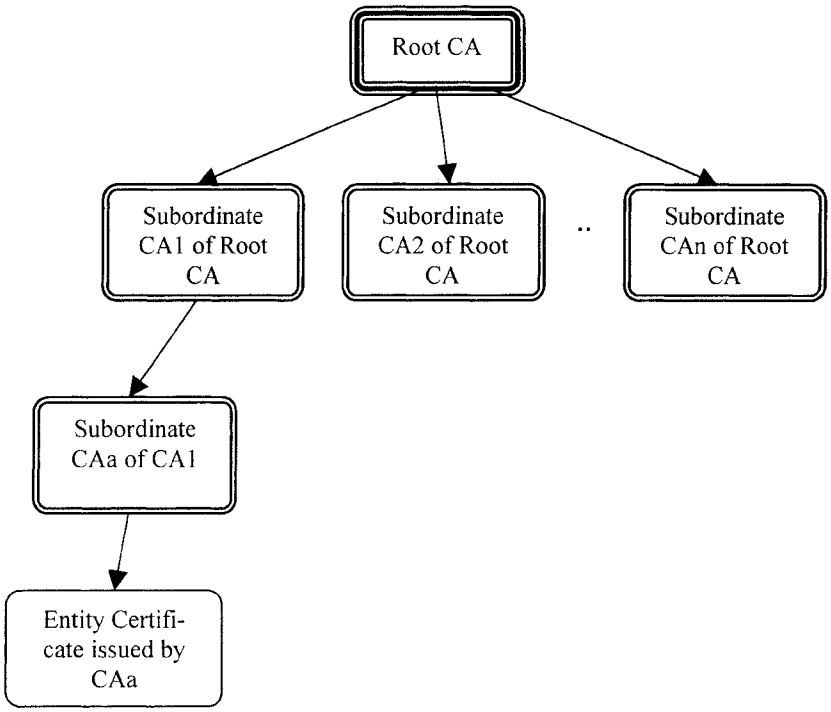


Fig. 3.3 Example of a hierarchy of certificate authorities

In this model, the root CA is at the top of the hierarchy. The root CA's certificate is a *self-signed certificate*, that is, the certificate is digitally signed by the same entity (the root CA) that the certificate identifies. The CAs that are directly subordinate to the root CA have CA certificates signed by the root CA. CAs under the subordinate CAs in the hierarchy have their CA certificates signed by the higher-level subordinate CAs.

Organizations have a great deal of flexibility in terms of the way they set up their CA hierarchies. Fig. 3.3 shows just one example; many other arrangements are possible.

Certificate Chains

CA hierarchies are reflected in certificate chains. A *certificate chain* is series of certificates issued by successive CAs. Fig. 3.4 shows a certificate chain leading from a certificate that identifies some entity through two subordinate CA certifi-

CSC ServiceWorks – Ex. 1005
Page 53 of 339

Petitioner Exhibit 1002-3183

cates to the CA certificate for the root CA (based on the CA hierarchy shown in Fig. 3.3).

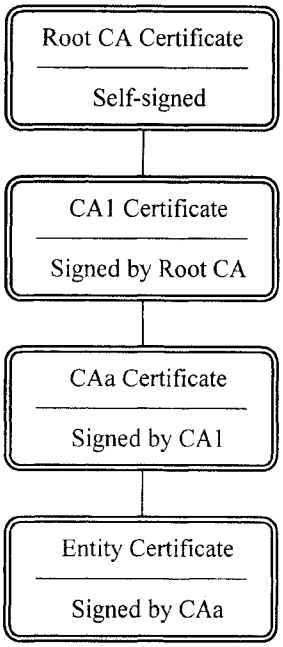


Fig. 3.4 Example of a certificate chain

A certificate chain traces a path of certificates from a branch in the hierarchy to the root of the hierarchy. In a certificate chain, the following occur:

- Each certificate is followed by the certificate of its issuer.
- Each certificate contains the name (DN) of that certificate's issuer, which is the same as the subject name of the next certificate in the chain.

In Fig. 3.4, the CAa certificate contains the DN of the CA1, that issued that certificate. CA1's DN is also the subject name of the next certificate in the chain.

- Each certificate is signed with the private key of its issuer. The signature can be verified with the public key in the issuer's certificate, which is the next certificate in the chain.

In Fig. 3.4, the public key in the certificate for the CA1 can be used to verify the CA1's digital signature on the certificate for the CAa.

CSC ServiceWorks – Ex. 1005
Page 54 of 339

Petitioner Exhibit 1002-3184

3.1.5 Validation

The other basic PKI operation is certificate validation. The information in a certificate can change over time. A certificate user needs to be sure that the certificate's data is true, that is, the user needs to *validate* the certificate. There are two basic methods of certificate validation. A PKI can use either or both methods.

- The user can ask the CA directly about a certificate's validity every time it is used. This is known as *online* validation.
- The CA can include a *validity period* in the certificate – a pair of dates that define a range during which the information in the certificate can be considered as valid. This is known as *offline* validation.

Verify a Certificate Chain

Certificate chain verification is the process of making sure a given certificate chain is well-formed, valid, properly signed, and trustworthy. A PKI usually uses the following procedure for forming and verifying a certificate chain, starting with the certificate being presented for authentication.

1. The certificate validity period is checked against the current time provided by the verifier's system clock.
2. The issuer's certificate is located. The source can be either the verifier's local certificate database (on that client or server) or the certificate chain provided by the subject (for example, over an SSL connection).
3. The certificate signature is verified using the public key in the issuer's certificate.
4. If the issuer's certificate is trusted by the verifier in the verifier's certificate database, verification stops successfully here. Otherwise, the issuer's certificate is checked to make sure it contains the appropriate subordinate CA, and chain verification returns to step 1 to start again, but with this new certificate. Fig. 3.5 presents an example of this process.

CSC ServiceWorks – Ex. 1005
Page 55 of 339

Petitioner Exhibit 1002-3185

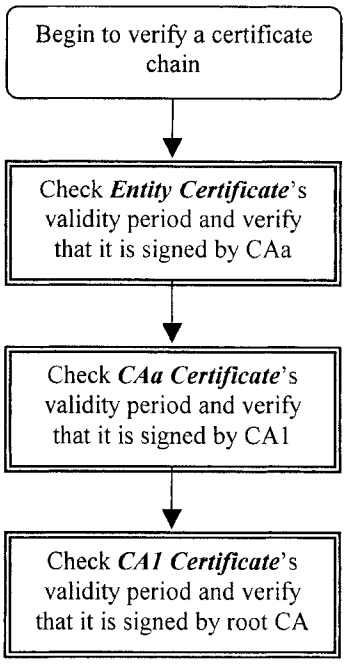


Fig. 3.5 Verifying a certificate chain all the way to the root CA

Certificate Revocation Lists (CRLs)

Closely related to the validation method is certificate *revocation*. Certificate revocation is the process of letting users know when the information in a certificate becomes unexpectedly invalid. This can occur when a subject's private key becomes compromised, or, more benignly, when a certificate's identifying information changes (e.g. the subject gets a new telephone number).

If a certificate is validated online with the CA every time it is used, then the revocation problem becomes trivial, as the CA can simply state that the certificate is no longer valid. However, when validity periods are employed, the certificate revocation method becomes critical (especially in the case of private-key compromise).

In the absence of online approaches, the most common revocation method uses *certificate revocation lists* (CRLs). A CRL is a list of revoked certificates that is signed and periodically issued by a CA. It is essential that the user check the latest

CSC ServiceWorks – Ex. 1005
Page 56 of 339

Petitioner Exhibit 1002-3186

CRL during validation to make sure that a certificate she is about to use has not been revoked.

One of the chief concerns with the CRL approach is what happens between the time when a CA receives notification that a certificate should be revoked and when the CA publishes its next CRL. Since the revoked certificate will only appear on the next CRL, any user checking the current CRL will not know of its revocation and will assume that the certificate is still valid. We call this the *CRL time-granularity problem.*

Another concern is the size of the CRL. A CA can be expected to certify thousands, or even hundreds of thousands, of subjects. While the rate of revocations for a given population is generally unpredictable, the CRLs for such CAs can be expected to grow very large. When a CRL is too large it can be difficult to retrieve by users, whose access to the CA may have limited bandwidth. Also, since CRLs are signed, their signatures need to be verified before the CRL can be used, and the time required to verify the signature on a large CRL and process its entries can become significant.

These problems have lead to several refinements of the CRL approach. One is to issue separate CRLs for different revocation reasons and/or for different certificate subjects. For example, the CA could issue one CRL for routine revocations (e.g., a change in a certificate subject's identifying information) and another CRL for revocations due to a security compromise. Similarly, a CA could issue one CRL for its end-user subjects and another for the other CAs it may certify. These measures have the effect of partitioning a large CRL into pieces that can be selectively digested. For example, a user might not be very worried about routine revocations and so would only need to check the security-compromise CRL. Also, when processing a certification path the user need only check the CA CRLs (until reaching the end of the path).

While these steps help reduce CRL sizes, they do little to alleviate the CRL time-granularity problem. Another measure has been proposed to address that problem: *delta-CRLs*. A delta-CRL is simply a (CA-signed) list of CRL changes that have occurred since the last full CRL was issued. Delta-CRLs allow revocation notifications to be issued more frequently, and so reduce the probability that a revoked certificate will be falsely validated. Delta-CRLs also help with the CRL size problem. A certificate validating system could start with a full CRL, and then need only process delta-CRLs as they are issued, updating its own copy of the full CRL.

3.1.6 Authentication

Authentication is the process of using a PKI. When a CA certifies an entity and a user then validates that certification, the entity is said to have been *authenticated.*

CSC ServiceWorks – Ex. 1005
Page 57 of 339

Petitioner Exhibit 1002-3187

A certificate can contain entity or nonentity information. When a certificate identifies an entity, it is called an *identity certificate*. Authenticating an identity certificate is called *identity authentication*.

Certificates that contain nonentity information, such as a permission or credential, are called *credential certificates*. Credential certificates identify things such as permissions (e.g., an access computer xyz), credentials (e.g., as a certified stock broker), or other attributes (e.g., as VP Marketing for "ABC Inc."). A credential certificate may or may not identify the entity to which the credential is attached. We call authenticating a credential certificate *credential authentication*.

In the context of network interactions, authentication involves the confident identification of one party by another party. Authentication over networks can take many forms. Certificates are one way of supporting authentication.

Network interactions typically take place between a client, such as browser software running on a personal computer, and a server, such as the software and hardware used to host a web site. *Client authentication* refers to the confident identification of a client by a server (that is, identification of the person assumed to be using the client software). *Server authentication* refers to the confident identification of a server by a client (that is, identification of the organization assumed to be responsible for the server at a particular network address).

Client and server authentication are not the only forms of authentication that certificates support. For example, the digital signature on an email message, combined with the certificate that identifies the sender, provide strong evidence that the person identified by that certificate did indeed send that message. Similarly, a digital signature on an HTML form, combined with a certificate that identifies the signer, can provide evidence, after the fact, that the person identified by that certificate did agree to the contents of the form. In addition to authentication, the digital signature in both cases ensures a degree of non-repudiation, that is, a digital signature makes it difficult for the signer to claim later not to have sent the email or the form.

3.1.7 Limitations of PKI Authentication

Whenever authentication is performed using the PKI, whether online or offline, it is called *in-band authentication*. Authentication performed using more traditional methods, such as over the telephone or physically meeting someone, is called *out-of-band authentication*. The goal of every PKI is to minimize the need for out-of-band authentication.

It is unlikely that out-of-band authentication can ever be completely eliminated. At the very least, a person wishing to use a PKI needs to first have their identity and/or credentials verified by their CA. This initial verification cannot be per-

CSC ServiceWorks – Ex. 1005
Page 58 of 339

Petitioner Exhibit 1002-3188

formed using the PKI, since there is no other CA to vouch for the person's identity/credentials. Thus the bootstrapping process requires out-of-band authentication. Also, different PKIs require different degrees of out-of-band authentication as identity and credential information changes over time and needs to be updated.

The extent to which out-of-band authentication is required in a PKI is partly a result of how much the PKI's designers want to provide *irrefutability*. A signature made by Alice is said to be irrefutable if Alice can not, at a later date, deny that she did in fact make the signature. If the PKI is to be used as the foundation of an electronic replacement for paper-based signatures, then irrefutability is an important consideration. In general, the more out-of-band contact Alice has with her CA, the less she will be able to engage in such fraud.

3.1.8 Registration Authorities

Interactions between entities identified by certificates (sometimes called *end entities*) and CAs are an essential part of certificate management. These interactions include operations, such as registration for certification, certificate retrieval, certificate renewal, certificate revocation, and key backup and recovery. In general, a CA must be able to authenticate the identities of end entities before responding to the requests. In addition, some requests need to be approved by authorized administrators or managers before being serviced.

As previously discussed, the means used by different CAs to verify an identity before issuing a certificate can vary widely, depending on the organization and the purpose for which the certificate will be used. To provide maximum operational flexibility, interactions with end entities can be separated from the other functions of a CA and handled by a separate service called a *registration authority* (RA).

An RA acts as a front end to a CA by receiving end entity requests, authenticating them, and forwarding them to the CA. After receiving a response from the CA, the RA notifies the end entity of the results. RAs can be helpful in scaling a PKI across different departments, geographical areas, or other operational units with varying policies and authentication requirements.

3.1.9 Certificates and the LDAP Directory

The lightweight directory access protocol (LDAP) for accessing directory services supports great flexibility in the management of certificates within an organization. System administrators can store much of the information required to manage certificates in an LDAP-compliant directory. For example, a CA can use information in a directory to pre-populate a certificate with a new employee's legal name and other information. The CA can leverage directory information in other ways to is-

CSC ServiceWorks – Ex. 1005
Page 59 of 339

Petitioner Exhibit 1002-3189

sue certificates one at a time or in bulk, using a range of different identification techniques depending on the security policies of a given organization. Other routine management tasks, such as key management and renewing and revoking, can be partially or fully automated with the aid of the directory.

Information stored in the directory can also be used with certificates to control access to various network resources by different users or groups. Issuing certificates and other certificate management tasks can thus be an integral part of user and group management.

3.1.10 Key Management

Before a certificate can be issued, the public key it contains and the corresponding private key must be generated. Sometimes it may be useful to issue a single person one certificate and key pair for signing operations, and another certificate and key pair for encryption operations. Separate signing and encryption certificates make it possible to keep the private signing key on the local machine only, thus providing maximum non-repudiation, and to back up the private encryption key in some central location where it can be retrieved in case the user loses the original key or leaves the company.

Keys can be generated by client software or generated centrally by the CA and distributed to users via an LDAP directory. There are tradeoffs involved in choosing between local and centralized key generation. For example, local key generation provides maximum non-repudiation, but may involve more participation by the user in the issuing process. Flexible key management capabilities are essential for most organizations.

3.2 X.509

3.2.1 Introduction

X.509 [3.65] is the authentication framework designed to support X.500 directory services [3.64]. Both X.509 and X.500 are part of the X series of international standards proposed by the ISO and ITU. The X.500 standard is designed to provide directory services on large computer networks. X.509 provides a PKI framework for authenticating X.500 services.

The first version of X.509 appeared in 1988, making it the oldest proposal for a worldwide PKI. This, coupled with its ISO/ITU origin, has made X.509 the most

CSC ServiceWorks – Ex. 1005
Page 60 of 339

Petitioner Exhibit 1002-3190

widely adapted PKI. There are at least a dozen companies worldwide that produce X.509-based products, and that number is growing. Visa and MasterCard have adapted X.509 as the basis for their secure electronic transaction standard (SET) [3.55]. Netscape's famous World Wide Web software also uses X.509. And there are numerous X.509-based products available from companies, such as Entrust and TimeStep that support corporate intranets. Efforts are currently underway to design an X.509-based PKI that will support a global network such as the Internet. Along with PGP [3.67], X.509 is the only PKI system that has yet to be put into practical use.

3.2.2 The X.509 Standard

X.500

A full understanding of X.509 PKIs requires some basic knowledge of the X.500 directory that X.509 was originally designed for. The X.500 directory[3.64] is very similar to a telephone directory where, given a person's name, one can find auxiliary information about that person. However, X.500 provides more than just a name, address, and phone number. An entry in an X.500 directory can contain a host of attributes, such as the name of the organization the person works for, their job title and their email address, to name a few. An X.500 directory entry can represent any real-world entity, not just people but also computers, printers, companies, governments, and nations. The entry can also contain the certificate specifying the entity's public key.

Distinguished Name

To support looking up entries in the directory, each entry is assigned a globally unique name, called a *distinguished name* or DN. To help ensure their uniqueness, these names are assigned in a very specific fashion. The X.500 directory is arranged in a hierarchical fashion, call the *Directory Information Tree* or DIT (see Fig. 3.6).

CSC ServiceWorks – Ex. 1005
Page 61 of 339

Petitioner Exhibit 1002-3191

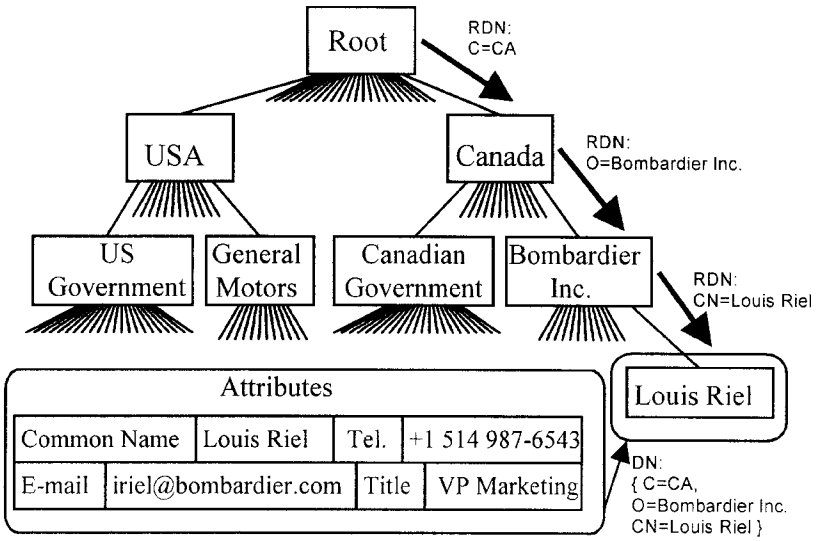


Fig. 3.6 The X.500 directory information tree

Each node, or *vertex*, in the tree has one parent (except the root vertex) and any number of children. Each vertex, except the root, is assigned a *relative distinguished name* (RDN) that is unique among all the vertex's siblings. The RDNs of each of the vertex's ancestors are concatenated with the vertex's own RDN to form the entry's DN. Fig. 3.6 illustrates this process. Under the root vertex there is an entry for each country in the world. These entries are assigned an RDN that is the country's unique two-letter code assigned to it by the ISO. Beneath each country's vertex are entries for all of the country's organizations, such as its government, its states or provinces, and federally-chartered companies. Each of these is assigned a unique RDN that is the name of the organization. Finally, each organization creates entries for all of its employees, and for other entities the organization might control. Each of these is also assigned a unique RDN. In our example, Mr. Louis Riel works for Bombardier, a Canadian company. Bombardier assigns an RDN to Mr. Riel, that is simply his name (specified as his common name, abbreviated as CN in the figure). Bombardier was itself assigned an RDN, Organization = Bombardier by Canada, designating it as the organization named Bombardier, and Canada's RDN is it's two-letter country code, Country = CA. Mr. Riel's DN is thus the concatenation of these RDNs, starting from the root: Country = CA, Organization = Bombardier, CommonName = Louis Riel.

CSC ServiceWorks – Ex. 1005
Page 62 of 339

Petitioner Exhibit 1002-3192