VMC Command	Code	Sub-command	VMC Data	Dispenser Response
EXPANSION COMMAND	5FH / 77H **FTL** SEND BLOCK	FCH	Y1-Y33	None

The VMC is sending data to the dispenser whose destination address will always be (58H/70H). Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 = Destination address of command & data (58H/70H)
Y2 = Block #
Y3 - Y33 = Data (maximum of 31 bytes)

VMC Command	Code	Sub-command	VMC Data	Dispenser Response
EXPANSION COMMAND	5FH / 77H **FTL** OK TO SEND	FDH	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/70H). Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 = Destination address of command (58H/70H)
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	Dispenser Response
EXPANSION COMMAND	5FH / 77H FTL REQ TO SEND	FEH	Y1-Y5	Z1 (immediate or POLLed)

The VMC is requesting to send data to the dispenser whose destination address will always be (58H/70H). Note that all FTL Commands / Responses are defined in Section 2.6.

Y1 = Destination address of command (58H/70H)
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/70H)

or

Z1 = 1CH which indicates RETRY / DENY
Z2 = Destination address of response
Z3 = Source address of response (58H/70H)
Z4 = Retry delay

VMC Command	Code	Sub-command	VMC Data	Dispenser Response
EXPANSION COMMAND	5FH / 77H DIAGNOSTICS	FFH	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.

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.

Section 11
Age Verification Device
VMC/Peripheral Communication Specifications

11.1 Introduction

Due to legal restrictions, a variety of products are only allowed to be vended via vending machines by checking the customers age. The age and the rules vary from country to country.

This is i.e. related in some countries to cigarettes or alcoholic products. Some services or product contents may restrict a different age, related to the vending machine, this needs different ages to be checked within the same machine.

Age verification may be done with different electronic means, i.e. public cashless systems, which know the card users age, i.e. biometric systems, i.e. ID-card-readers or driving license readers, etc.

A common and state of the art usage in some countries is a public cashless system working as an Age Verification Device. Therefore it is good practice to define first an interface of commands as an addition to the cashless devices.

Second as MDB describes two cashless devices, which in some machines may be both only cashless readers, it is necessary to define an Age Verification Device only as an additional device, allowing the two readers within the machine working as before. The cashless readers which run as a multi-function device may choose to run the additional set of commands or respond as slaves on two peripheral addresses – the cashless 1 or 2 and the Age Verification Device address.

Therefore this paper describes two additional diagnostic commands for the cashless systems, to work as age verification devices. Second this paper describes a command set for an age verification device, which uses only two commands for age verification purpose -- the structure of these two commands is similar to the cashless diagnostic commands, therefore allowing any VMC, to use the same command interface for cashless and Age Verification Device as well.

These command are not bound to a cashless-transaction and may be therefore be used, if verification is done by other cards (i.e. without payment functions.) These command are independent of the cashless function (i.e. payment out of order, transaction memory full, ...) and do not interfere with the payment sequences. Sequences at MDB are changed slightly only.

Observing the age verification is done by the VMC. Only the VMC knows, what type of products it sells. The cashless device delivers the only information to VMC, whether the cashless media finds a valid age. The cashless device will approve a payment always, when the VMC requests this (MDB command request vend). The cashless device will not deny a payment, even if the age verification is not found. This allows simultaneous vend of age protected and free products from a vending machine.

After each power on or after reception of MDB-Reset the cashless device or Age Verification Device will ignore age verification. First after the VMC switches on age verification with the MDB-command "**DRAVP**" (Diagnostic Request Age Verification On) and Y4>0, verification cards will be checked. Only in this case the cashless device or Age Verification Device sends responses to the second new command "**DRAVS**" (Diagnostic Response Age Verification Status) to the VMC.

11.2 VMC Commands

The Age Verification Device uses the MDB address

0x68 (the next address after the second cashless device)

It implements a command set similar to a cashless device with a reduced command dictionary. All the not used commands are reserved for further use to hold the software functions compatible to a cashless subdevice.

The following describes the age verification commands common to the standalone Age Verification Device as well as a subdevice within the cashless device, whereas chapter 4 describes the additional setup commands for the standalone age verification device. Note, that these commands are the same commands as for a cashless device.

11.2.1 General Format EXPANSION Diagnostic

The MDB command EXPANSION Diagnostic allows transfer of manufacturer specific information between cashless reader and VMC. For transmission of the age verification information, the EXPANSION diagnostic command will be used. While implemented in a cashless device, this is similar to a virtual subdevice within the reader, whereas, when used with a separate address, these may be treated as normal standardized commands.

General format:

expansion (17H) (67H) (6FH)	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.

11.2.2 Switch On / Off of Age Verification

Diagnostic Request Age Verification On/Off (**DRAVP**)

This command is used to switch On or Off the age verification and to setup the minimum testing age within the device. While in state "on" each inserted media is checked and the result is messaged to the VMC.

After the VMC is powered on, the command DRAVP will be sent at least with Y4 = 0x00 or Y4 = 0xff to the age verification device.

Expansion	Diagnostics Request	Age verifi-cation On/Off	Length	Age	Ident
(17H) (67H) (6FH)	(FFH) Y1	(0x05) Y2	Y3	Y4	Y5-Y9

Diagnostics Response	Age verifi-cation On/Off	Length	Feature byte	Ident
(FFH) Z1	(0x05) Z2	Z3	Z4	Z5-Z9

Y1 : DIAGNOSTICS Request

Y2 : Age verification on/off

Y3 : Length, the number of bytes of this command, not including Y1-Y3, therefore set to 6.

Y4 Age

Y4 = 0x00	Switch off age verification. Additionally informs the card reader, that the VMC software supports age verification, but age verification is not necessary for any product
0x00<Y4<0x64	Level for age verification (0x01 - 0x63 = 1..99 years). Additionally informs the card reader, that the VMC software supports age verification and age verification is necessary
0x63<Y4<0xFF	Reserved for future use
Y4 = 0xFF	Informs the card reader, that the VMC software supports age verification and that age verification will be switched on at xx.xx.xxxx automatically and the level of age will be changed to the default checking.

Y5-Y9 Ident "DRAVP" (hex 0x44 0x52 0x41 0x56 0x50)

Used to prevent misinterpretation of this command and to separate it against possible other manufacturer defined 17 FF 05 commands.

The Age Verification Device takes the given age and responses with the diagnostic response. The VMC will detect, that an Age Verification Device is connected (or built in as a subdevice in cashless), which is doing age verification.

As the verification of the requested minimum age is depending of the (later) inserted media, the requested minimum age is only set to the age verification device. Whether a verification is really possible, will be messaged later within the DRAVS command.

The DRAVP command will be sent by VMC always after power up and after each RESET within the known initializing sequence to the Age Verification Device (cashless or stand alone). If the VMC is aware of a necessary age, the minimum age will be set to a value > 0, i.e. for today's cigarette vendor to 0x12 = 18.

If different products with different age levels are sold, the VMC may send this command before each vend transaction and temporarily change age due to selected product minimum age. Switch off of the age verification is only allowed, if all selections of the vendor do not require a verification.

The age verification device responds with:

Z1 :	DIAGNOSTICS Response	
Z2 :	Age verification on/off	
Z3 :	Length, the number of bytes of this command, not including Z1-Z3, therefore set to 6.	
Z4	Feature Byte	
	b0 = 0	A customer card is not in reading position, but may be inserted (refer to b7)
	b0 = 1	A customer card is in reading position.
	b1...b6	Reserved, should be set to 0
	b7= 0	A customer card is not inserted
	b7= 1	A customer card is inserted, but may not be in reading position (refer to b0)
Z5-Z9	Ident "DRAVP" (hex 0x44 0x52 0x41 0x56 0x50)	

11.2.3 Check of Age Verification

Diagnostic Request Age Verification Status (DRAVS)

If the VMC activated the age verification with DRAVP, the Age Verification Device is checking each inserted media for age information and sends after insertion the DRAVS response to the VMC. The VMC may send the command itself to the age verification device, to get an actualisation of the status. The verification device answers with the actual response. The command may be sent in all MDB states (especially within cashless devices).

expansion (17H) (67H) (6FH)	Diagnostics Request (FFH) Y1	Age verifi-cation Status (0x06) Y2	length Y3	Features Y4	Ident Y5-Y9

Y1 *: DIAGNOSTICS Request*

Y2 *: Age Information*

Y3 *: length, the number of bytes of this command, not including Y1-Y3, therefore set to 6*

Y4 *Feature bits*
b0..b7: Reserved, should be set to 0

Y5-Y9 *Ident "DRAVS" (hex 0x44 0x52 0x41 0x56 0x53)*

If the VMC has activated the age verification with the DRAVP, each inserted media will be checked for age information and after insertion, the DRAVS response will be sent to the VMC.

Diagnostics Response (FFH) Z1	Age (0x06) Z2	length Z3	feature byte 1 Z4	feature byte 2 Z5	Ident Z6-Z10

Z1 : DIAGNOSTICS Response

Z2 : Age verification status

Z3 : length, the number of bytes of this command, not including Z1-Z3, therefore set to 7

b0=0: A customer card is not in reading position, but may be
b0=1: A customer card is in reading position

b1=0: Age information is not available on the customer card
b1=1: Age information is available on the customer card

b2=0: Age verification is not possible (MSAM error or no MSAM)
b2=1: Age verification is possible (MSAM ok and present)

b3=0: The age level from DRAVP command can't be checked
b3=1: The age level from DRAVP command (or a higher value) can be checked

b4=0: The customer is not allowed to buy the product, because the age information on the card is less than the value in DRAVP
b4=1: The customer is allowed to buy the product, because the age information on the customer card is equal or greater than the value in DRAVP

b5=0: reserved, should be set to zero
b6=0: Age verification information *) is valid

b6=1: Age verification information *) is invalid and set to 0, because age verification is under progress (busy)

b7=0: A customer card is not inserted
b7=1: A customer card is inserted, but may not be in reading position (refer to b0)

b0...b3: Reserved, should be set to 0

b4=1: Age verification done by private ident media 1

b5=1: Age verification done by private ident media 2
b6=1: Age verification done by driving license reader

b7=1: Age verification done by public cash card

Z6-Z10 Ident "DRAVS" (hex 0x44 0x52 0x41 0x56 0x53)

*) Age verification information refers to feature byte 1 (b1…b4) and feature byte 2 (all bits)

**) must be valid only, if age verification is positively checked (b4=1 of feature byte 1)

If a DRAVS response with positive checked age information sent from the age verification device, the VMC will enable the vend for selected product for typically 30 seconds. This duration should be programmable.

11.3 MDB Interface

11.3.1 MDB initializing

The general MDB-session consists of the known init-sequence as well as the polling sequence. The init sequence is extended with the DRAVP command.

RESET – 10h

POLL – 12h
To obtain "JUST RESET" response

SETUP CONFIGURATION DATA – 11 00h
To send the VMC's configuration data and obtain the reader's data

SETUP MAX/MIN PRICE – 11 01h
To send the maximum and minimum prices in the VMC. (Reader Level 01/02 syntax, 16 bit credit).

EXPANSION REQUEST ID – 17 00h
To obtain additional reader 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)
To send the maximum and minimum prices in the VMC. (Reader Level 03+, 32 bit credit).

DRAVP – 17 ff 05 06 Age 'D' 'R' 'A' 'V' 'P' *)
switch on or off youth protection, set age level to be checked

POLL – 12h
To obtain "DRAVP" response

**)

READER ENABLE – 14 01h
To enable reader (if desired)

POLL – 12h
To obtain further responses, loop it.

*) the DRAVP may be sent in the following contents as often as needed, to switch on or off the verification or to change the verification age.

**) the cashless reader as well as the Age Verification Device are required to check the actual date and it is suggested for the VMC, to send an expansion diagnostic date/time command to actualize the date within the age verification device.

11.3.2 MDB Polling Loop, Vend Sequence

The polling loop will lead to a vend following the known sequence and is extended with an optional DRAVS.

Customer inserts card

POLL – 12h
DRAVS, card present, age verification status

POLL – 12h
Begin Session (value = 0, > 0 or –1). *)

Customer presses selection and/or inserts money.

VEND REQUEST – 13 00 xx xx xx xx yy yyh **)
ACK (xx = vend price, yy = selection number)

POLL – 12h
looped until vend approved or denied is sent. During this loop, display messages should be shown on the vending machines display

VEND SUCCESS/FAILED – 13 02 yy yyh or 13 03h **)
vend is completed

SESSION COMPLETE – 13 04
close session

POLL – 12h
End session

*) only if cashless is used, independent of cashless credit

**) only if cashless payment is done

All answer will be seen in the known format, the new command DRAVS is enabling a cash vend, if the "age valid" (b4 = 1) is set.

11.4 Age Verification Device Command/Response Formats

11.4.1 Reset

RESET (68H)

Reader response:

No Data response

11.4.2 Setup

SETUP (69H)	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 actual used level is 1

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

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 Age Verification Device is responding to a SETUP – Configuration data request from the VMC.

Z2 : 01 – the actual used level

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.

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 age verification device.

All pricing information sent between the VMC and the Age Verification Device 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 supersedes the payment reader's default NON-RESPONSE time defined in section 7.5 if the value reported here is greater.

Z8 : Miscellaneous Options – xxxxyyyy

11.4.3 Poll

POLL (6AH)

The POLL command is used by the VMC to obtain information from the verification device. In addition to an ACK, the VMC may receive the following POLL responses from the verification device.

Reader responses:

Just Reset (00H) Z1

Z1 : JUST RESET
Indicates the device 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

Display Request (02H) Z1	Display Time Z2	Display Data Z3-Z34

Z1 : DISPLAY REQUEST
The Age Verification Device 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 Age Verification Device may overwrite the message before the time has expired.

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

Z1 : PERIPHERAL ID
Age Verification Device 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 to b31 not used (should be set to 0)

Malfunction / Error	Error Code
(0AH) Z1	Z2

Z1 : MALFUNCTION/ERROR
The Age Verification Device is reporting a malfunction or error.

Z2 : Error Code - xxxxyyyy

Transient Error Handling
The error will be reported to the VMC until it has been ACKnowledged. The error state will be cleared in the age verification device, 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 Age Verification Device is still functional, multi-message responses will allow normal responses in addition to the error report.

Time/Date Request (11H)

Z1

Z1 : TIME DATE REQUEST
In certain circumstances it will be necessary to synchronize the real time clock of the Age Verification Device with real time clock of the VMC. The Age Verification Device 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 age verification device.

11.4.4 Expansion commands (request ID)

Expansion (6FH)	Request ID (00H) Y1	Manufacturer Code Y2-Y4	Serial Number Y5-Y16	Model Number Y17-Y28	Software Version Y29-Y30

Y1 : REQUEST ID
The VMC is requesting Age Verification Device identification information. The information included above (Y2-Y30) provides the Age Verification Device 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, "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.

Age Verification Device response:

Peripheral ID (09H) Z1	Manufacture Code Z2-Z4	Serial Number Z5-Z16	Model Number Z17-Z28	Software Version Z29-Z30	Optional Feature Bits Z31-Z34

11.4.5 EXPANSION - Write Time/Date File

Expansion (6FH)	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 Age Verification Device 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.

11.4.6 EXPANSION - Diagnostics

Expansion (6FH)	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.

Age Verification Device 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.

11.5 Age Verification Device Non-Response Time

The default maximum non-response time for the Age Verification Device is 5 seconds. This is the maximum time for which an Age Verification 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 Age Verification Device Configuration Data supersedes this default value if Z7 is greater.

.

11.6 Age Verification Device Power Requirements

The current draw for any Age Verification 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.

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).
>
> **FFFF**h 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.

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 l'Afrique de l'Ouest.

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].

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].

Table A.1 (Continued)

ENTITY	Currency	Code		Decimal
		Alphabetic	Numeric	Position
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.

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.

Table A.1 (Continued)

ENTITY	Currency	Code		Decimal
		Alphabetic	Numeric	Point
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)

ENTITY	Currency	Code		Decimal
		Alphabetic	Numeric	Point
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)

ENTITY	Currency	Code		Decimal
		Alphabetic	Numeric	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

Table A.1 (Continued)

ENTITY	Currency	Code		Decimal
		Alphabetic	Numeric	Point
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.

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].

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

Table A.1 (Continued)

ENTITY	Currency	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).

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.

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.)

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
	Ekwele	EQE*	-	12/89

* Non ISO code
# Change in country name

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	Guinea Escudo	GWE	-	Between 1978-1981
ICELAND	Old Krona	ISJ*	-	1989/1990
ISRAEL	Old Shekel	ILR*	-	1989/1990
	Pound	ILP	-	Between 1978-1981
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

* Non ISO code

Table 3 (Continued)

ENTITY	Historic Currencies	Code	Numeric	WD
MOZAMBIQUE	Mozambique Escudo	MZE	-	Between 1978-1981
NICARAGUA	Cordoba	NIC	-	10/90
PERU	Sol	PES	-	02/86
	Inti	PEI	-	07.91
	Sol	PEH*	-	1989/1990
POLAND	Zloty	PLZ	616	01/97
ROMANIA	Leu A/52	ROK*	-	1989/1990
SOUTH AFRICA	Financial Rand	ZAL	991	03/95
SOUTHERN RHODESIA#	Rhodesian Dollar	RHD	-	Between 1978-1981
SPAIN	Spanish Peseta ("A" Account)	ESA	996	Between 1981-1983
	(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
	Old Shilling	UGW*	-	1989/1990
UKRAINE	Karbovanet	UAK	804	09/96

* Non ISO code
# Change in country name.

Table 3 (Continued)

ENTITY	Historic Currencies	Code	Numeric	WD
URUGUAY	Old Uruguay Peso	UYN*	-	12/89
	Uruguayan Peso	UYP	-	03/93
VIETNAM	Old Dong	VNC*	-	1989/1990
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

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

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.

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

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.

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.

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
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.

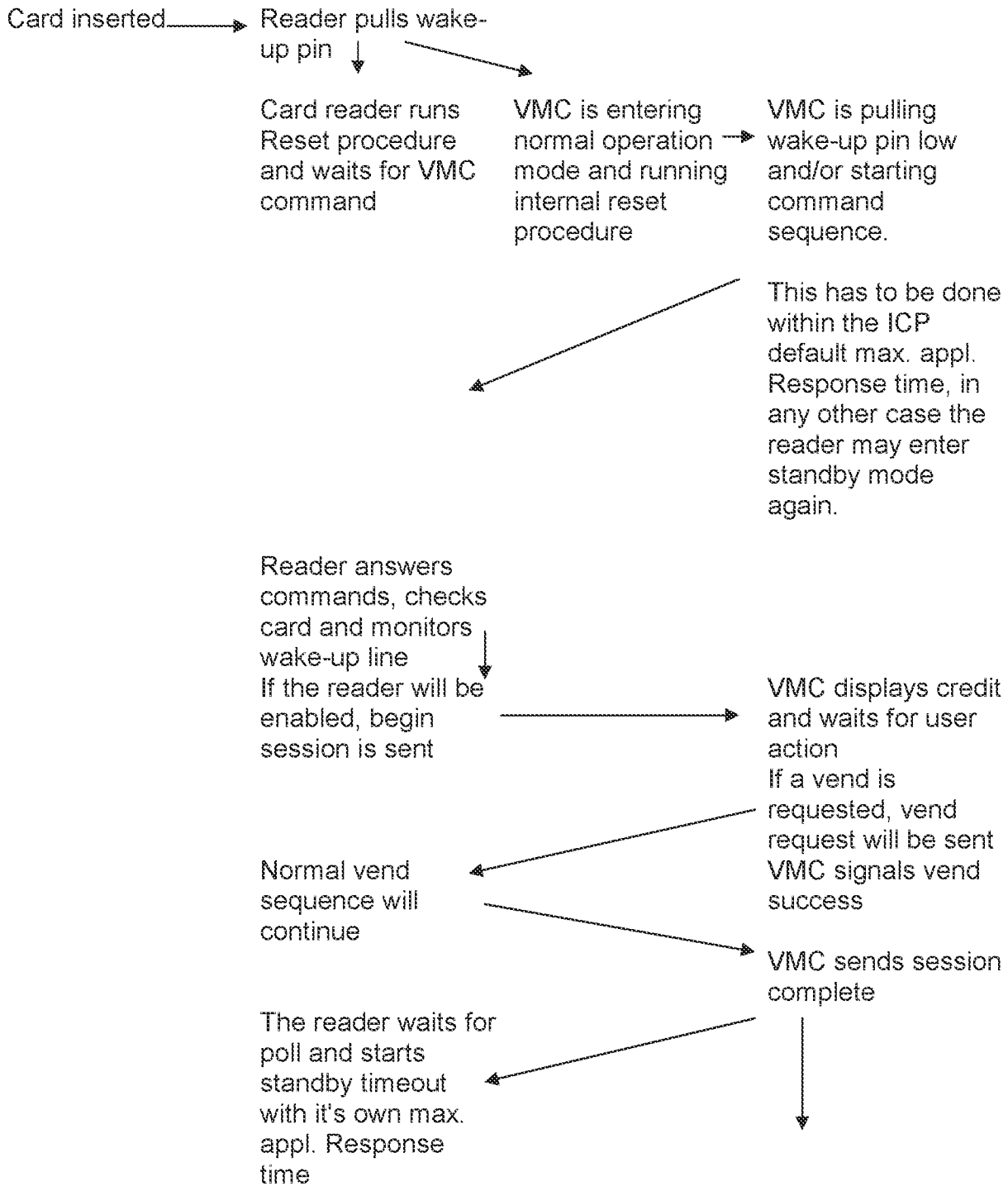
The reader should be in a power saving mode after this timeout period where power consumption is less than 10 uA.

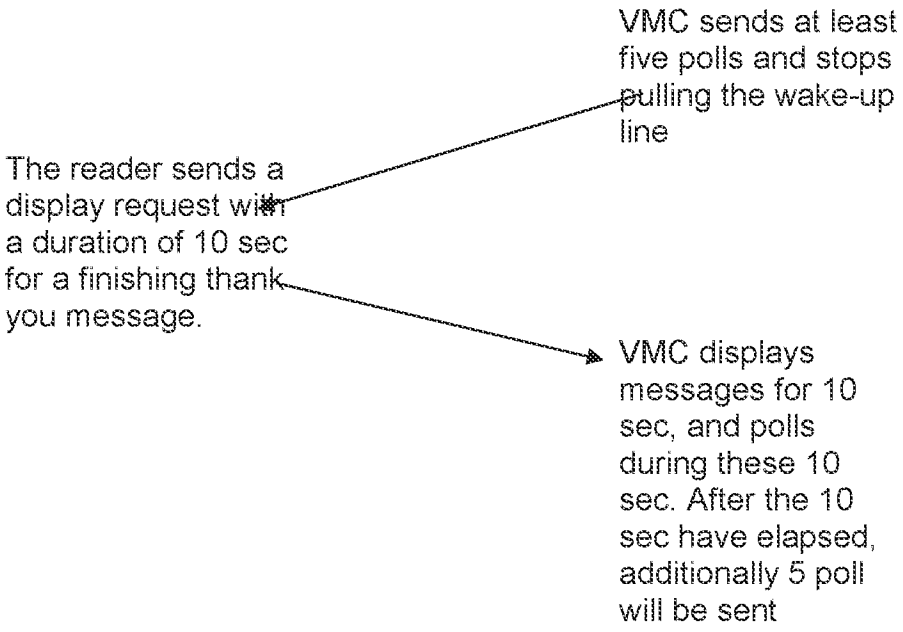
To allow the reader holding VMC operating, at least 5 poll have to be sent, after the cancel session or session complete. If any one of these polls is answered different with only a ACK, 5 polls have to be sent again. Note, that if a display message is sent, display time is added!

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.

A2.5 Session Example



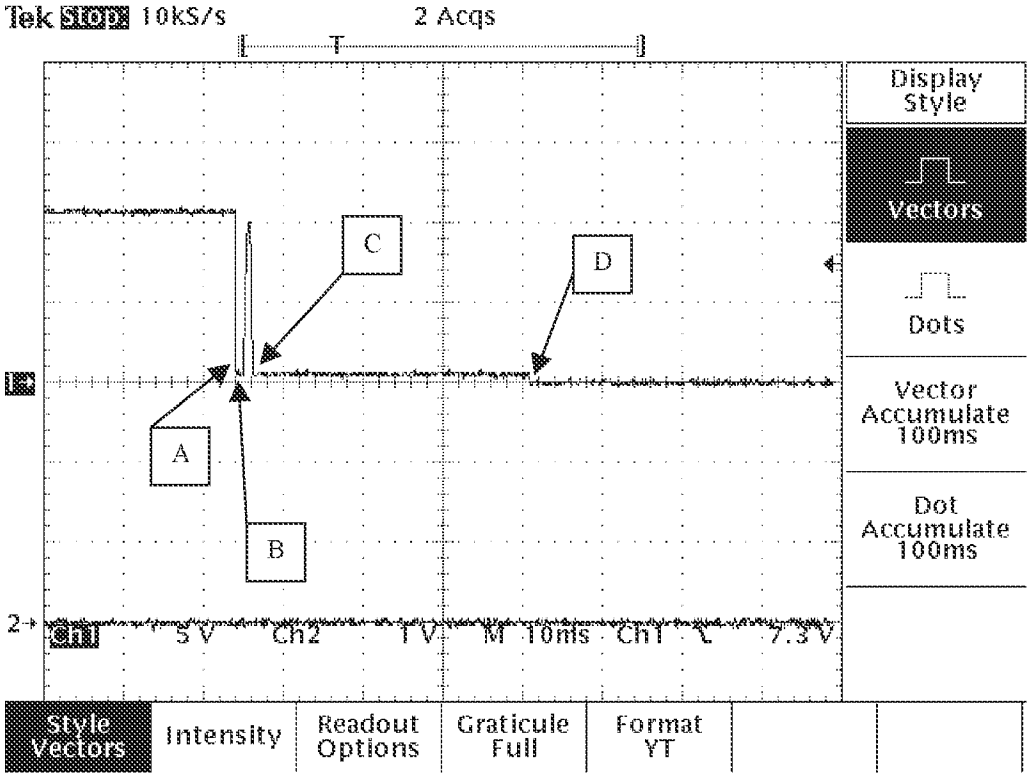


A2.6 Hardware Considerations

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 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.)

(this page intentionally left blank)

Appendix 3

MDB Recommended "Best Practices"

The following sections make recommendations that are intended to help reduce compatibility issues. Note that when developing a device you should not assume other devices or VMCs will follow these recommendations. Your device or VMC must meet the full MDB specifications!

1. **Physical Connections (Power/Voltage/Connection)**
2. **Timing Considerations (Lowest Level/Time-out)**
3. **Commands, Repetition, ACK, NAK**
4. **Logical Level, Processing**

1. Physical Connections (Power/Voltage/Connection)

Voltage specification (General)

Verify that the VMC meets the min MDB voltage at max load with the min input line voltage.

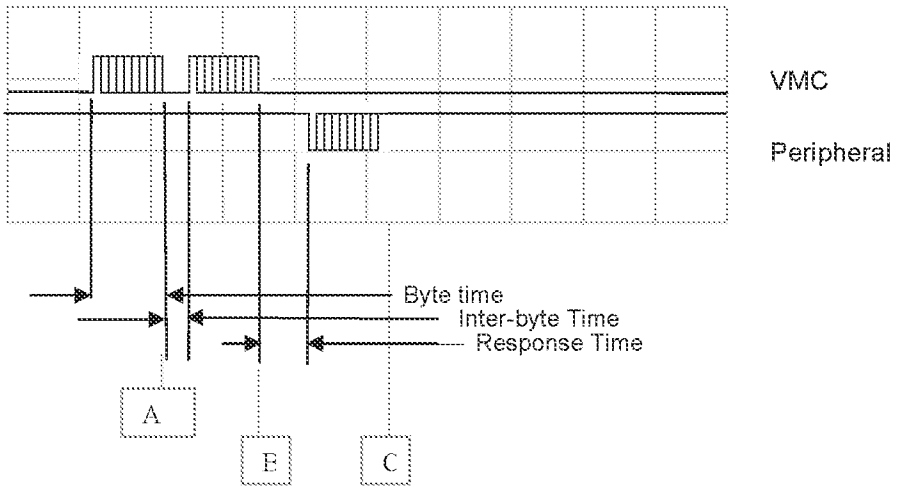
2. Timing Considerations (Lowest Level/Time-out)

Timing Considerations (General)

To avoid timing issue (Section 3.1 Timing Definitions) it is recommended that you allow for some margin in your design. See table below:

Item	MDB Specification	Tolerated values
Communication startup	200ms	500ms
Communication response time (when waiting for a response)	5ms max	20ms*
Communication response time (when sending a response)	5ms max	4ms
Interbyte time (when receiving data)	1ms max	5ms*
Interbyte time (when sending data)	1ms max	0.8ms
Non-Response time (the time the device may be busy performing other processes. I.e., validating coins)	Varies per device	Plus the time between polls
Application Non-Response time (time that can be reprogrammed to be different from the default Non-Response time.	Varies per device	Plus the time between polls

*Using the tolerated values will provide compatibility with older equipment manufactured under the EVMMA version of the MDB specification that had the Communication response time at 20ms and Interbyte time at 5ms. The transmitting device must always use the values of the MDB specification.



Please note, that the receiving device at the bus (master or slave) will get a receive interrupt (using standard UART devices) only after the byte is fully transmitted. These are the positions A, B, and C in the above diagram.

Therefore, the receiving device needs to set a higher value for the interbyte timeout, because it needs to add at least the transmission time for one byte (which is 1 start bit + 9 data bits + 1 stop bit at a rate of 9600 baud equal 1.2 ms). The same happens

for the response timeout, because the response is first detected, while the first byte is fully received.

Another common implementation error is checking the response timeout after the whole response message is received. This will never work because if, for example, the response is more than 5 bytes, the transmission time for 5 bytes will be more than 5 ms and will always timeout.

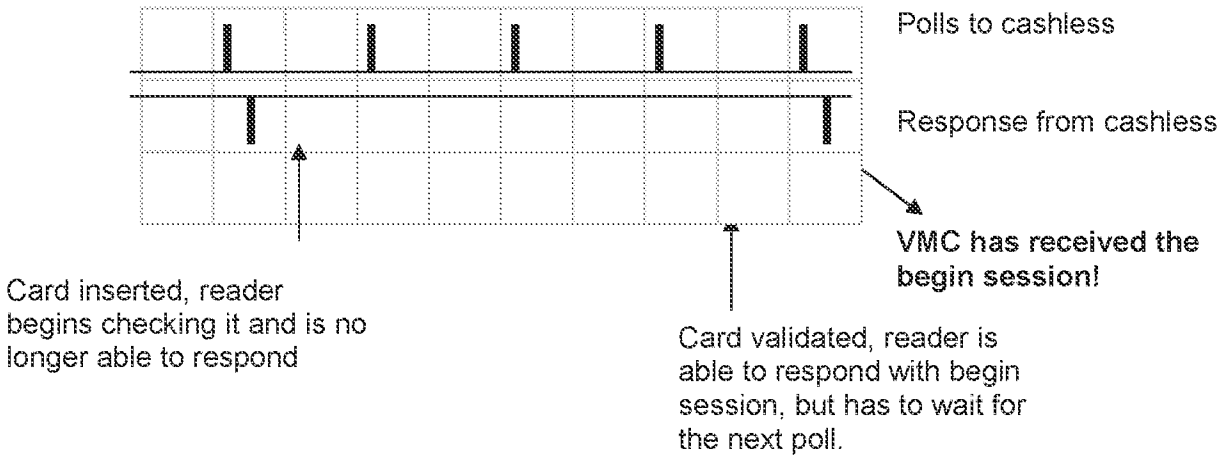
POLL Frequency (General)
Section 2.4.3 states, "Each peripheral should be polled every 25-200 milliseconds." However, the VMC is likely to stop communication during a vend or at other times when it does not need to communicate with the peripherals. Note that this may cause the peripheral(s) to RESET, see "Non-communication Time-out"-section in this document.

Because of this, poll frequency is not as important as many people think it is.

While not specifically prohibited, polling at a high rate while waiting for a response will usually delay the response, as the peripheral will have to service the POLL. Polling at a very low frequency, however may decrease coin or bill acceptance rate.

For all devices, the recommended VMC POLL frequency is 125ms - 200ms.

Example for a cashless device card acceptance:

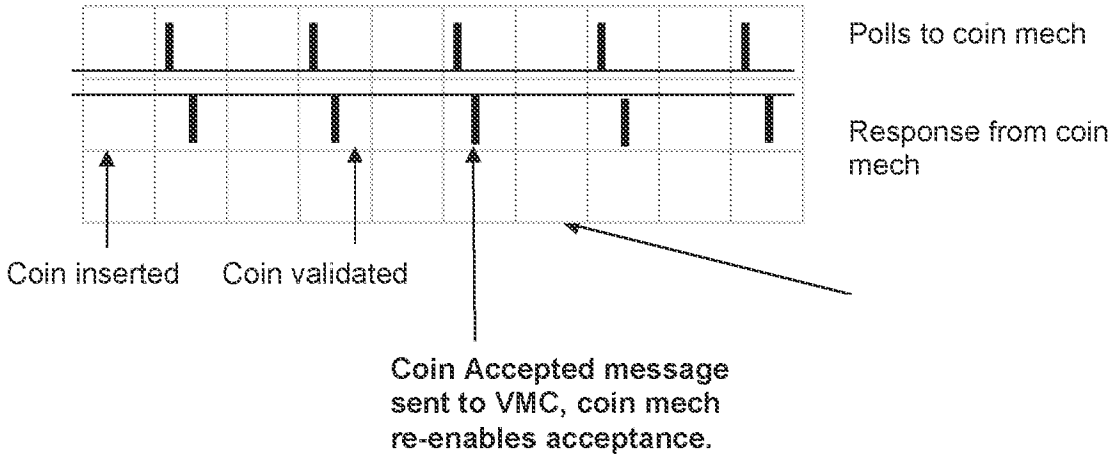


As shown in the above diagram, the time from card insertion to credit being displayed on the vending machine is not specifically related to the polling rate. After the card is inserted, the card reader validates the card. During this time, some card readers are no longer able to answer the poll, others answer with an ACK only.

When card validation is finished, the reader is ready to send the begin session, which will result in the balance of the card being displayed on the VMC. Obviously, this and only this depends on polling frequency. The time to the next poll has to be added to the validation time to get the maximum time before the credit is displayed.

Please note that some readers may need significant processing time to answer the polls. If a developer increases the polling frequency, this would extend the validation time instead of getting a faster reaction with begin session.

Example for a coin acceptor:



Note that some coin acceptors can send more than one coin message in response to a poll. The VMC must be able to parse multiple coin messages from one poll response.

General Data Response Timeout

Unless otherwise specified, a VMC should wait at least 30 seconds for a response to commands that require data to be returned. This does not infer that the device is not ACKing POLL commands, but rather the VMC is waiting for data pertaining to the command. I.e., for a PAYOUT VALUE command, the coin mech should respond to each PAYOUT VALUE POLL within 30 seconds.

Non-communication Timeout (General)
If a peripheral does not communicate with the VMC for an extended period of time, that peripheral should take care of any relevant house-keeping and then RESET. This time should be of sufficient length to guarantee that communications with the VMC have been completely lost. The recommendation is to wait at least 10 times the max response time for a device.

If the VMC does not successfully communicate with a peripheral for the 'application maximum response time', it should attempt to RESET that peripheral once every 10 seconds (Section 2.4.3 POLLing) and continue operations (if possible) with the other MDB peripheral(s) that are still responsive.

Poll Responses covered by note 1 -Sent once each occurrence (Coin Mech)
Some devices send this response each time the changer detects the condition. For example, the changer sees the gate open so it sends the escrow request, if the next time it checks it see the gate open it will send the escrow request again. Other devices will only send it once until the gate returns to the normal position.

It is recommended to send it only once.

3. 3. Commands, Repetition, ACK, NAK

NAK and RET (Section 2.2 Block Format)
The purpose of a NAK is ONLY to indicate a message has been received with a bad checksum. NAK is never intended to be used for a command that is understood, but not executable.

Since the error may be caused by the corruption of the address byte (shown in the following example), it is not recommended to use the NAK, but rather to not response. The 5ms non-response timeout will be treated as if it were a NAK (Section 2.2 Block Format/Master-to-Peripheral, Peripheral-to-Master and Response Codes).

RET is a VMC-only response that is sent to a peripheral to force it to retransmit its previous (and presumably good) response. (Section 2.2 Block Format/Response Codes).

Example of NAK or 'no NAK' with an error in the address byte:

The following example shows how you can get in trouble with a simple RESET COMMAND sent to a cashless device. Whereas the cashless device itself receives the command without error, the bill validator in the system sees a voltage transient (corruption) of the address byte.

VMC sends	Cashless received	Billval received	Cashless response	Bill validator response	
POLL to cashless	POLL valid CRC	command to other address			
			Sends a JUST RESET	Sends nothing	
Sends ACK to previous received just reset	ACK	ACK			
			Nothing	Nothing	
RESET to cashless	RESET valid Checksum	Instead of command to its address, receives command to address 30H with Checksum 10H (because the destination 10H address byte was modified by transient voltage)			
			Sends ACK after 4ms	Sends NAK after 1 ms	*
			Sends ACK after 1ms	Sends NAK after 4 ms	**
			Sends ACK after 3ms	Sends nothing	***

As is shown, with only a single bit toggled (10h is modified to 30h). Three different reactions are possible:

* 1st Example (shown in Blue):
The VMC receives a NAK first, but 3ms later, an ACK would arrive. If the VMC immediately sends a different command after the NAK the further answer of the next device would collide with the ACK of the cashless and cause a second failure.

** 2nd Example (shown in Red):
The VMC receives the correct ACK first and continues immediately (if it is using a very fast polling rate). The NAK of the bill validator will collide in any case with the next message and cause further errors!

*** Last example (shown in Green):
The VMC receives the correct ACK first and continues immediately (if it is using a very fast polling rate). The bill validator will not cause any further errors, because it sends nothing. In this, and only this case, if the cashless device has a checksum

error too, both devices would not answer. The VMC would then repeat the command after 5 ms, because it would interpret the timeout as an NAK.

Recommendations from here:

Newer peripherals should never send a NAK, to avoid further handling errors.

Newer VMCs should never try to increase the polling rate if they receive a NAK from a peripherals, instead they should wait for the full timeout period to expire (and skip) further ACK's and NAK's from other peripherals. Please note that if you have four peripherals on the bus, the VMC may receive at least four ACK's and/or NAK's in or out of sequence!

To improve system reliability you should implement the bit counting method defined in the note of page 2-4 of the MDB specification.

Command Repetition (General)
VMC commands which are not ACKed should be repeated for the duration of the non-response time-out. If the command is not a POLL it is recommended that the command should alternate with a POLL. This does not mean that the VMC cannot communicate with other peripherals on the bus, but it should continue to communication with any non-responsive peripheral until it can reliably conclude that it is offline. At that point, it should start trying to RESET that peripheral once every 10 seconds. (Section 2.4.3 POLLing). When it receives a response to the RESET the VMC will need to re-initialize the peripheral.

Command Repetition (special commands)
VMC commands which are not ACKed should be repeated for the duration of the non-response time-out. Please note, that this is a general guideline, which in some circumstances may not be a "successful" implementation.

Condition 1 (coin mech dispense)
If a dispense command is not ACKed, this may be
a) a misunderstanding by the peripheral
b) a corrupted bus signal
c) another peripheral corrupting the bus

If the command itself did not arrive at the coin mech, repetition is ok. If the command arrived at the coin mech, but the VMC did not see the ACK, repetition obviously leads into multiple coin dispense!!!

In this situation, it is recommended not to re-send the command multiple times, although the choice is ultimately down to the system designer, and to wait for a while before restarting communications. This will allow any noise on the bus to dissipate.

Condition 2 (bill validator or coin mech acceptance)
If a bill validator accepts a bill or a coin mech accepts a coin, this is reported during the next poll to the VMC. This message is then ACK'ed by the VMC.
If this ACK is not detected by the bill validator or coin mech, for whatever reason, the peripheral repeats the message (this means, the same coin or bill value is sent again).

If the bill or coin value message did not arrive at VMC, repetition is ok. However, if the command arrived at the VMC, but the bill validator or coin mech did not see the ACK, repetition obviously leads into increasing credit!!!

Recommendation to minimize this effect especially for bill validators with high denomination values:
Whenever a VMC receives a bill (or coin) message, it should send the ACK, process the bill (or coin), wait for the recommended maximum response timeout (20ms) and send an additional poll.
If the VMC receives the same bill (or coin) message again after 20ms, (instead of receiving an ACK only) this can be assumed to be a repetition due to non-received ACK. If nothing is reported or a different value is sent, the ACK was understood or a new bill (or coin) has arrived.
This solution assumes, that bill (or coin) insertion is much slower than 20ms (which obviously is true especially for bill vals)

Command Order (General)
In most cases the VMC can send any command at any time in any order. Note the Cashless device spec is the only peripheral that defines the sequence of commands.

Command Out-Of-Sequence (Cashless Payment Device)
If the VMC receives a Command Out-Of-Sequence from a cashless payment device, it is a clear indication that the state of the cashless payment device is no longer in synch with the VMC. The VMC should take care of any relevant house-keeping and then issue a RESET to the cashless payment device. This will put both parties in a known state of operation.

4. Logical Level, Processing

Maintaining MDB Level Compatibility (General)
In a system where the peripheral supports a higher level MDB protocol than the VMC, the peripheral should revert to the lower level MDB protocol to communicate with the VMC. (Section 1.3.1 Levels and Section 2.4.4 Levels)
In a system where the VMC supports a higher level MDB protocol than a peripheral, it is the responsibility of the VMC to revert to the lower level MDB protocol when communicating with the peripheral. (Section 1.3.1 Levels and Section 2.4.4 Levels)

Response data length (General)
Note that some responses for peripherals can be variable length (tube status, poll, etc.). For example, a peripheral can send multiple messages in response to a poll command. Note that the 9th mode bit should be set on the last byte of the data being received (see section 2.5 Typical Session Examples)

Scale Factors (General)
The VMC needs to be able to handle devices with different scaling factors. The VMC needs to determine the least common dominator and adjust the values from each device.

Decimal point (General)
The decimal point information is only used to set the position on a credit display (it doesn't adjust the values).

Country Codes (General)
Do not require devices to have the same country code. In July 2000 the spec changed to use the ISO4217 numeric currency codes. Devices before that date used the international telephone codes.

Just Reset (General)
If a device sends a just reset response, the VMC should re-initialize the device (request setup information, re-enable the device, etc.). Don't send a reset command.

Multiple Coin Reporting
The VMC must take into account that coin mechs can send the value of more than one coin in one poll response.

Multiple Bill Reporting
The VMC must take into account that bill validators can send the value of more than one bill in one poll response.

Power-Up Sequence (Cashless Payment Device)
The following sequence is recommended as the power-up process for cashless payment devices. Post-RESET ACKs are not explicitly listed and are implied.

Send RESET until ACKed.
POLL until JUST RESET response.
Send SETUP/CONFIG command.
POLL until READER CONFIG response.
Send MAX/MIN PRICE command.
Send EXPANSION ID REQUEST.
POLL until PERIPHERAL ID response.

Send READER ENABLE command when ready.

Cashless Payment Device Enable/Disable (Cashless Payment Device)
While it is specifically allowed for "grandfather" reasons, a VMC should never need to disable a cashless payment device during a session. However, if this does occur, the cashless payment system should complete the session-in-progress normally (Section 7.4.12 READER – Disable), and subsequently refuse to start any new sessions with the VMC until enabled.

Level 2 BEGIN SESSION Command (Cashless Payment Device)
The description of Byte Z8 of the Level 02/03 BEGIN SESSION message (Section 7.4.4 POLL) appears to match the EVA-DTS Standard v.5.0, App. A.1 Definitions. All NAMA MDB specification references in this document are based on Version 3.0 (Draft 1), dated March 26, 2003, always refer to the latest EVA-DTS version.

Cashless Payment Device Discounting (Cashless Payment Device)
The VMC should not make any financial decision(s) based on the BEGIN SESSION balance. Some cashless peripherals support various types of discounting. Consequently, the VMC should not terminate a session if the reported balance is less than the minimum price or refuse to issue a VEND REQUEST when the list price of a selected item exceeds the reported balance of funds.

Similarly, if a cashless payment device reports a starting balance of 0xFFFF in the BEGIN SESSION message, the VMC should proceed normally i.e., permit a product selection. A BEGIN SESSION balance of 0xFFFF means that the available fund balance is not currently known and/or should not be displayed. It is not meant to suggest that the balance is insufficient for operation. An appropriate message for the customer should be displayed instead of the balance – i.e. "Please make a selection".

Revalue Limit Requests (Cashless Payment Device)
Similar to discounting, some cashless devices are capable of granting "bonus" credit to users (i.e., giving $6.00 credit for a $5.00 bill). There may also be cases where a cashless device pre-deducts sales tax resulting in a credit that is less than the amount in the REVALUE command. Finally, most cashless devices that store credit on the media have a maximum allowable credit.

Consequently, the VMC should issue a REVALUE LIMIT REQUEST prior to determining which fund sources (e.g. note values) are applicable to a user. In a multivend environment, this means the VMC must issue multiple REVALUE LIMIT REQUESTs.

If a cashless device cannot accept credit, either because the operation is not acceptable at this time or because the current media has reached its maximum credit limit, the device should respond to a REVALUE LIMIT REQUEST with a REVALUE DENIED not a REVALUE LIMIT of $0.00. The REVALUE DENIED response clearly signals that revalue is not an acceptable operation.

Balance Display (Cashless Payment Device)
For VMCs that opt to show the available funds, it is important to consider the following:
Cashless payment devices with active discounts will deduct less than the VEND REQUEST amount. The displayed balance in the VMC must reflect the difference between starting balance and the amount in the VEND APPROVED message (not the VEND REQUEST). This assures that the displayed balance on the VMC is correct, and (where applicable) matches the cashless payment device's display.

Because the REVALUE APPROVED message does not contain an amount field like VEND APPROVED, the VMC is not capable of tracking card balance correctly in a "bonusing" environment.

Multi-Vend (Cashless Payment Device)
Multi-vending is the practice of vending multiple products within a single session. While multi-vending is a function of the VMC, it should only be attempted when the multivend bit (b1) of the Miscellaneous Options byte (Section 7.4.2 Setup- Config Data/ Byte Z8) of the cashless device's configuration data is set (b1=1).

If a VEND DENIED scenario occurs during a multi-vend session, the VMC has the option to terminate or continue the vend session. It may be that the user tried to buy something that cost more than his balance. If the VMC has less expensive goods to vend, continuing the session would give the user an opportunity to select something affordable.

If a VEND FAILURE scenario occurs during a multi-vend session, the VMC should always issue a VEND FAILURE to the cashless payment device. The VMC has the option to terminate or continue the vend session. It may be that the user selected an empty column, and another selection will be successfully vended.

Display Messages (Cashless Payment Device)
If Byte Y3 (Columns) and/or Y4 (Rows) of the SETUP/CONFIG message are zero, VMC display is not available for use by the cashless payment device (Section 7.4.2 SETUP – Config Data).
If the display is available, a Display Request message can be sent anytime after the power-up sequence has been completed. In practice, there are only a few conditions under which the cashless payment device should make a Display Request:

1. Immediately after the power-up sequence is completed to display the cashless payment system's software revision number. This should not create significant problems because it only happens at power-up.
2. Anytime the cashless device is out of service.
3. In the enabled state to indicate an error accessing the media (e.g. busy signal for a credit card reader). This should not create a conflict because a) it is transient, and b) the user should be concentrating on the purchase process.
4. In the enabled state to prompt the user (e.g. for a PIN). This should not create a conflict because a) it is transient, and b) the user should be concentrating on the purchase process.
5. In the enabled state to inform the user of the funds available for purchase. This should not create a conflict because a) it is transient, and b) the user should be concentrating on the purchase process.
6. During session idle (e.g. after a VEND DENIED to indicate the reason for the refusal). This should not create a conflict because a) it is transient, and b) the user should be concentrating on the purchase process.

If the VMC reports itself to support Full ASCII (Y5 = xxxx001b) then it will support all printable ASCII characters (0x20 thru 0x7F). If values outside this range are used, the results are dependent upon the actual display controller chip. This is strongly discouraged.

Selected Number (Item Number or Product Code?) (Cashless Payment Device)
The selected number should be the vending machines selection number, which is normally the product key index. If the VMC i.e. has a two digit input, where one is alphanumerical, ("A-1" or "C-6" or ..), it has to convert it in a appropriate way to a number. To be compatible to all versions of card-readers and DTS-versions, ensure the number is in the range of 1-n. The maximum of n depends on the level used and options (1-255 or 1-65535).

The conversion method and the maximum selection number should be published by the VMC vendor to ensure the correct settings of the cashless device. Vice-versa, the cashless device vendor should publish the maximum usable numbers of selection, and the default action, if a selection number out of this range is sent.

Normally, this default action should result in a simple conversion to the maximum number and accepting the price from the vending machine, skipping all internal discounts etc.

Combining a VMC and a cashless device which do not have compatible maximum selection numbers is not an issue MDB has to solve, but is an application setup error.

Bill Stacking/Escrowing (Cashless Payment Device)
As a general practice, the VMC should escrow any bills tendered for credit to a cashless payment device until it has verified that the cashless payment medium can accept the full credit amount. This is done via the REVALUE LIMIT REQUEST command/response sequence. Once the value has been deemed acceptable, the VMC should stack/secure the bill prior to issuing the REVALUE REQUEST to the cashless payment device. This provides maximum protection against theft attempts. (Section 7.4.16 Revalue)

Mixed Tender Transactions (Cashless Payment Device)
Historically, this practice has been avoided by the VMC disabling the other peripherals when one becomes active (i.e., if someone inserts a bill into the validator, the VMC will disable the cashless payment device). If mixed tender transactions are to be supported, we must determine which fund source has priority for purchases, as well as for dispensing change.

There are two issues here:
1. If revalue is permitted, always revalue first, and then any purchase(s) should be from the card.
2. If revalue is not allowed, use cash first, and then deduct remaining funds from card.

Example: A mixed-tender VMC accepts $1.00 bill and a user inserts a $5.00 card.

Revalue Permitted: The $1.00 bill is stacked and a REVALUE REQUEST for $1.00 is sent to the cashless payment device. Once approved, any purchases should come from the $6.00 card balance.

Revalue Not Permitted: The $1.00 remains in escrow. The user selects a $1.50 item. The VMC sends a VEND REQUEST for $0.50 to the cashless payment device. If and only if it gets a 'vend approved', it will use/stack the $1.00 in escrow and sell the product. If it cannot stack it, the vend will be aborted and a vend failure will be sent. (Note: The cashless payment device will assume a $0.50 product was sold even though the Item Number may have been sold previously for $1.50.)

Obviously, this combination of settings causes more problems than the "non stacking" combination.

First: if the cashless gives a discount, the discount may reduce the price to a value less than the vend request (because the calculation uses the $1.50 value). This would result in stacking less than the whole bill, which is not possible! In this case, a vend denied should be sent. This method would temporarily disable the mixed payment.

Second: if refund is not possible, aborting of a vend will result in a credit loss situation. The VMC should use the opposite vend procedure – i.e. first stack the bill and then send the vend request. But, if in this case a 'vend denied' is received, the VMC needs to give change for at least the bill value!

MDB does not specify handling procedures for all these combinations – the operator needs to check the VMC and/or cashless capabilities as this is not an issue with the standards but a "market feature" problem.

Fund handling with a VEND FAILURE (Cashless Payment Device)
Normally funds are the responsibility of the fund source, (i.e., the cashless payment device). If a VEND FAILURE occurs the funds in question can be handled as follows:

NOTE: To prevent double refunds where the cashless payment device provides a process for refunds, the cashless device must indicate that the media supports refunds, regardless of whether or not it can actually transfer the lost funds back to the payment media.

The correct handling for vend failure is always, that no credit should be converted i.e. cash credit is escrowed, card credit is refunded. Card credit will never be transformed to cash!!

If the cashless device is not capable of refunding, for whatever reason, the VMC, and maybe the cashless device, may produce a log file or a statistic to ensure this is recorded. However, the credit balance in this case is always lost and may only be refunded to the customer by manual intervention (hotline, etc.)

If the cashless device is capable of refunding, nothing else is necessary. Sometimes, if a special card is used or the card is no longer present, refunding is not possible. In this case the same procedure as described above must be followed.

If the system allows the card refund amount to be transformed to cash, the following should be taken into account:

a. The VMC can make a record of the lost funds and remove them from escrow.
b. The VMC can retain the credit and allow it to be used as part of a cash purchase.
c. The VMC CANNOT dispense the funds as change. In the case of a credit card charge or where the original source of funds was a credit card transaction, this constitutes a cash advance, all be it small.
d. Please note further, that the VMC may have problems dealing with a discount amount.
e. Please note further, that the cashless payment scheme may not allow this behaviour.

Fund Handling with a Negative Vend Failure
After a vend is approved, it is up to the cashless device how it handles the negative vend value

State Machine (Cashless Payment Device)
The defined state machine within the standard is information for both VMC and cashless programmers of the logical steps required to run the device.

In any case, the state machine should never be used as medium to swap the Master-/Slave device functions. In MDB, the VMC is always the Master device. This results in a unspecified sequence of commands for the VMC (as for all other devices). i.e. even if the device has reached the begin session state, the VMC is allowed to send, for example, an FTL command. If the cashless is not able to support this command in the current state, it may send the applicable response (i.e. FTL denied), but will continue in the reached state!!

Further examples of this are multiple "Vend Session Complete" or similar commands. Because the cashless device enters the inactive state with the first vend session complete, further repeated commands will never produce any problems and may simply be ignored.

A lot of cashless devices use the "out of sequence" message in this case. This may be appropriate in terms of "educating the VMC programmer", but will never solve the issue. The "out of sequence" message usually causes the VMC to send a reset command to re-sync the devices. This is not a problem for the VMC, but can cause the cashless device to run into problems - mainly because the reset sequence of a lot of cashless devices can take many seconds, during which the customer is unable to use their cards. This obviously can lead to complaints.

The "Out of sequence" message should be the last resort for a cashless device, to be used only if it is unable to solve state machine problems any other way. Unfortunately, due to the polling mechanism with a finite polling frequency, the loss of synchronisation between the VMC and the cashless state is unavoidable.

An example of this is as follows:
After a card insertion we get a begin session.
Both devices enter the session idle state.
The customer presses the escrow lever and takes the card out simultaneously.
The VMC would send a Reader Cancel command, whereas the cashless would like to transmit an end session (because its session ended when the card was taken out).

The situation then arises that the cashless device is in the inactive state (no card present), but cannot send the message to the VMC (no poll available, instead a wrong command for this state).

The VMC, on the other hand, believes it is sending the correct command, as it is still in the session idle state. Hence, it would repeat the cancel session, until it is answered. It would then get a totally unnecessary "out of sequence", and maybe an additional "end session".

Espacenet

Bibliographic data: CN1561508 (A) — 2005-01-05

Code identification method and system

Inventor(s): DONALD KEECH WINSTON [GB] ± (KEECH WINSTON DONALD)

Applicant(s): SWIVEL TECHNOLOGIES LTD [GB] ± (SWIVEL TECHNOLOGIES LTD)

Classification: **- international:** ***G06Q20/00; G07F7/10; H04L9/32;*** (IPC1-7): G07F19/00; G07F7/10; H04L9/18

- cooperative: **G06F17/00 (KR); G06Q20/02 (EP, US); G06Q20/04 (EP, US); G06Q20/10 (EP, US); G06Q20/12 (EP, US); G06Q20/32 (EP, KR, US); G06Q20/322 (EP, US); G06Q20/347 (EP, US); G06Q20/382 (EP, US); G06Q20/385 (EP, US); G06Q20/388 (EP, US); G06Q20/4014 (EP, US); G06Q20/425 (EP, US); G07F7/10 (EP, US); G07F7/1075 (EP, US)**

Application number: CN20018012009 20010907

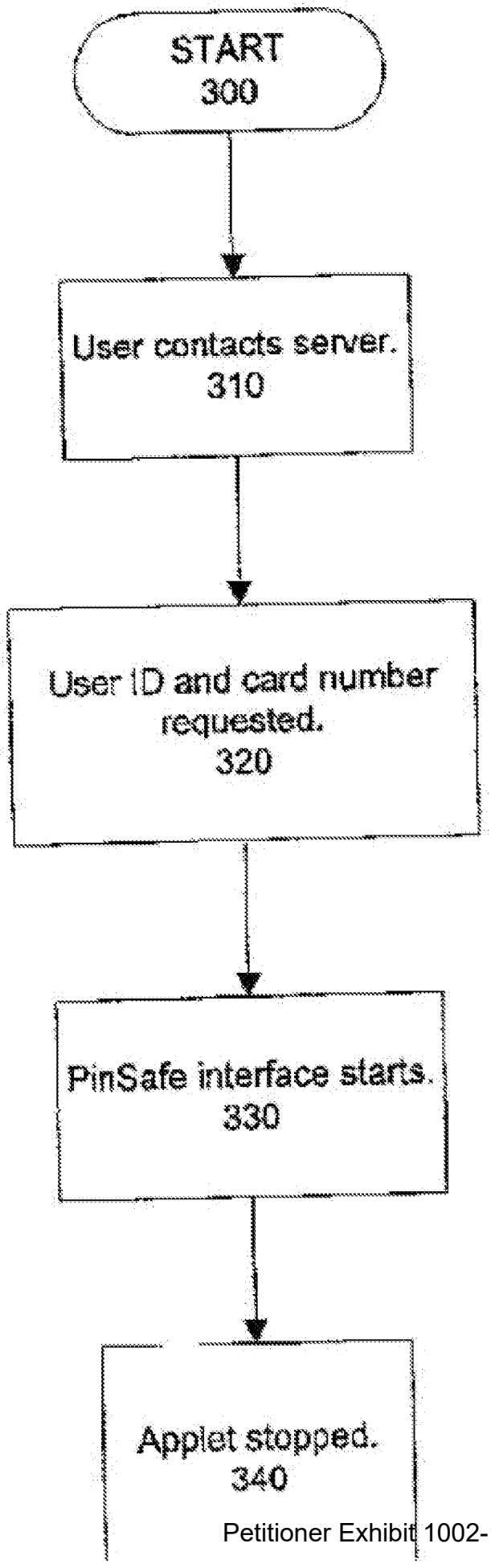
Priority number(s): GB20000021964 20000907 ; US20000663281 20000915 ; US20010915271 20010727

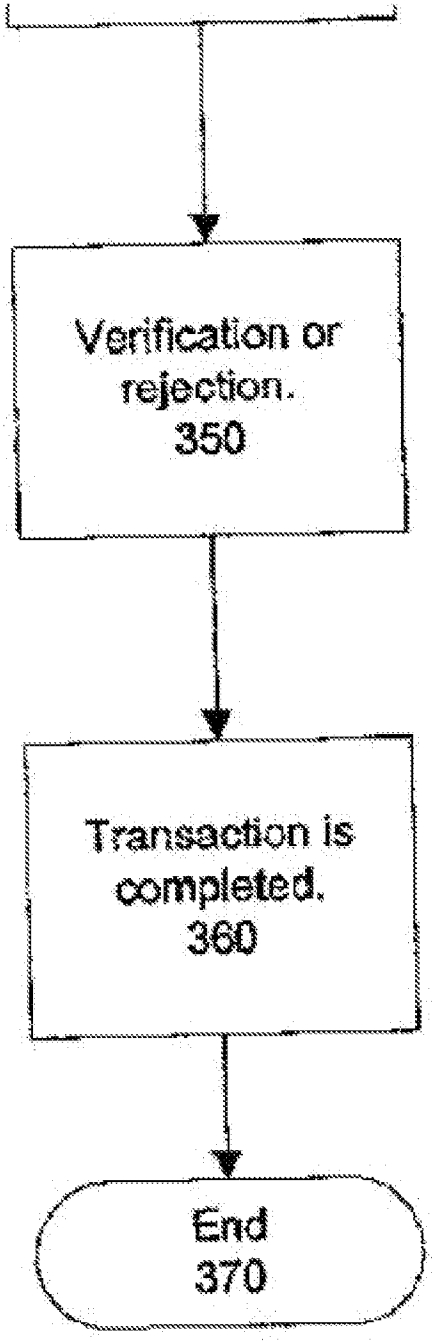
Also published as: AU2005100466 (A4) AU2005100466 (B4) AU8784701 (A) BR0113887 (A) CA2421495 (A1) CN1279498 (C) CY1113961 (T1) DK1316076 (T3) EA004422 (B1) EA200300263 (A1) EP1316076 (A2) EP1316076 (B1) ES2403039 (T3) JP2004508644 (A) KR20030036766 (A) MXPA03002050 (A) NO20030982 (L) NZ524391 (A) PT1316076 (E) US2002029342 (A1) US2002059146 (A1) US7392388 (B2) WO0221463 (A2) WO0221463 (A3) less

Abstract not available for CN1561508 (A)
Abstract of corresponding document: US2002029342 (A1)

A method and system for secure identification of a person in an electronic communications environment, wherein a host computer is adapted to be able to communicate with a plurality of electronic devices operated by the user. The user is issued with a user code, known only to the user and stored in the host computer. When the user is required to identify themselves to the host computer, the host computer generates a pseudo-random security string and applies the user code to the pseudo-random security string to generate a transaction code. The host computer also transmits the pseudo-random security string to one of the electronic devices which

displayed by the electronic device to the user. The user applies their known user code to the displayed pseudo-random security string and determines the transaction code. The user enters the transaction code into an electronic device and the entered transaction code is then transmitted back to the host computer. Positive identification is achieved when the host computer determined transaction code matches the transaction code entered by the user. In addition, the system could employ a secure user code entry interface which would allow secure input of the user code.




Verification or rejection.
350
Transaction is completed.
360
End
370

Description: CN1561508 (A) — 2005-01-05

Code identification method and system

Description not available for CN1561508 (A)
Description of corresponding document: US2002029342 (A1)

A high quality text as facsimile in your desired language may be available amongst the following family members:

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application is a continuation-in-part of U.S. patent application Ser. No. 09/663,281, filed Sep. 15, 2000 which claims priority from U.K. Patent Application Number GB 0021964.2, filed Sep. 7, 2000, both of which are incorporated herein by reference in their entirety.

FIELD OF THE INVENTION

[0002] The present invention relates to the field of secure transactions and more specifically to the verification of a user's identity for conducting transactions.

BACKGROUND OF THE INVENTION

[0003] The present invention relates to a system and method for identifying a user or device and, optionally, for conducting transactions between the user or device and a third party, for example, by way of a telephone connection or an electronic computer system such as the Internet.

[0004] Various systems are know for conducting electronic transactions in a more or less secure manner over a telecommunications link or the like. One well known system is known as electronic funds transfer at point-of-sale (EFTPOS), in which a user is issued with a credit or debit card bearing a unique identification number, usually embossed on the card in human-readable form and also encoded on a machine-readable magnetic strip on the reverse of the card. For further identification purposes

the card typically includes a space for a user permanently to include his or her signature. In use, when a user wishes to make a purchase in, for example, a retail store, he or she presents the debit or credit card to a store employee. The card is then swiped through a card reader, and information relating to the identity of the card, the identity of the retail store and the value of the goods or services being purchases is transmitted by way of a telephone connection to a remote computer server operated by the card issuer (normally a bank or suchlike). The remote computer server checks that the user's card account contains sufficient funds or credit to cover the proposed transaction, checks that the user's card account is currently operational (for example, to check that the card has not been reported stolen), and then issues a confirmation signal back to the card reader to indicate that the transaction may be authorized. The store employee must then obtain a specimen of the user's signature and compare this with the signature on the reverse of the card so as to check the identity of the user. If the signatures appear to match, the store employee operates the card reader to complete the transaction, and the funds required to cover the transaction are then electronically transferred from the user's card account to the retail store. If the signatures do not appear to match, then the store employee may request additional proof of identification before authorizing the transaction, or may simply refuse the transaction and retain the user's card, which may have been stolen, thereby preventing any unauthorized transfer of funds. This system is open to fraudulent abuse, since it is possible for a card to be stolen and for a thief to forge the signature of an authorized user.

[0005] In a development of this system, a card user may be issued with a personal identification number (PIN), which is usually a four digit code, and which is theoretically known only to the user and to the card issuer. Instead of or in addition to providing a specimen of his or her signature at the point-of-sale, the card user is required to enter his or her PIN into the card reader, and this information is transmitted to the remote computer server together with the card and retail store identification data and data regarding the value of the transaction. By providing an extra identification check by way of the PIN, this system helps to prevent fraud by forgery of signatures, but is still not completely secure because the PIN does not change between transactions, and may therefore be intercepted together with card identification data when being transmitted between the card reader and the remote server. Furthermore, it is possible for a thief to observe a user entering his or her PIN into a card reader and to remember the PIN. If the thief is also able to obtain card identification details, for example, from a discarded till receipt or through conspiracy with the store employee, it is a simple matter to produce a fake card including all the appropriate identification information for later fraudulent use, or even to rob the authorized card user of his or her card.

[0006] The Protocol of the present invention is currently the only identity verification solution available that can be used across all platforms, using a common user interface. A number of other attempts to solve the problem of identity verification are currently available and include Public Key Infrastructure (PKI), SMART Cards, and biometrics.

[0007] A Public Key Infrastructure is a combination of hardware and software products, policies and procedures. PKI provides the basic security required to carry out electronic business so that users, who do not know each other, or are widely distributed, can communicate securely through a chain of trust. PKI is based on digital IDs known as 'digital certificates' which act like 'electronic passports' and bind the user's digital signature to his or her public key. The PKI approach is only applicable for Internet or other transactions that use a computer because the complexity of the software at the users' end of the transaction requires significant computing resources. The

approach is not well suited to high volume transaction processing because of this complexity.

[0008] Smart Cards are a response to the problem of credit/debit card fraud. Smart Cards are cards that have a microchip embedded within the card which enables personal details about the cardholder to be stored securely on the card, which can then be used to verify the identity of the person using the card. The Smart Card system relies upon there being a Smart Card reading apparatus at the point of sale. Currently, few high street merchants have invested in such equipment, and recent industry estimates expect a hybrid smart card/magnetic strip environment for the next 10-15 years. In addition, smaller or independent retailers find the cost of such equipment is a deterrent to uptake. Few Smart Card systems address the problem of "card not present" fraud such as e-commerce, m-commerce, interactive TV and telephone order unless the consumers invest in Smart-Card readers for the home. Similarly, any Smart Card can be copied ("skimmed/cloned") and can subsequently be used fraudulently in card not present situations. Most major card issuers have plans to roll out such Smart Cards within the next few years, although the costs of the equipment, the cards themselves and the availability of the chips may delay this process. The present invention has been designed to be able to act as a security overlay to such Smart Card systems and can make any transaction as secure as those for which the Smart Cards are designed.

[0009] A number of companies are currently developing biometric solutions to the problem of cardholder verification. The Biometric systems can use fingerprints, voice recognition, retinal scans or tissue samples to positively identify the cardholder. Similar to smart cards these biometric systems would require complex and costly equipment at the point of sale and would not provide any protection against fraud in card not present situations.

BRIEF SUMMARY OF THE INVENTION

[0010] According to a first aspect of the present invention, there is provided a coded identification system, the system comprising an electronic computer, a specific electronic communications device that is operable to be in communication with the electronic computer, and at least one electronic communications device that is operable to be in communication with the electronic computer, wherein the electronic computer includes data relating to the specific electronic communications device, including a permanent identification code, a mask code and an identification code enabling electronic communication between the electronic computer and the specific electronic communications device, and wherein the permanent identification code is input to the at least one electronic communications device and transmitted to the electronic computer, the electronic computer generates a pseudo-random string and transmits this to the specific electronic communications device, the mask code is applied to the pseudo-random string so as to generate a volatile identification code in accordance with predetermined rules, the volatile identification code is transmitted back to the electronic computer by the specific electronic communications device or the at least one electronic communications device, the electronic computer checks the volatile identification code transmitted thereto against a volatile identification code obtained by applying the mask code to the pseudo-random string in accordance with the predetermined rules, and in which a positive identification is made when the volatile identification codes are found to match by the electronic computer.

[0011] According to a second aspect of the present invention, there is provided a method for identifying a specific electronic communications device [illegible]

electronic computer having stored therein data relating to the specific electronic communications device or user thereof, including a permanent identification code, a mask code and an identification code enabling communication between the electronic computer and the specific electronic communications device, wherein the permanent identification code is input to at least one electronic communications device and transmitted thereby to the electronic computer, the electronic computer associates the permanent identification code with the identification code enabling communications there between and the specific electronic communications device and generates a pseudo-random string before transmitting this to the specific electronic communications device, the mask code is applied to the pseudo-random string in accordance with predetermined rules so as to generate a volatile identification code, the volatile identification code is input to the specific electronic communications device or at least one electronic communications device and transmitted to the electronic computer where it is compared with a volatile identification code generated therein by applying the mask code to the pseudo-random string, and a positive identification is made when the volatile identification codes match.

[0012] The specific electronic communications device may be a separate device from the at least one electronic communications device, or may be the same device. For example, the specific electronic communications device may be a mobile telephone, a pager, a land-line telephone, a personal digital assistant or a computer which may be owned or specifically operated by a given person. The at least one electronic communications device may be an electronic funds transfer (EFT) or electronic funds transfer at point-of-sale (EFTPOS) terminal, or may be the same mobile telephone, pager, land-line telephone, personal digital assistant or computer which may be owned or specifically operated by the person as hereinbefore described.

[0013] The permanent identification code may be supplied to a user in the form of a card bearing human and/or machine-readable data.

[0014] The identification code enabling electronic communication between the electronic computer and the specific electronic communications device may be a mobile telephone or pager number where the specific electronic communications device is a mobile telephone, pager or personal digital assistant, or may be an e-mail address or similar code allowing specific communication with a given specific electronic communications device.

[0015] Where the specific electronic communications device is a mobile telephone or the like, the pseudo-random string may be transmitted in the form of a text message under the short messaging service (SMS) protocol. Other well-known communications protocols may be employed where appropriate, depending on the nature of the specific electronic communications device.

[0016] Embodiments of the present invention provide additional security of identification in a number of ways. Firstly, in addition to requiring the person to have access to the permanent identification code, the system requires the person to be in possession of an appropriate specific electronic communications device. Secondly, because the system requires the user to cause his or her mask code to operate on the pseudo-random string so as to generate a volatile identification code in accordance with the predetermined rules, without the mask code being electronically transmitted together with the permanent identification code, it is difficult for an unauthorized person to intercept communications between the electronic computer, the specific electronic communications device and/or the at least one electronic communications device so as to determine the mask code and the permanent identification code.

[0017] It will be appreciated that the present invention extends to situations where it is required to establish a secure identification of a specific electronic communications device rather than of a person as such. For example, the present invention may be used as part of a secure "hand-shaking" protocol between remote computers, serving positively and securely to identify the specific electronic communications devices, which may itself be an electronic computer, to the electronic computer. Both the electronic computer and the specific electronic communications device will have the mask code stored within their memories but will not communicate the mask code between each other except by way of a secure connection, ideally entirely separate from their normal means of communication.

[0018] The mask code may take various forms. In a currently preferred embodiment, a person is issued with or selects a four digit numerical string, for example, 3928, analogous to the well known PIN codes currently used when operating automated teller machines (ATMs). However, different lengths of mask code may be used as appropriate. The pseudo-random string (which may be numeric, alphanumeric or any other combination of characters) transmitted to the specific electronic communications device in response to a signal sent by the at least one electronic communications device is displayable thereon in a predetermined form, with the characters making up the pseudo-random string being displayed preferably as a linear array. The person operating the specific electronic communications device then takes the first digit of his or her mask code, in this example 3, and notes the character in third position (say from left to right) along the pseudo-random string. The person then takes the second digit of his or her mask code, in this example 9, and notes the character in ninth position along the pseudo-random string, and so on for the digits 2 and 8 of the mask code. The characters selected from the pseudo-random string form the volatile identification code which is then input into the at least one electronic communications device and transmitted to the electronic computer for verification. Alternatively, the volatile identification code may be transmitted to the electronic computer by way of the specific electronic communication device. If the volatile identification code received by way of the electronic computer corresponds to an expected volatile identification code calculated by the electronic computer applying the mask code to the pseudo-random string, a positive identification is take to have been made. The prime security feature is that the mask code is never transmitted between the electronic computer, the specific electronic communications device or the at least one electronic communications device, and is thus safe from interception by unauthorized third parties. The secondary security feature is that a person must be in possession of his or her own specific electronic communications device, since the electronic computer will transmit the pseudo-random strong only thereto.

[0019] For additional security, after the volatile identification code has been transmitted to the electronic computer for verification and found to match a volatile identification code generated by the electronic computer, the electronic computer may transmit a message to the specific electronic communications device requesting that the person confirms that the identification is correct. Only when the person responds affirmatively to the message by transmitting a confirmatory message from the specific electronic communications device to the electronic computer so the identification process finally completed.

[0020] In some embodiments of the present invention, it is not necessary for a person operating the specific electronic communications device to view the pseudo-random string and to apply the mask code manually thereto. Instead, a computer program may be provided in a memory of the specific electronic communications device which [illegible]

the person to enter his or her mask code when prompted, and which then applies the mask code automatically to the pseudo-random string, returning the appropriate volatile identification code for input into the specific electronic communications device or the at least one electronic communications device.

[0021] In a further development, at least one position in the pseudo-random strong may be chosen to contain a character representative of a predetermined parameter or condition. Advantageously, the position of the character and its representational meaning are know only to the electronic computer and the person operating the specific electronic communications device. For example where the electronic computer is operated by a bank and the permanent identification code is the person's bank account number, then one of the positions in the pseudo-random string, say the seventh, may be chosen to be representative of a balance of the person's bank account, with 0 for example indicating zero funds and 9 indicating a balance over [pound]1000, with FIGS. 1 to 8 being representative of balances there between on a linear scale. Alternatively, for greater security, the at least one position in the pseudo-random strong may be chosen to contain a flag character, with say any one of the digits 1 to 5 indicating a balance below [pound]500 and any one of the digits 6 to 9 indicating a balance above [pound]500. It will be apparent that many other representational schemas may be applied so as to convey information in the pseudo-random string. Because the position and meaning of the at least on representative character in the pseudo-random strong is preferably selectable by the person rather than following a set format which may become known to unauthorized third parties, it remains difficult to extract meaningful information should the pseudo-random string be intercepted during transmission. Furthermore, the person may be required to identify the position and/or meaning of the at least one representative character after receiving the pseudo-random string, thereby providing an additional layer of security in the identification process.

[0022] It will be apparent that in the embodiment described hereinabove, the pseudo-random string must be at least ten characters long, since a mask code made up of the numbers 0 to 9 requires at least ten positions along the pseudo-random string to be functional. However, a person of ordinary skill will appreciate that different mask codes and string lengths may be used as required by selecting appropriate coding schemas. It is to be emphasized that the pseudo-random string issued by the electronic computer in response to an identification request from the at least one electronic communications device will be different for each request, and that it will therefore be extremely difficult to determine a given mask code given a series of potentially interceptable pseudo-random strings and volatile identification codes. Indeed, in embodiments where the specific electronic communications device is a separate device from the at least one electronic communications device, for example, a mobile telephone and an EFTPOS terminal respectively, then the pseudo-random string and the volatile identification code are never transmitted along the same route, for example, a given temporary telephone connection. In embodiments where the specific electronic communications device is the at least one electronic communications device, for example, a remote computer terminal adapted for secure connection to the electronic computer, then the pseudo-random string may be transmitted along the same route, but not together at the same time. In the latter embodiment, an initial request to log on to the electronic computer may only be considered if it emanates by way of a direct modem link from a predetermined telephone number associated with the person, the pseudo-random string is then transmitted back along the modem link to the remote terminal and the volatile identification code transmitted to the electronic computer by way of the same direct modem connection.

[0023] In a particularly preferred embodiment, the electronic computer is operated by a

debit or credit card issuer, the specific electronic communications device is a mobile telephone, the at least one electronic communications device is an EFTPOS terminal operated by a retailer, the permanent identification code is a person's debit or credit card account number, the mask code is a four digit number as described above, the identification code enabling electronic communications between the electronic computer and the specific electronic communications device is a telephone number of the mobile telephone. It is to be understood that the debit or credit card issuer may be a bank which issues standard debit cards enabling purchases to be made against funds in the person's current account or standard credit cards enabling purchases to be made against a credit account, or may alternatively be a specialist service provider issuing dedicated debit cards to subscribers, where the subscribers must arrange for funds to be transferred to the service provider as requires so as to keep at least a minimum positive balance associated with their dedicated debit card accounts.

[0024] When a person first applies for an account from the card issuer, he or she is issued with an account number and a card which bears the account number and name of the account holder in the usual way, for example by way of embossing the card with human-readable indicia and by way of providing machine-readable data on a magnetic strip on a reverse portion of the card. The person must supply the usual details, such as name and home address, to the card issuer, together with his or her mobile telephone number. It is also necessary for the mask code to be issued to the card issuer or to be agreed between the card issuer and the person. The mask code is preferably issued separately from the card, for example by way of separate postal deliveries, and is never transmitted together with the account number and/or telephone number. When the person wishes to make a purchase using the debit or credit card, he or she presents the card to a retailer. The retailer then swipes the card through the EFTPOS terminal, which then contacts a main computer operated by the card issuer.

[0025] The card/account number is transmitted to the main computer by way of a modem link, together with transaction details including the price of the purchase being made. The main computer then correlates the card/account number with the person's mobile telephone number and, if there are sufficient funds in the account to cover the intended purchase, generates a pseudo-random string which is transmitted to the mobile telephone by way, for example of and SMS message over a cellular telecommunications link. The person applies the mask code to the pseudo-random string as hereinbefore described, and then gives the volatile identification code thus generated to the retailer. The retailer, in turn, enters the volatile identification code into the EFTPOS terminal, which then transmits this data back to the main computer where it is correlated with the person's account details and compared with a volatile identification code temporarily stored in the main computer and generated therein by applying the mask code to the pseudo-random string independently of the person. If the volatile identification codes match, the main computer transmits a confirmation message to the EFTPOS terminal authorizing the transaction, and the necessary funds to cover the purchase are then transferred automatically to the retailer and debited from the person's card account.

[0026] In the event that there are insufficient funds in the person's account to cover the cost of the purchase, the main computer may issue a signal to the EFT terminal that the transaction is not authorized, and may issue a message to the mobile telephone advising the person to add finds to the account. In the event that the volatile identification codes are found not to match, then the main computer may issue a signal to the EFTPOS terminal so as to inform the retailer, who may then ask the person to check that the correct volatile identification code has been generated and to provide the correct code for transmission to the main computer. If the person gives the wrong

volatile code more than a predetermined number of times, for example three times, then the main computer may suspend that person's account temporarily for reasons of suspicion of fraudulent use. The authentic card holder must then apply to the card issuer, together with suitable verification of his or her identity, before the account is reactivated and/or a new account and card is issued.

[0027] In some embodiments, the person may communicate with the central computer directly by way of his or her mobile telephone. This is possible because transmissions from a mobile telephone include details of the number of telephone number of the mobile telephone, and because the main computer is able to correlate mobile telephone numbers with card accounts. One useful feature that may be provided is an emergency account lock that may be activated in the event that the credit or debit card or even the mobile telephone is stolen. Such a lock may be activated by transmitting a predetermined lock code, for example 9999, to the main computer. Alternatively, or in addition, a lock code may be issued in mask code format, which is useful in the event that a person is robbed and threatened with violence so as so hand over his or her card and mobile telephone, together with his or her mask code.

[0028] A further useful security feature may be provided wherein, after the volatile identification code has been transmitted to the electronic computer for verification and found to match a volatile identification code generated by the electronic computer, the electronic computer may transmit a message to the mobile telephone requesting that the person confirms that the transaction is authorized. The message may be sent in SMS or voicemail format, and may include details of the transaction. Only when the person responds affirmatively to the message by transmitting a confirmatory message from the mobile telephone to the electronic computer is the transaction finally authorized.

[0029] The credit or debit card of this embodiment of the present invention may also be used to make secure purchases over the Internet. In this scenario, the at least one electronic communications device may be a computer server operated by an Internet retailer. When a person wishes to make a secure purchase, he or she submits the account number to the server, by way of e-mail or through the retailer's website, and the server then transmits the account details and purchase details to the main computer operated by the card issuer as before. An SMS message containing the pseudo-random string is then transmitted to the person's mobile telephone, and the person then causes a volatile identification code to be generated and then submitted to the retailer's server from where it is transmitted to the main computer for verification before the transaction is authorized and funds released.

[0030] A person may have more than one account with the card issuer, and may accordingly select or be assigned more than one mask code, one for each account. Alternatively or in addition, more than one mask code may be assigned to each account, and the main computer may indicate by way of one or more characters in the pseudo-random string that it is expecting the person to apply a particular mask code, selected from a plurality of prearranged mask codes, to the pseudo-random string, thus providing an additional level of security.

[0031] It is to be appreciated that the present invention is not limited to credit or debit card transaction, but provides a secure method and system of identification in a wide variety of situations. For example, access to a building or vehicle may be controlled by providing a central computer holding details of all people authorized to enter the building or vehicle, and a swipe card bearing a unique identification number or code in magnetically-coded format may be issued to each person authorized to enter the

building or vehicle. At entrances to the building or vehicle, electronic locks linked to card scanners and electronic keypads may be provided, the card scanners and keypads allowing communication with the central computer. When an authorized person wishes to enter the building or vehicle, he or she swipes the swipe card through the card scanner, which then transmits the unique identification number or code to the central computer. The central computer correlates the unique identification number or code with personal details of the person, including a predetermined mask code, and then transmits a pseudo-random string to the keypad for display on a display provided thereon. The person must then apply his or her mask code to the pseudo-random string and enter the volatile identification code thus generated into the keypad, which then transmits the volatile identification code to the central computer for comparison with a volatile identification code generated in the central computer as hereinbefore described. If the volatile identification codes match, then the central computer issues a signal to unlock the electronic lock. Such a system provides a significant advantage over existing electronic locks operated by keying in a predetermined code, because each time a person enters the building or vehicle, he or she will have to enter a different volatile identification code. This means that a potential thief of the like will not be able to gain access to the building or vehicle merely by observing an authorized person keying in an entry code and subsequently entering the same entry code.

[0032] Furthermore, it is not necessary to provide a swipe card to each person authorized to enter the building or vehicle. Instead, each person is issued with a unique and memorable permanent identification number or code, which may be input by way of the electronic keypad when access to the building or vehicle is required. The unique permanent identification number or code is then correlated in the central computer with the appropriate mask code and a pseudo-random string transmitted to the electronic keypad for display on a display thereof as before.

[0033] It will be appreciated that in the above embodiments, the electronic keypad and optional card scanner form the at least one electronic communications device as well as the specific electronic communications device. For added security, albeit involving additional inconvenience, persons authorized to enter the building or vehicle may be provided with mobile telephones as specific electronic communications devices, with the pseudo-random string being transmitted to the mobile telephone rather than to a display on the electronic keypad.

[0034] Alternative uses for the system and method of the present invention include any situation where secure identification of a person in an electronic communications environment is required. For example, the system and method maybe employed for a secure remote log-in to a computer and secure telecommunications in general (e.g. business-to-business e-commerce transactions, air traffic control communications, etc.). The system and method may also be implemented in the context of a vehicle immobilizer and/or alarm, whereby an authorized user of a vehicle is requested to apply a mask code to a pseudo-random string so as to deactivate the immobilizer or alarm.

[0035] A further use for the present invention is a secure ticketing system. A supplier of travel tickets, concert tickets, cinema and theater tickets and tickets for sporting events, among others, may issue a "virtual" ticket in the form of a permanent customer identification code and a pseudo-random string transmitted from a host computer to a specific electronic communications device. Upon arrival at a venue or upon request by a ticket inspector, a person to whom the "virtual" ticket has been issued may be required to apply his or her mask code to the pseudo-random string and to provide the virtual identification code generated thereby, together with the permanent customer identification code, to the ticket inspector. The ticket inspector may, for example, [illegible]

electronic communications device by way of which this information may be transmitted back to the host computer for verification, and to which a verification signal may be sent by the host computer in the event that the person is positively identified as an authorized ticket holder.

[0036] Yet another use of the present invention is in a parcel or postal depot, such as a post office, or a catalog store or a warehouse or the like, where people visit to pick up parcels, post or other articles and it is necessary to positively identify a person before handing over the parcels, post or other articles. A person picking up an article will have been issued with a pseudo-random string and, upon collection, is asked to supply a volatile identification code generated by the application of his or her mask code to the pseudo-random string.

[0037] According to another aspect of the present invention, there is provided an identity verification secure transaction system comprising a host computer for storing a user code associated with a user and for supplying a pseudo-random security string for a transaction. The host computer determines a one time transaction code by applying the user code to the pseudo-random security string. There is at least one electronic device in electronic communication with the host computer used for administering and completing the transaction by receiving and displaying the pseudo-random security string. The user determines the transaction input code by applying their user code to the pseudo-random security string displayed on the electronic device. The user enters the transaction input code in the electronic device displaying the pseudo-random security string, or in a device in communication with the host computer. The entered user transaction code is sent to the host computer for verification with the one time transaction code. The pseudo-random security string may be displayed and user entry of the transaction code may entered in any combination of devices including an Electronic Funds Transfer Point of Sale (EFT/POS) device, a wireless device associated with the user, a user computer connected via the Internet with the host computer or any device capable of communicating electronically with the host computer. Further, the host computer may transmit the one time transaction code for display on an electronic device, the system may be used to complete a transaction with a merchant through a merchant computer or web site which is in electronic communication with the host computer and a user computer or device. The system may be used to provide security or regulated access to a database or account information.

[0038] The present invention also provides a method for verifying an identity for conducting secure transactions in which the system stores information about a user pin associated with a host computer; generates a pseudo-random security string, determines a transaction code by applying the user pin to the pseudo-random security string, and transmits the pseudo-random security string to an electronic device. The electronic device displays the pseudo-random security string so that the user can determine a user transaction input code by applying their user code to the pseudo-random security string. The user enters the transaction input code on the same or a different electronic device in electronic communication with the host computer. The user entered transaction code is transmitted to the host computer for verification that the host computer determined transaction code matches the user entered transaction input code. The system of the present invention completes the transaction, allows access to a database or account information when the host computer determined transaction code matches the user entered transaction input code.

[0039] Another aspect of the present invention includes a secure user code entry interface system which is comprised of a secure user code entry interface that can

code entry interface is stored and running on an electronic device where the electronic device has a display. Viewable on the display if the secure user code entry interface which contains at least one active display for entry, by the user, of one digit of the user code per cycle of the interface. The active display of the interface illuminates at least one display digit on the interface and the user keys any key of a keypad or mouse or touches any area of a touch sensitive screen when the illuminated digit matches the digit to be entered in their user code. A random run on time is added to time when the user enters the keystroke so that the active display remains active and therefore information relating to the number entered can not be determined. The secure user interface contains one cycle for each digit of a user code.

[0040] According to a still further aspect of the present invention, there is provided an identity verification secure transaction system comprising a host, at least one electronic device, and a secure user interface. The host computer stores information about the user which includes account and user code information. The at least one electronic device is in electronic communication with the host computer and displays the secure user input interface for entry of the user code. The at least one electronic device has at least a display and a user input device. The secure user code entry interface contains at least one cycle for each digit of the user code and contains an active display for entry of the user code. The user enters each digit of the user code by a response through a user input device at a response time when a display digit which corresponds with the appropriate digit of the user code is illuminated in the active display of the interface. After entry of each digit within a cycle is entered a random run on time is added to the time when the user responded in order to extend each cycle of the active display so that the anyone could not determine which digit was selected by viewing the user interface. After entry of the entire user code the entered code is transmitted to the host computer for verification with the host computer stored user code. The user may enter their response by keying any key on a keyboard or mouse or by touching any area of a touch sensitive display.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0041] For a further understanding of the nature, objects, and advantages of the present invention, reference should be had to the following detailed description, read in conjunction with the following drawings, wherein like reference numerals denote like elements and wherein:

[0042] FIG. 1 is a schematic diagram showing a preferred embodiment of the present invention.

[0043] FIG. 2 is a schematic diagram showing a preferred embodiment of the dual channel schema.

[0044] FIG. 3 is a process flow diagram showing the steps a user would take while interacting with the system of the present invention.

[0045] FIG. 4 is a schematic diagram showing a preferred embodiment of the single channel schema of the present invention.

[0046] FIG. 5 is a schematic diagram showing an additional embodiment of the single channel schema of the present invention.

[0047] FIG. 6 is a schematic diagram of an additional embodiment of the single channel schema of the present invention.

[0048] FIG. 7 is a schematic diagram of an additional embodiment of the single channel schema of the present invention.

[0049] FIG. 8 is a schematic diagram showing an additional embodiment incorporating various aspects and features of the present invention.

[0050] FIG. 9 is a schematic diagram showing a secured database access system of the present invention.

[0051] FIG. 10 is a schematic diagram of a secure system for retrieving bank account information.

[0052] FIG. 11 is a representation of pseudo-random string.

[0053] FIG. 12 is a schematic diagram showing the modification and integration process of the user's temporary or transactional.

[0054] FIG. 13a is a graphical representation of the user interface of the present invention.

[0055] FIG. 13b is a graphical representation of the user interface of the present invention.

[0056] FIG. 13c is a graphical representation of the user interface of the present invention.

[0057] FIG. 13d is a graphical representation of the user interface of the present invention.

[0058] FIG. 13e is a graphical representation of the user interface of the present invention.

[0059] FIG. 13f is a graphical representation of the user interface of the present invention.

[0060] FIG. 13g is a graphical representation of the user interface of the present invention.

[0061] FIG. 13h is a graphical representation of the user interface of the present invention.

[0062] FIG. 14 is a graphical representation of the start screen of the PIN Safe interface of the present invention.

[0063] FIG. 15a is a graphical representation of the first cycle of the PIN Safe user interface.

[0064] FIG. 15b is a graphical representation of the second cycle of the PIN Safe user interface.

[0065] FIG. 15c is a graphical representation of the third cycle of the PIN Safe user interface.

[0066] FIG. 15d is a graphical representation of the fourth cycle of the PIN Safe user interface.

[0067] FIG. 15e is a graphical representation of the PIN Safe user interface using symbols or characters instead of numbers.

[0068] FIG. 16 is a schematic diagram showing features of the present invention utilized in a database access system via the Internet.

[0069] FIG. 17 is a schematic diagram containing features of the present invention utilized in the access of multiple databases via the Internet.

[0070] FIG. 18 is a schematic diagram illustrating various features and components of the present invention communicating via the Internet.

[0071] FIG. 19 is a schematic diagram illustrating various features and components of the present invention communicating via the Internet.

[0072] FIG. 20 is a schematic diagram of various features and components of the present invention communicating via the Internet.

[0073] FIG. 21 is a schematic diagram illustrating the access and data channels of an additional embodiment of the present invention.

[0074] FIG. 22 represents a schematic diagram displaying a generic server gateway schema incorporating various aspects of the present invention.

[0075] FIG. 23 shows a schematic diagram illustrating a generic integration platform of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0076] FIG. 1 shows a host computer 1 operated by a credit/debit card issuer, a user 2 having a mobile telephone 3, and an EFTPOS terminal 4. The user 2 is issued with a card (not shown) having a unique 16-digit account number embossed and magnetically encoded thereon, this 16-digit account number being correlated in the host computer 1 with account details relating to the user as well as a 4-digit mask code selected by or assigned to the user 2 upon initial registration with the credit/debit card issuer and a unique telephone number of the mobile telephone 3. The 16-digit account number is chosen for a compatibility with existing credit/debit card protocols, and the 4-digit mask code for compatibility with existing PIN protocols. When the user 2 wishes to make a purchase from a retailer (not shown) operating the EFTPOS terminal 4, he or she presents the card, which is then scanned by the EFTPOS terminal 4. Details regarding a purchase are also entered into the EFTPOS terminal 4 by the retailer, and these are transmitted, together with the account number, to the host computer 1 by way of a modem link 5. The host computer 1 then correlates the account number with details of the user 2, including the telephone number of the mobile telephone 3, and generates a 13-digit pseudo-random string which is transmitted to the mobile telephone 3 by way of an SMS or voicemail protocol 6. The first three digits of the pseudo-random string are not random and are reserved to indicate to the user that a received SMS message is from the host computer. For example, the first three digits may be "T1:" or "T2:" or the like, so as to indicate that the host computer 1 is expecting the user 2 to apply a first or a second mask code to the pseudo-random string. The next 10-digits of the pseudo-random string provide sufficient redundancy for any 4-digit mask code to [illegible]

thereupon in the manner hereinbefore described. By choosing a string length of 13 digits for the pseudo-random string, compatibility with existing mobile telephone displays and EAN13 (European Article Number) barcode protocols is ensured.

[0077] Upon reception of the pseudo-random string by the mobile telephone 3, the user 2 must apply the mask code thereto as hereinbefore described so as to generate a volatile identification code, which is then passed 8 to the retailer and entered into the EFTPOS terminal 4 for transmission to the host computer 1. Alternatively, the volatile identification code may be returned by the user 2 to the host computer 1 by way of the mobile telephone 3. When the host computer 1 receives the volatile identification code, it compares this with a volatile identification code generated within the host computer 1 by applying the mask code to the pseudo-random string and, if the volatile identification codes are found to match, issues a signal to the EFTPOS terminal 4 so as to authorize the purchase and to transfer necessary funds to the retailer. Optionally, before authorizing the transfer of funds, the host computer 1 may send a message to the mobile telephone 3, for example in SMS or voicemail format 6, preferably including details of the transaction, and requesting that the user 2 return a signal 7 so as finally to confirm the transaction. This may provide added peace-of-mind for unusually large transactions and may alert a user 2 in the event that fraudulent use is being made of his or her card.

[0078] The present invention may be implemented in both a single and dual channel schema which are disclosed and discussed in relation to FIGS. 2-10.

[0079] The Dual Channel protocol is appropriate for all users who own a G2 mobile phone. The types of transaction might include: (1) Electronic Funds Transfer at the Point of Sale (EFT/POS) and (2) Telephone orders. EFT/POS are transactions where the user would make a purchase at a merchant in the normal way and when the credit/debit card is swiped through the card reader, the merchant would be prompted to ask for the customer's transaction affirmation code (TAC) or mask code. The user remembers a their four digit PIN number which is used to determine the TAC from the pseudo-random string, which is given at the point of sale. If the user intends to make multiple purchases within a short space of time or in an area where mobile phone reception is poor the user can elect in advance to use the same TAC for a single day. A telephone order transaction would essentially use the same method as above with the exception that the merchant physically enters the card details in the usual manner before being prompted for the TAC.

[0080] Additional features of the dual channel schema are that the customer will be able to choose alternative user-friendly methods of identifying the TAC from the pseudo-ramndom security string. such as an Enigma interface or voice recognition system. An Enigma Interface would include minor modifications to a SIM card in a phone or pager during manufacture but customers could avoid any calculation of the TAC themselves. Users will be able to key in their PIN and by pressing an additional key of their choice, the phone or pager will automatically compute the resultant TAC, without the customer even seeing the Security String. This computation would be a completely internal, ensuring that only the TAC is displayed, and the PIN is not retained in the mobile phone or pager. A voice recognition interface could be implemented in voice activated phones and be able to compute the appropriate TAC on the simple command "TAC!" from an approved voice.

[0081] Customers could also have the option of choosing, when applying for an enabled card, a geometric shape, as will be discussed in more detail below, in which the security string will always be delivered. The customer would simply register his

chosen geometric shape to be displayed on screen and then visually apply their PIN pattern to determine the corresponding resultant TAC. This display can be interfaced by a WAP mobile phone, a G3 mobile phone, an Internet site display prompt or a secondary dedicated terminal placed at the point of sale.

[0082] The protocol of the present invention may be 'bolted-on' to an existing database server and can at least run on unmodified EFT/POS hardware such as: (1) AMEX; (2) Split dial EPOS; and (3) VISA AVS3. In addition, the dual channel protocol can be used to upgrade the security of Mondex systems (these already use a 4-PIN digit at POS).

[0083] The dual demand schema may use a standard G2 mobile phone, G3, and WAP device to receive the security string. If these devices include a modified SIM card interface for this security string the device may also include a GUI or an Enigma interface to simplify the derivation of the TAC.

[0084] FIG. 2 represents a diagram showing the protocol for the present invention applied to a point of sale environment. FIG. 2 displays the main components and steps for this transaction and displays two different options. The first option utilizes a split dial electronic funds transfer point of sale machine (EFT/POS), where the details of the transaction are directly sent via the Authorization Server 207. The second option utilizes the merchant acquirer's network.

[0085] In the direct dial scenario, the user 201 receives a security string 210 from the Authorization Server 207 which resides on the device 202. The security string 210 resides on the device 202, such as a mobile phone, until the user is ready to make a purchase. When the user 201 is ready to make a purchase they hand over, in step 220, their enabled credit card 204 to a merchant 205 to conduct the electronic funds transfer or point of sale (EFT/POS). The card 204 is swiped as usual at the merchant's 205 EFT/POS terminal. The user 201 reviews the security string 210 residing on their device 202 and determines their TAC for that particular sale. The four digit TAC 230 is provided to the merchant 205 by the user 201. The user 201 may provide the TAC verbally, by entering it into the POS terminal, or by entering the number on the mobile device 202. The credit card 204, TAC 230, and transaction amount are then sent, via the direct dial network 240, to the Authorization Server 207. The Authorization Server 207 confirms with the card issuer 209 that the account has sufficient funds in the account and that the TAC corelates with the user's PIN number and the issued security string 210. In the event that the account number, transaction amount, and TAC are verified the Authorization Server 207 allows the transaction to proceed.

[0086] In the second scenario, referred to as the merchant acquirer network scenario, the same initial steps apply. The user 201 receives a security string 210 which resides on the device 202, such as a mobile phone, and that when the user 201 is ready to purchase an item from the merchant 205 they, in step 220, present the merchant 205 with the registered credit or debit card 204. The card 204 is swiped at the EFT/POS terminal and again the user 201 determines their four digit TAC 230, via the security string 210 residing on their mobile phone or device 202. In this scenario, the transaction information including the account number of the card 200 and amount of purchase are routed via path 250 to scheme 252. The standard credit card transaction details and the pre-authorized PIN are sent to the card issuing host server 209. The scheme 252 sends the card 204 information and pre-authorization PIN to the card issuer host 209 via communications path 256. At the same time, the scheme 252 communicates with the Authorization Server 207 and verifies that the pre-authorized PIN correlates to the user's PIN. The card issuer 209 proceeds with the transaction and upon verification allows the transaction to proceed.

[0087] In addition to the dual channel schema described above, the present invention also allows for a single channel schema whereby a user would be able to use the present invention for such transactions as online purchasing via internet websites. The single channel schema and protocol is conducted via either a computer, a WAP device, Smart Card, Proprietary System or a G3 mobile phone, where the security string is received and the TAC transmitted on the same device. This protocol does not require a secondary channel to conduct a secure transaction.

[0088] The single channel protocol runs via an applet downloaded by the user onto their computer, WAP device or G3 mobile phone. The security string and the TAC can only be received by an enabled server and transmitted via an SSL link. The present invention is resistant to 'ghost' sites, where the user is unaware that the site they are dealing with is not certified, because the merchant (whether certified or not) would only be in possession of the users 'User name or card ID' and not the relevant TAC.

[0089] The single channel solution solves the problem encountered by transmitting the relevant TAC and security string over the Internet by instructing the users ISP (Web browser) to transmit only the user name to the merchant and the relevant TAC to the enabled server/database.

[0090] FIG. 3 shows each step along the process a user would take to register and use the single channel schema. The process is started in step 300 and in step 310 the user contacts the server host of the present invention through a single channel device such as a personal computer, an internet connected hand held device, a cell phone or wireless phone, or any device that may support a web browser via a single communication channel. Upon contact with the server or host of the present invention a log on web page containing the interface applet is sent to the user's device. In step two 320 the user is requested to input their user ID and preauthorized credit card or debit card number through an appropriate entry method. The user interface may include on screen drop down menus or other various user friendly applications to enhance the entry process of the user ID and credit card or debit card number. The user ID is sent to the server for verification. If the server verifies the user's identity a security string is sent to the client web page using the low processing overhead protocol (LPO protocol) with a prompt to initiate the applet. The applet is used to abstract and repack the TAC code according to the LPO protocol and start the Pin Safe interface.

[0091] In step 330 the Pin Safe interface is started enabling safe user entry of a PIN or TAC. The LPO protocol extraction is carried out using an automatic System Identification Digit (SID) and System Outgoing Digit (SOD) generation. As will be described in more detail below, the TAC code is pulled from the security string and repacked according to the LPO protocol and sent to the server host for verification. In step 340 the applet is stopped and destroyed, all values are zeroed and the security string residing on the device is cleared. The user sees an interface which identifies that the device is awaiting a response from the server. In step 350 the log on to the server is verified or rejected according to the user ID and TAC code response. If verified, confirmation is sent to the client browser followed by requested service access or transaction. In step 360 the session or transaction is finished allowing the user to close the session or the process or the session may be automatically closed triggered by some length of time of inactivity. The user's information with the single channel schema is terminated at step 370.

[0092] FIG. 4 displays the main components for a preferred embodiment of the single channel schema of the present invention. The user 401 would visit the secure host 407

the present invention and the server 407 would provide applets 470 for downloading to the user's device 403. The user 401 downloads an applet 470 via path 421 which is then stored on the device 403 as the customer applet 422. The web merchant 405 would also visit the Authorization Server 407 via path 450 and download the an applet 470 via path 451 which is stored on the merchant site 405 as merchant applet 452. The user 401 using the device 403 visits the web merchant site 405 via path 430 and selects items they wish to purchase by placing them in the basket 406 and selecting the appropriate credit or debit card for use 407. The merchant site 405 then accumulates the items in the basket 406, information about the card 407, and utilizing the merchant applet 452 routes the information along path 431 to the Authorization Server 407.

[0093] The Authorization Server 407 starts the verification process and using communications path 432 routes the appropriate information back through the merchant applet 452 to the customer applet 422 resident on the user's device 403. The user 401 is requested to enter the TAC. Once the user has entered the TAC, the TAC is sent along path 433 through the merchant back to the Authorization Server 407 to validate the response. In addition, the Authorization Server 407, at step 434, validates that there are sufficient funds in the account and in step 435 verifies that the information about the card 407, TAC, and account funds availability are verified. The Authorization Server 407 sends an "accept" notice along path 436 to the merchant site 405 which is then relayed, via path 437, to the users device 403.

[0094] FIGS. 5-7 also relate to single channel schemas utilizing different aspects and security protocols. In FIG. 5, the user 501 visits a merchant internet site 505 and would select various items for purchase. Upon checkout, payment is demanded via path 510 from the merchant site 505 to the user 501. The personal computer or device 503 contains an applet 522 which communicates with the site 505 and includes the proper software or applet 522 to notify, along path 520, the Authorization Server 507 that a transaction authorization is needed. The merchant domain name, transaction amount, user ID, and Transaction Authorization Code (TAC) are transferred from the user's device 503, along path 530, to the Authorization Server 507. Already present on the personal computer or user's device 503 is the security string for the user to determine their TAC code.

[0095] The Authorization Server 507 communicates with the merchant internet site 505, via path 540, to certify the card and transaction amount information. The Authorization Server 507 also forwards a transaction ID via path 541 to the user 501 through the user's personal computer 503. The transaction ID is forwarded to the merchant's internet site, along path 542, from the user's personal computer 503. The Authorization Server 507 certifies that the amount of purchase, the card information, and TAC are appropriate and sends the card details and amount along path 550 to the merchant internet site 505. The transaction details are sent from the merchant internet site 505 to the card issuer 509, via path 560, and ultimately the card issuer 509 sends payment via path 570 to the merchant internet site 505.

[0096] The single channel schema displayed in FIG. 6 is similar to the single channel schema displayed in FIG. 5 except that a wireless device 604 is included to remove the security string from the user's personal computer 603. In the schema illustrated in FIG. 6, the security string is omitted and simply the four digit TAC 620 for that transaction is transmitted from the Authorization Server 607 to the user's wireless device 604.

[0097] FIG. 7 is a single channel schema similar to the single channel schemas disclosed in FIGS. 5 and 6 except that instead of the four digit TAC being [illegible]

from the Authorization Server 707 to the wireless device 704, as described above in relation to FIG. 6, a thirteen digit security string 720 is sent to the wireless device 704. The schema disclosed in FIG. 7 discloses that as the user 701 selects items to be purchased from the merchant internet site 705 the payment demand along path 710 is sent to the user via the user's personal computer 703. The applet 722 then prompts the user to enter the TAC code, which the user determines from the security string 720 sent from the Authorization Server 707 to the wireless device 704. The applet 722 forwards the merchant domain name, transaction amount, user ID, and TAC to the Authorization Server 707 along path 730. The Authorization Server 707 certifies the transaction, along path 740, and forwards the user account number and amount along path 750 to the merchant internet site 705 . The transaction details are sent from the merchant internet site 705 to the card issuer 709, along path 760, and payment is then forwarded from the card issuer 709 to the merchant internet site 705 along path 770.

[0098] In the various online merchant scenarios employing the single or dual channel schema, as seen in FIGS. 2-7, there may be instances when the merchant does not have a particular item in stock and therefore can not process or complete the entire transaction immediately. In these instances, the merchant typically does not complete the transaction until the merchandise is dispatched. However, the user may have already input their TAC and the system would want to send the user a new pseudo-random security string.

[0099] The present invention overcomes this hurdle by having the Authorization Server receive the payment request and the active TAC. The merchant's server typically would transmit the order request to the authorisation server within a nominal 1-minute time out. However, if the merchant has received a purchase order for goods not in stock that order request will be delayed. The delayed order request will not be sent to the authorisation server until the goods have been received and are ready to be dispatched to the customer. Upon reception of the user's TAC and transaction details and the absence of the merchant's transmission of the order within the 1-minute timeframe the authorisation server will default to a deferred payment program.

[0100] The deferred payment program will hold the active TAC at the Authorization Server and is proof that the user has ordered the goods. A new security string can then be issued to the user for use during the next transaction. The authorisation server program will immediately send an email to the user stating details of the goods that he has requested from the merchant. Every week, or some other predetermined time interval, the Authorization Server will remind the user of his order request. The user is therefore informed of any pending transactions that will be eventually cleared through his account.

[0101] When the goods arrive at the merchant's depot and are ready to dispatch, the merchant details are then transmitted to the Authorization Server and the transaction is completed. If by this time the user has insufficient funds to cover the transaction amount the transaction would be declined, as typical in a standard credit card transaction.

[0102] FIG. 8 represents an additional schema utilizing features of the present invention in which a user has a pre-authorized or debit account 804. The user would see a live device 805, such as a vending machine, and would select items via path 810 thereby triggering the live device 805 to demand payment. The payment demand would be routed through the preauthorized liquid account 804 which is done by swiping the pre-authorized account 804, such as a credit or debit card, in step 840 through a card swipe device 806. In addition the micro payment demand would also notify the cardholder

swipe device 806 that a TAC would be requested. The user may have a personal device 803, such as a wireless phone, which would contain either a TAC or security string whereby the user would determine the TAC and enter the TAC 830 into the card swipe device 806. Alternatively, the user could enter the TAC 830 into the wireless device 803 which would wirelessly transmit the TAC 830 to the card swipe device 806 or Authorization Server 807. The details of the transaction are sent along path 850 from the card swipe device 806 to the Authorization Server 807. The Authorization Server 807 contains the information on the liquid account and if verified would notify a micro payment host 808 along path 860 to authorize payment. The micro payment host 808 then transfers payment along path 870 to the live device 805.

[0103] FIG. 9 represents a data control schema whereby elements of the present invention can be used to add a security overlay and pre-authorization into a database for controlling access to a database. In FIG. 9 the user 901 through their computer or laptop 903 wants access to a database 909. Access is requested along path 910 from the Authorization Server 907. A security string is sent from the Authorization Server 907 to the computer 903, via path 920, whereby the user determines their TAC. The user inputs the TAC which is transmitted to the Authorization Server 907 along path 930. Provided the TAC matches the appropriate PIN verified for the user 901 the Authorization Server 907 allows access to the database 909 along path 940. Further, the system can simply transmit the TAC, instead of the security string. The access data is then transmitted to the user's computer 903 through the Authorization Server 907 via path 950. In addition, the security string can be sent to the user 901 via an alternate path 921 such as through use of a wireless device 904.

[0104] FIG. 10 represents a remote bank balance inquiry schema whereby a user can check the balance of an account. In the schema presented in FIG. 10, the user 1001 through use of a cell phone, pager, or wireless device 1004 can request the balance of an account located in a bank 1008. The user is provided with a security string or TAC, via path 1010, which is resident on the wireless device 1004. The user determines their TAC code and either presents their TAC code through a bank teller (not shown) or inputs it into the wireless device 1004. The TAC code is sent to the Authorization Server 1007 which verifies that the TAC code is appropriate for the security string and corresponds with the user's PIN. The Authorization Server 1007 then communicates with the bank 1008 along path 1020 to retrieve the account information thereby providing the user with the requested information.

[0105] Two important aspects of the present invention which are utilized in the dual and single channel schemas described in relation to FIGS. 2-10 are the low processing overhead protocol and the security string operation. Certain wireless devices, such as web devices, cannot run high level encrypted programs due to their low processing overhead. The present invention incorporates a low processing overhead protocol which enables such devices to run highly secured transactions or downloads without using a large memory foot print. An additional benefit of the low processing overhead protocol is that existing transaction data issuing servers could also process information quicker than traditionally encrypted systems. The low processing overhead protocol evades the possibility of a correlation between the TAC and security string by simultaneously using multiple security strings. Only one of the multiple security strings is actually relevant and the remaining strings are used to hide the relevant string. The security strings contain identical digits but are arranged in different random orders. The user's applet receives the multiple security strings and distinguishes which string is relevant by using a system identifying digit (SID). The system identifying digit knows which of the security strings is genuine and instantly dumps the irrelevant strings and processes only the correct and relevant string. As an example, if the identifying digit

value was 4, the present invention would identify that the fourth security string was the relevant security string.

[0106] During a transaction, as will be described in conjunction with FIGS. 11 and 12, the user inputs their PIN and the TAC is internally calculated on the applet of the wireless device, personal computer EFT/POS, or as seen in FIG. 11, a thirteen digit security string 1100 would be sent from the Authorization Server to the user; device identifying a string of random digits, in this instance thirteen (13). The security string 1100 may come with a two letter identifying prefix 101 which identifies which server has issued the security string 1100. For example in FIG. 11, if the user's PIN was 2468 and the user applies that PIN number to the digit locations in the security string 1100. The user would look at the number in the second spot, the fourth spot, the sixth spot and the eighth spot to determine their transaction affirmation code or TAC for that particular transaction. In this instance, the user's PIN of 2468 would yield a TAC of 7693. Therefore, the user would input 7693 as the TAC to notify the Authorization Server to continue with the verification process.

[0107] Further explanation of the manner in which the TAC is secured within the transmitted secure security strings is explained in conjunction with FIG. 12. As seen in FIG. 12, the user, or customer 1201 has a known PIN 1202 (i.e. 1234). Stored on the user's device and downloaded from the server 1207 is the thirteen digit pseudorandom string 1203. In this instance, the customer's PIN value of 1234 as it relates to the pseudo string 1203 indicates a TAC code 1204 of '6891.' When the user is asked to verify or input the TAC 1204 to authorize the server 1207 to verify that the customer 1201 is in fact the authorized and registered customer the TAC 1204 may be manipulated and reversed in a myriad of ways to protect the code during transfer along the communications path to the server 1207. One method for providing a security overlay to the customer's PIN 1202 and the TAC code 1204 is to incorporate the TAC code into one thirteen digit string of a multitude of strings as previously described.

[0108] To identify the appropriate string the applet running on the customer's device would identify the relevant string through a system identifying digit 1205. The SID 1205 is used to identify which of the security strings is relevant. The SID 1205 may be determined in a myriad of ways including using certain numbers or combination of numbers of the user's PIN 1202, having the user set the SID 1205, and having the system server set the SID 1205. In the example shown in FIG. 12, the system set the SID value equal to 3. Therefore, the third string of nine strings is the relevant string. The nine (9) strings of thirteen (13) digits are sent via a data connect, such as a data stream 1230, to the user or customer's 1201 device. The applet on the device knows the SID 1205 value and extracts the relevant string 1203.

[0109] The customer reviews the relevant string 1203 resident on their device and determines their TAC 1204. The TAC 1204 is then intertwined into an outgoing relevant string which is grouped with eight (8) non-relevant strings. The outgoing data stream 1240 contains nine outgoing strings of thirteen digits. The location of the relative outgoing string is identified by a system outgoing digit (SOD) 1209 which can also be determined in a myriad of ways such as using or adding certain numbers of a customer's PIN 1202 or having the customer or system server select the SOD 1209.

[0110] In this example, the system set the system outgoing digit (SOD) 1209 value at 2. Therefore, the TAC 1204 will be integrated into the second of nine strings in the data stream of strings 1240. The TAC code 1204 may also be inversed, manipulated, have an automatic number added to it (i.e. each number is increased by one), or any other manner in which the PIN number can be modifed prior to transmission to the server 1207.

shown in FIG. 12, the TAC code 1204, is inversed to determine the location of the TAC numbers within the relevant outgoing string. For example, since the TAC 1204 in this example had a value of '6891' the inverse value of '1986' would dictate that in the first spot is the first digit of the TAC code, in the ninth spot is the second digit of the TAC and so forth until the TAC is integrated into the relevant security string.

[0111] The data stream of outgoing security strings 1240 containing the nine strings of thirteen digits is sent to the server 1207 which has an applet for verification. The server 1207 has an applet which knows the SOD 1209 value and can identify the relevant outgoing security string for verification of the user's PIN. Therefore, the applet on server the server 1207 knows the customer's PIN 1202 is '1234' and can determine that based upon the protocol established can determine that the SOD 1209 value was 2 and therefore the relevant string is the second string. The server 1207 will analyze the second string in relation to the user's stored PIN and expected response to verify that the response matches the TAC 1204 code from the initial string 1230.

[0112] Upon receiving the nine carrier strings, the server 1207 knows the outgoing digit position of the relevant TAC carrier string and instantly dumps the irrelevant strings and processes the correct selected TAC carrying string. The verification process at the server 1207 then matches the correct TAC with the issued security string and user's PIN number. If all three correlate, the authorization is completed and a new security string is transmitted to the user's applet.

[0113] Although in this example the number has been limited to nine lines of thirteen digits plus three (3) system digits per line (totaling 144 digits). It is not meant to limit the number of lines or digits that can be used. The nine lines of thirteen digits totaling 144 digits is intentionally less than the total global packet standard for many devices of 160 characters. Therefore, keeping the digit size below 160 keeps the processing overhead at a minimum allowing for low processing capability in WAP applications and wireless devices. In addition, this low processing overhead results in extremely fast verification times. The verification process also employs a filtering step followed by a single dimension array process which is not an intensive arithmetic computation system which would require more processing time.

[0114] In addition to the various single and dual channel schemas, the low processing overhead protocol, and use of the multiple security string security overlay the present invention may also provide a security overlay within the user interface. FIGS. 13a-13h represent various user interface examples to which a user may be provided for inputting a user's TAC. In the examples provided in 13a-13h the user would remember their personal PIN as a pattern rather than a numerical sequence. As an example, if the user had chosen to use the shape 1301 and shown display in FIG. 13e, they would only have to remember that they created a PIN which creates a small box 1303 inside of the shape 1301 disclosed in FIG. 13c. When the display is populated with random numbers then user applies their chosen design (i.e. small box 1303). In this example, the user's PIN from box 1303 would be '2389'. Therefore, knowing the PIN of '2389' and viewing the randomly generated numbers within the random display 1302 the user would see that the numbers '7538' correspond with their PIN number location. Therefore, the user's TAC for completing such a transaction or entry into the database, would be '7538'. The user interfaces disclosed in FIGS. 13a-h are merely exemplary and numerous displays, as well as colors and graphic symbols could be incorporated into the user interface. Therefore, the user would be able to create a graphic representation of their PIN without the need to remember the four digit PIN number.

[0115] Another feature of the present invention which deals with the user interface of

the system involves the use of a Pin Safe deterrent interface. Any device with a keyboard or touch sensitive interface which may be connected to a network or which is otherwise capable of downloading data or machine code may have the integrity of a password or key entry security system comprised. One way in which the system may be comprised is through the use of a Trojan program. A Trojan program is a small program which collects keyboard information for latter use. An additional program can also collect password or key entry information but fanes an unsuccessful logon attempt at the last digit of the logon entry and attempts to continue the logon with the real user unaware, by guessing the last digit (this is known as a "sniffer" program). Both of these techniques require actual data from a device keyboard or key pad or other input device. Whereas data may, by encryption or other means, be delivered and resent securely right up to and from the actual process occurring in the devices processing unit, if the security system requires meaningful user data entry to access or operate the security system that data may be intercepted and relayed greatly reducing the security of the system.

[0116] Although keyboard or small amounts of other input data may be redirected or stored with little or no user indication or system performance impact the same cannot be said for the device's graphical display, where the output is high throughput and device specific. Screen grabbing, or screen capturing, is possible but system resource intensive and therefore quite likely to be discovered by a user, especially on a device of comparatively low processing power. A good level of resistance could therefore be offered by an interface that provides information to a security system that is only meaningful to that system within the scope of its own time interface parameters and where any captured keyboard information has no external meaning. Similarly, any possible screen grabbed or screen captured information should not compromise the system's logon security.

[0117] The inputting of a Username, Password or PIN number in a computer, PDA, 2.5G or 3G mobile device is currently flawed for the following reasons: (1) the User can be seen from onlookers entering their PIN number into the device (called 'shoulder surfing'); (2) the keyboard could contain a 'Trojan' program that records the inputted Username, Password or PIN number (Trojans are downloaded without the knowledge of the User onto a computer and can reside there indefinitely); (3) PKI Certificates authenticate that the transaction was conducted on a certified computer, but they do not effectively authenticate the User behind the computer; and (4) computers running Microsoft Windows have a problem because Windows remembers the Username, Password or PIN number which creates a situation where the device stores the I/D of the User within the computer.

[0118] The "radar" deterrent or Pin Safe user interface of the present invention achieves a positive user I/D because the user has to be present during every transaction. The Pin Safe user interface is Trojan resistant because any key can be used to input a PIN or TAC which renders any Trojan key intercept information useless, as does the displayed information on screen.

[0119] In addition, the user interface is shoulder surfing resistant because there is nothing that could be gleaned from looking either at the screen or the keyboard input, rendering shoulder surfing a pointless exercise. Further, the system is resistant to PIN interception when using the Dual and Single channel (Applet) protocol. The protocol of the present invention is unique because it transmits a volatile TAC every time a transaction is made. A successful attempt to intercept/decrypt this information could not result in the user's real PIN being compromised.

[0120] Another feature of the present invention is that it is a multi-platform system. The PIN Safe user interface works on a wide variety of computers and applications because of its low memory footprint and simple generic user interface. The protocol and system as a whole is non device-specific and can run on any device such as a public use computer. The system does not have to run on a trusted computer system where the program history is known. With no digital certificate required for the computer the User could conduct a transaction on any computer worldwide.

[0121] Further, the user interface is easy to use because the user need know nothing about the protocol, TAC's and Security Strings. The PIN Safe user would merely input their unchanging PIN via the Pin Safe user interface. Further, the Pin Safe user interface is "tempest" proof because the interface does not display the users PIN or TAC (Pseudo PIN) on screen, and therefore is not subject to Electro-magnetic emissions from the VDU that could be the subject of surveillance via Tempest technologies. The strong protection gained by using the Pin Safe user interface of the present invention allows safe single PIN usage on a variety of accounts with differing security architectures which can be achieved by using a central PIN Authorization Server. Even if the security string resides on the device it is not a problem because the present invention does not require a digital certificate and therefore there is nothing in the memory of the computer that compromises the Users I/D if it falls into the wrong hands.

[0122] The Pin Safe user interface involves a unique method of inputting a PIN number into a computer, ATM, PDA, 2.5G or 3G Mobile Device. FIGS. 14 and 15a-15e are representative examples of the Pin Safe user interface screens. When a user wishes to conduct an online transaction, the Pin Safe applet will activate which will provide the "Start" user interface displayed in FIG. 14. Pressing any key on the user's computer screen TAC or PIN then activates the entry interface screen. The interface can be activated by using the keyboard, mouse, or a touch screen display.

[0123] As seen in FIGS. 15a-15e, the Pin Safe interface will now start to display (in this example in a clockwise manner) 12 digits in sequence (starting with 1 and ending in 12). During the display cycle, the User simply registers his PIN or TAC by pushing any key on their keyboard, mouse or any spot on the touch screen display when the digit they wish to register is illuminated. The Pin Safe display will rotate 4 times, once for every digit of a 4 PIN number.

[0124] At the 12thposition there is a dwell time to allow customer response for the starting of the next cycle accurately. When the first cycle for the first PIN number has finished the display will start again with another cycle. The cycles can also be identified by changing the illumination color. This process is repeated 4 times until all 4 digits are inputted to make up the User's 4 digit PIN.

[0125] For example, as seen in FIGS. 15a-15d, if the user's PIN was '2468' then on the first cycle the keyboard would be pressed when the 2<nd >digit was illuminated, see FIG. 15a. On the second cycle the keyboard would be pressed when the 4thdigit was illuminated (see FIG. 15b), on the third cycle the keyboard would be pressed when the 6thdigit was illuminated (see FIG. 15c), and on the fourth cycle the keyboard would be pressed when the 8thdigit was illuminated (see FIG. 15d). Only one display is seen at any one time on the screen preventing an onlooker from determining which PIN is being inputted. Further, the changing colors of the display background and the digits displayed can be pseudo-random.

[0126] After the User presses the keyboard to register the first [illegible]

run on period of time is activated. The run on process prevents shoulder surfers from seeing exactly which digit was registered. For example, as seen in conjunction with FIG. 15a, when the User wishes to register the first digit, as number 2, they would press any key on the keyboard when the number 2 or second digit is highlighted, however the display continues illuminating the numbers or digits after 2 around the cycle. The system may also illuminate only a portion of the numbers after the selected number, such as between 0 to 4 digits after the selected number, before speeding up the illumination of all numbers until completion of the cycle. A shoulder surfer would see the cycle speed up after the numbers 2, 3, 4, 5 or 6 were illuminated and would not be able to determine which digit had been registered. After the run on period, the system may increase the cycle speed to complete the cycle so that the user does not have to sit through the full cycle time to aide quick PIN entry. The run on period is normally less than the point in elapsed time from the key press to the time when the user would start to question whether a positive selection had been made. For short term visual memory, of a human, this is a maximum of around three seconds.

[0127] The run on period and increased cycle speed may be applied on all 4 cycles or displays. The dwell time between the digits being illuminated and the change in cycles is pseudo-random to prevent Trojan programs from determining which digit was inputted by correlating the display with the keyboard and the user's computer clock speed.

[0128] As seen in FIG. 15e, the Pin Safe user interface can also use characters, letters, or symbols instead of numbers on the display which would allows the user's code or pin to be any group of symbols or letters which spell a word. In addition, as previously discussed, in relation to FIG. 9, the present invention can be used for the remote access of data using either the Dual or Single Channel schema or protocol and the PIN Safe interface.

[0129] Enabling an existing database with the PIN Safe interface of the present invention can be done by providing an authentication server computer that registers the Users PIN number, issues and stores security strings, and correlates the received TAC to authenticate the user's identification.

[0130] In addition, the Pin Safe or Radar Interface can work within a computers own processor, within a LAN configuration, and over the Internet. Operating within a computers own processor the Pin Safe interface could act as a hack proof screensaver which means that when a user first started their computer they will be presented with the interface. The user must input their PIN accordingly and if the user decided to leave the computer for a short time, where there is the opportunity for criminal use of his computer, the user could press a function key which would activate the Pin Safe interface. Upon returning to the their computer they would simply click on their mouse or any key and enter their PIN via the Pin Safe interface.

[0131] In addition, if a user fails to input their PIN digit during any of the 4 sweep cycles, the present invention will allow the input of the PIN digit during any sweep (providied they are in the correct sequence). This means that a 'Reset' button will not require pushing unless the user has made a conscious mistake.

[0132] Additional schemas for employing the security features, measures, protocols, interfaces, and overlays of the present invention are discussed in connection with FIGS. 16-23.

[0133] As seen in FIG. 16, the Authorization Server 1607 is connected to the Entity 1

Client's, Host Gateway Server 1609. The Host Gateway Server 1609 is the database's 1611 connection to the Internet 1613 and it is placed outside the firewall 1615 that surrounds the host database 1611 (this is to ensure that any hacking activity cannot occur inside the database 1611). The remote data access configuration may also employ the Pin Safe interface 1623 in conjunction with the user 1601 and the user's device 1604. The system may also employ a backup server or database 1630.

[0134] The Authorization Server 1607 can be configured to act as dual or single channel system. Its architecture allows the Host Gateway Server 1609 to allow access to the database 1611 either via the present invention or via it's existing access procedure. This means that after installation, the enabled access trials can be conducted without affecting the original configuration.

[0135] FIG. 17 shows how multiple Clients 1740, 1750 can be accessed from one User 1701, using one PIN number. This is achieved by installing a Central PIN Authorization Server 1707 which consolidates the received TAC's with the issued security strings from any enabled Client 1740, 1750.

[0136] The Pin Safe interface can be applied various ways including the dual channel, single channel: Thin Client and single channel Applet embodiments. In the dual channel application as seen in FIG. 18, the User's TAC is inputted via the Pin Safe interface 1823 and it is sent directly to the Authorization Server 1807 through the Internet 1813. With the dual channel application no security string is sent to the Users computer 1822 and instead it is sent to the mobile device 1804 via SMS.

[0137] As seen in FIG. 18, the Security String is sent from authorization computer 1807 to the User's mobile device 1804. The user inputs the TAC via the Pin Safe interface 1823 and the Authorization Server 1807 receives the TAC via the Internet 1813.

[0138] In the single channel Thin Client application, as seen in FIG. 19, the Pin Safe interface applet 1923 resides on the Authorization Server 1907. The User 1901 accesses this applet 1923 remotely from any computer 1922 and does not need to 'set up' the computer 1922 by pre-downloading any form of program beforehand. As seen in FIG. 19, the User accesses the Authorization Server 1907 and applet 1923 via the Internet 1913. The User 1901 inputs their PIN, which is correlated at the source or Authorization Server 1907.

[0139] In the single channel Applet application, as seen in FIG. 20, the Pin Safe interface applet 2023 resides on the users computer 2022. The applet 2023 needs downloading only once and would be automatically sent to the user's computer 2022 during the registration process. The Pin Safe interface has been specifically designed with an extremely small memory footprint making the process of downloading and use very fast.

[0140] As seen in FIG. 20, the User accesses the Authorization Server 2007 via the Internet 2013. The user 2001 inputs their PIN, which the applet 2023 converts into a TAC (it does this automatically using the volatile security string resident in the applet 2023) and then sends, via the Internet 2013, for correlation at the Authorization Server 2007.

[0141] FIG. 21, shows a typical data access application where an Authorization Server 2107 has been fitted to a Gateway Server 2109 accessing a Database 2111. FIG. 21 assumes that the user 2101 has registered with the system and has the Pin Safe Interface applet 2123 on their computer. To access information from the Database 2111

the Authorization Server 2107 sends a new security string to the user's computer or G2 mobile phone 2104 via the Internet 2113 or through a wireless connection 2151. The security string 2151 resides on the device 2104 until the user 2101 wishes to access the Database 2111.

[0142] The User 2101 sends his volatile TAC to the Authorization Server 2107 to confirm his/her identity. In the dual channel scenario the user obtains their TAC from the G2 mobile device 2104 via either visual extraction (using their PIN as a sequencer) or Smart PIN or SIMM extraction where the User 2101 enters their PIN into the device 2104 and the relevant TAC digits are displayed on the device 2104 screen. The TAC is then inputted into the user's computer (not shown). In the single channel scenario the user simply inputs their PIN into the Pin Safe interface 2123. The PIN is then converted into a TAC within the applet 2123 and transmitted via path 2120 to the Authorization Server 2107.

[0143] Only when the user's identification is positively confirmed, by correlating the received TAC to the user's PIN and previously issued security String is the request 2130 for data, via the Gateway Server 2109, initialized via path 2130. The requested data can now be routed via path 2140 to the user's computer.

[0144] The Pin Safe interface is not required if the security string delivery and TAC extraction are conducted on a second device such as through the dual channel protocol. Using a G2 mobile phone a user can receive a security string and extract the TAC independent of the data accessing computer. This means that the TAC can be entered into the data accessing computer without the requirement of the Pin Safe interface because a TAC is inherently secure against shoulder surfing, Trojans, Tempest technologies and online user identification theft.

[0145] FIG. 22 displays a generic Server/Gateway Schema incorporating various aspects of the present invention. The generic secure server schema may also incorporate UPS (Uninterruptible Power Supply), Dual Redundancy, Disk Mirrored, Linux Web Server 2245 and Internal Firewall 2215, the Pin Safe applet 2223, a user database 2207 and an internal maintenance any reporting function 2211.

[0146] FIG. 23 shows the Generic Integration Platform which displays the Authorization Server 2307 inside a firewall 2215. The Authorization Server 2307 is connected to a Net Server 2317 and a host database 2311. The host database 2311 may also be inside it's own firewall 2316.

[0147] Additionally the authorization process identifies the user via a response rather than an identifying account and its parameters which negates the so called "Friendly Fraud" from misuse of online fraud guarantees. An added benefit is that there is also an audit trail for database files access.

[0148] Any reference herein to a computer means any personal computer, ATM, PDA, G2.5 Mobile Device, G3 Mobile Device, or any device with a CPU. Any reference herein to a transaction means any financial transaction, remote Data Access procedure, or any interface transaction between a user and a system. The numbers on the various user interfaces and displays are merely exemplary and the use of characters, letters, colors and such may be used individually or in combination and still fall within the intended scope of the present invention.

[0149] While the preferred embodiment and various alternative embodiments of the invention have been disclosed and described in detail herein and it may be [illegible]

will be apparent to those skilled in the art that various changes in form and detail may be made therein without departing from the spirit and scope thereof, and that the scope of the present invention is to be limited only by the following claims.

Claims: CN1561508 (A) — 2005-01-05

Code identification method and system

Claims not available for CN1561508 (A)
Claims of corresponding document: US2002029342 (A1)

A high quality text as facsimile in your desired language may be available amongst the following family members:

AU2005100466 (B4) CA2421495 (A1) DK1316076 (T3) ES2403039 (T3) JP2004508644 (A) KR20030036766 (A) MXPA03002050 (A) NZ524391 (A) PT1316076 (E) US2002029342 (A1) WO0221463 (A2) US2002059146 (A1)

- Original claims
- Claims tree

1. An identity verification secure transaction system comprising:
a host computer for storing a user code associated with a user, for supplying a pseudo-random security string for a transaction, wherein said host computer determines a one time transaction code by applying said user code to said pseudo-random security string; and
at least one electronic device in electronic communication with said host computer for administering said transaction by receiving and displaying said pseudo-random security string and for receiving a user transaction input code, wherein said user transaction input code is determined by applying said user code to said pseudo-random security string displayed on said at least one electronic device and said user transaction input code is sent to said host computer;
wherein said host computer verifies that said user input code matches said one time transaction code.

2. The system of claim 1, wherein said at least one electronic device is an Electronic Funds Transfer Point of Sale (EFT/POS) device.

3. The system of claim 1, wherein said at least one electronic device is comprised of an electronic Funds Transfer Point of Sale (EFT/POS) device for administering said transaction and receiving said user transaction input code and a wireless device associated with said user for receiving and displaying said pseudo-random security string.

4. The system of claim 3, where said one time transaction code is received and

displayed by said wireless device instead of said pseudo-random security string.

5. The system of claim 1, wherein said at least one electronic device is a wireless device associated with said user.

6. The system of claim 5, wherein said one time transaction code is sent to said wireless device instead of said pseudo-random security string.

7. The system of claim 1, wherein said at least one electronic device is comprised of:
a user computer, in electronic communication with said host computer, for receiving and displaying said pseudo-random security string and receiving said user transaction input code; and
a merchant computer, in electronic communication with said user computer and said host computer, for administering said transaction, wherein one of said at least one electronic device relays said user transaction input code to said host computer for user identity verification.

8. The system of claim 7, wherein said user computer and said merchant computer communicate via the Internet.

9. The system of claim 7, wherein said one time transaction code is received and displayed by said user computer instead of said pseudo-random security string.

10. The system of claim 1, wherein said at least one electronic device is comprised of:
a wireless device associated with said user for receiving and displaying said pseudo-random security string,
a user computer, in electronic communication with said host computer, for receiving said user transaction input code; and
a merchant computer, in electronic communication with said user computer and said host computer, for administering said transaction, wherein one of said at least one electronic device relays said user transaction input code to said host computer for user identity verification.

11. The system of claim 10, wherein said one time transaction code is received and displayed by said wireless device instead of said pseudo-random security string.

12. The system of claim 1, wherein said host computer upon verification allows completion of said transaction.

13. The system of claim 1, wherein said host computer upon verification allows access to a database.

14. The system of claim 1, wherein said host computer upon verification allows access to account information.

15. A method of verifying an identity for conducting secure transactions comprising the steps of:
storing information about a user pin associated with a host computer;
generating a pseudo-random security string by said host computer;
determining a transaction code by applying said user pin to said pseudo-random security string;
transmitting said pseudo-random security string to at least one electronic device,
displaying said pseudo-random security string on said at least one electronic device for use by said user to determine a user transaction input code by applying said user pin;

to said pseudo-random security string;
inputting said user transaction input code on said at least one electronic device;
transmitting said user transaction input code from said at least one electronic device to said host computer; and
determining, by said host computer, whether said transaction code and said user transaction input code match.

16. The method of claim 15, further including the step of completing a transaction when said transaction code and said user transaction input code match.

17. The method of claim 16, further including the step of providing access to a database when said transaction code and said user transaction input code match.

18. The method of claim 16, further including the step of providing access to account information when said transaction code and said user transaction input code match.

19. The method of claim 15, further including the step of transmitting and displaying said pseudo-random security string on an Electronic Funds Transfer Point of Sale (EFT/POS) device.

20. The method of claim 15, further including the step of transmitting and displaying said pseudo-random security string on a wireless device associated with said user.

21. The method of claim 15, further including the step of transmitting and displaying said pseudo-random security string on a user computer wherein said user computer is in electronic communication with said host computer.

22. The method of claim 21, further including the step of communicating between the said host computer and said user computer via the Internet.

23. The method of claim 15, further including the step of transmitting and display said transaction code to said at least one electronic device.

24. A secure user code entry interface system comprising:
a secure user code entry interface for entry of a user code on an electronic device wherein said electronic device has a display; wherein said secure user code entry interface contains at least one active display for entry of at least one digit of said user code by a user; wherein said active display illuminates at least one display digit within said active display and said user enters said at least one digit of said user code by a response through an input device at a response time when said at least one display digit which corresponds with said at least one digit of said user code is illuminated in said active display; and
a random run on time is added to said response time to extend said at least one active display.

25. The secure user code entry interface system of claim 24, wherein said response is entered by keying any one of a plurality of keys of a keyboard.

26. The secure user code entry interface system of claim 24, wherein said response is entered by keying any one of a plurality of keys of a mouse.

27. The secure user code entry interface system of claim 24, wherein said response is entered through any area of a touch sensitive display.

28. The secure user code entry interface system of claim 24, wherein said secure user code entry interface program contains a plurality of cycles of said at least one active displays for entry of each digit of said user code.

29. The secure user code entry interface system of claim 24, wherein said random run on time is less than three (3) seconds.

30. An identity verification secure transaction system comprising:
a host computer for storing a user code associated with a user;
an electronic device in electronic communication with said host computer, wherein said electronic device has a display and a user input device; and
a secure user code entry interface viewable on said display of said at least one electronic device for entry of said user code, wherein said secure user code entry interface contains at least one cycle with an active display for entry of said user code;
wherein said user enters at least one user code digit of said user code by a response through said user input device at a response time when a display digit which corresponds with said at least one user code digit of said user code is illuminated in said active display, and
wherein said each digit of said at least one user code digit if entered in each cycle of said at least one cycle and a random run on time is added to said response time to extend each cycle of said at least one cycle; and
wherein the entered said user code is transmitted to said host computer for verification with the stored said user code.

31. The identity verification secure transaction system of claim 30, wherein said response is entered by keying any one of a plurality of keys of a keyboard.

32. The identity verification secure transaction system of claim 30, wherein said response is entered through any area of a touch sensitive display.

[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G07F 19/00
G07F 7/10 H04L 9/18

[12] 发明专利申请公开说明书

[21] 申请号 01812009.1

[43] 公开日 2005 年 1 月 5 日

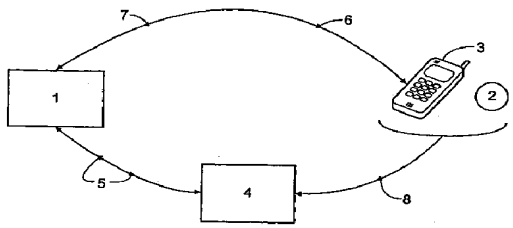
[11] 公开号 CN 1561508A

[22] 申请日 2001.9.7 [21] 申请号 01812009.1
[30] 优先权
[32] 2000. 9. 7 [33] GB [31] 0021964.2
[32] 2000. 9.15 [33] US [31] 09/663,281
[32] 2001. 7.27 [33] US [31] 09/915,271
[86] 国际申请 PCT/GB2001/004024 2001.9.7
[87] 国际公布 WO2002/021463 英 2002.3.14
[85] 进入国家阶段日期 2003.3.7
[71] 申请人 斯维沃安全有限公司
地址 英国北约克郡
[72] 发明人 温斯顿·唐纳德·基奇
[74] 专利代理机构 北京英赛嘉华知识产权代理有限责任公司
代理人 余 朦 陈宇萱
权利要求书 9 页 说明书 32 页 附图 24 页

[54] 发明名称 代码识别方法及系统

[57] 摘要

一种用于在电子通信环境中安全识别个人的系统和方法，其中一台计算机主机被改造成能与由个人操作的一个特定电子通信设备进行通信。个人被配备了一个掩码，该掩码只为个人所知并且保存在计算机主机中，但是从来不在个人与计算机主机之间电子传送。当个人需要使其自身被计算机主机识别出来的时候，计算机主机向特定电子通信设备发送一个伪随机字串，而掩码则必须根据预定规则被应用于该伪随机字串，用以产生一个易失性识别码，该易失性识别码随后被回送到计算机主机。当该易失性识别码与计算机主机中通过将其中保存的掩码应用于伪随机字串所得到易失性识别码相匹配时，计算机主机将会获得一个肯定的识别结果。这样，个人的掩码从未被电子传送，由此避免被截取，并且对每个不同的伪随机字串来说，易失性识别码各不相同，由此使通过欺诈截获的通信变得毫无意义。



ISSN1008-4274

知识产权出版社出版

1. 一种代码识别系统，该系统包括一台电子计算机，一个特定电子通信设备，该设备可被操作而与电子计算机通信，以及至少一个电子通信设备，该设备可被操作用于与电子计算机进行通信，其中，所述电子计算机包含涉及所述特定电子通信设备的数据，该数据包括一个永久识别码、一个掩码和一个允许实现电子计算机与特定通信设备之间电子通信的识别码，其中所述永久识别码被输入至所述少一个电子通信设备并被发送到所述电子计算机，所述电子计算机产生一个伪随机字串并将其发送到所述特定电子通信设备，所述掩码被应用于所述伪随机字串，以便根据预定规则产生一个易失性识别码，所述易失性识别码由所述特定电子通信设备或所述至少一个电子通信设备被回送给所述电子计算机，所述电子计算机通过将所述掩码根据预定规则应用于所述伪随机字串，从而获取一个易失性识别码，并对照该易失性识别码来检查发送到其自身的易失性识别码，其中，在所述电子计算机发现这两个易失性识别码相互匹配时，它将产生一个肯定的识别结果；该方法的特征在于：

i）所述伪随机字串包含一个由字符组成的第一线性阵列，在该第一阵列中，每个字符都具有一个指定的数字位置（第一、第二、第三等等）；

ii）所述掩码包含一个由数字组成的第二线性阵列，在该第二阵列中，每个数字都具有一个指定数字位置（第一、第二、第三等等）；以及

iii）用于将所述掩码应用于所述伪随机字串以产生所述易失性识别码的预定规则根据所述第二阵列中的数字按照位置顺序依次选择所述第一阵列中的数子位置，并且顺序地返回由所述第一阵列中选出的字符以形成一个第三线性阵列，该第三线性阵列形成了所述易失性识别码。

2. 如权利要求1所述的系统，其特征在于，所述特定电子通信设备和所述至少一个电子通信设备是同一设备。

3. 如权利要求1所述的系统，其特征在于，所述特定电子通信设备和所述至少一个电子通信设备是单独的设备。

4. 如上述权利要求中的任意一项权利要求所述的系统，其特征在于，所述特定电子通信设备是移动电话、寻呼机或个人数字助理。

5. 如权利要求3或从属于权利要求3的权利要求4所述的系统，其特征在于，所述至少一个电子通信设备是一个EFTPOS终端或类似设备。

6. 如上述权利要求中的任意一项权利要求所述的系统，其特征在于，所述永久识别码以带有个人和/或机器可读的标记的形式而被提供。

7. 一种用于将一特定电子通信设备或是其用户识别给电子计算机的方法，所述电子计算机上存有涉及所述特定电子通信设备或其用户的数据，该数据包括一个永久识别码、一个掩码和一个允许实现所述电子计算机与所述特定通信设备之间的电子通信的识别码，其中所述永久识别码被输入给至少一个电子通信设备并由此被发送到所述电子计算机，所述电子计算机将所述永久识别码与允许实现电子计算机与特定电子通信设备之间通信的所述识别码相关联，并且在将该识别码被发送到特定电子通信设备之前产生一个伪随机字串，所述掩码根据预定规则而被应用于该伪随机字串，用以产生一个易失性识别码，该易失性识别码被输入给所述特定电子通信设备或所述至少一个电子通信设备，并被传送给所述电子计算机，在所述电子计算机中，所述易失性识别码被与所述电子计算机中通过将所述掩码根据预定规则应用于伪随机字串而产生的一个易失性识别码进行比较，当这两个易失性识别码匹配时，所述计算机将产生一个肯定的识别结果；该方法的特征在于：

i）所述伪随机字串包含一个由字符组成的第一线性阵列，在该第一阵列中，每个字符都具有一个指定的数字位置（第一、第二、第三等等）；

ii）所述掩码包含一个由数字组成的第二线性阵列，在该第二阵列中，每个数字都具有一个指定的数字位置（第一、第二、第三等等）；以及

iii）用于将所述掩码应用于所述伪随机字串以产生所述易失性识别码的预定规则根据所述第二阵列中的数字按照位置顺序依次选择所述第

一阵列中的数子位置，并且顺序地返回由所述第一阵列中选出的字符以形成一个第三线性阵列，该第三线性阵列形成了所述易失性识别码。

8. 如权利要求7所述的方法，其特征在于，所述伪随机字串包含至少一个字符，该字符代表的是涉及个人的数据的某个条件。

9. 如权利要求7或8所述的方法，其特征在于，所述特定电子通信设备和所述至少一个电子通信设备是同一设备。

10. 如权利要求7或8所述的方法，其特征在于，所述特定电子通信设备和所述至少一个电子通信设备是单独的设备。

11. 如权利要求9或10所述的方法，其特征在于，所述特定电子通信设备是移动电话、寻呼机或是个人数字助理。

12. 如权利要求10或从属于权利要求10的权利要求11所述的方法，其特征在于，所述至少一个电子通信设备是一个EFTPOS终端或类似设备。

13. 一种身份验证安全交易系统，包括:

i）一台计算机主机，用于存储与用户关联的用户代码，用于为交易提供一个伪随机安全字串，其中，所述计算机主机通过将所述用户代码应用于所述伪随机安全字串来确定一个一次性交易代码;

ii）至少一个电子设备，该设备通过接收并显示所述伪随机安全字串与用于管理交易的所述计算机主机进行电子通信，并且用于接收一个用户交易输入代码，其中，所述用户交易输入代码是通过将所述用户代码应用于显示在所述至少一个电子设备上的所述伪随机安全字串来确定的，并且所述用户交易输入码被发送到所述计算机主机; 其中:

iii）所述计算机主机验证所述用户输入代码与所述一次性交易码相匹配。

14. 如权利要求13所述的系统，其特征在于，所述至少一个电子通信设备是一个交易点资金电子过户（EFT/POS）设备。

15. 如权利要求13所述的系统，其特征在于，所述至少一个电子通信设备包括一个用于管理所述交易并接收所述用户交易输入代码的交易点资金电子过户（EFT/POS）设备，以及一个与所述用户关联并用于接收和显示所述伪随机安全字串的无线设备。

16. 如权利要求15所述的系统，其特征在于，所述无线设备接收和显示的是所述一次性交易码，而不是所述伪随机安全字串。

17. 如权利要求13所述的系统，其特征在于，中所述至少一个电子设备是一个与所述用户关联的无线设备。

18. 如权利要求17所述的系统，其特征在于，发送到所述无线设备的是所述一次性交易码，而不是所述伪随机安全字串。

19. 如权利要求13所述的系统，其特征在于，所述至少一个电子设备包括：

i）一台用户计算机，它与所述计算机主机进行电子通信，用于接收和显示所述伪随机安全字串，并且接收所述用户交易输入代码码；以及

ii）一台商家计算机，它与所述用户计算机和所述计算机主机进行电子通信，用于管理所述交易，其中，所述至少一个电子设备中的一个设备将所述用户交易输入代码转达给所述计算机主机，以便进行用户身份验证。

20. 如权利要求19所述的系统，其特征在于，所述用户计算机和所述商家计算机通过互联网通信。

21. 如权利要求19或20所述的系统，其特征在于，所述用户计算机接收和显示的是所述一次性交易码，而不是所述伪随机安全字串。

22. 如权利要求13所述的系统，其特征在于，所述至少一个电子设备包括：

i）一个与所述用户关联的无线设备，用于接收和显示所述伪随机安全字串；

ii）一台用户计算机，它与所述计算机主机进行电子通信，用于接收所述用户交易输入代码；以及

iii）一台商家计算机，它与所述用户计算机和所述计算机主机进行电子通信，用于管理所述交易，其中，所述至少一个电子设备中的一个设备将所述用户交易输入代码转达给所述计算机主机，以便进行用户身份验证。

23. 如权利要求22所述的系统，其特征在于，所述无线设备接收和显示的是所述一次性交易码，而不是所述伪随机安全字串。

24. 如权利要求13到23中的任一权利要求所述的系统，其特征在于，所述计算机主机基于验证来允许完成所述交易。

25. 如权利要求13到24中的任一权利要求所述的系统，其特征在于，所述计算机主机基于验证来允许访问一数据库。

26. 如权利要求13到25中的任一权利要求所述的系统，其特征在于，所述计算机主机基于验证来允许访问一账户信息。

27. 一种用于通过验证身份以实施安全交易的方法，包括以下步骤：

i）保存与一计算机主机有关的用户 pin 的信息；

ii）由所述计算机主机产生一个伪随机安全字串；

iii）通过将所述用户 pin 应用于所述伪随机安全字串来确定一个交易

代码;

iv）将所述伪随机安全字串传送给至少一个电子设备;

v）将所述伪随机安全字串显示在所述至少一个电子设备上，以便由所述用户通过将所述用户代码应用于所述伪随机安全字串来确定一个用户交易输入代码;

vi）在所述至少一个电子设备上输入所述用户交易输入代码;

vii）将所述用户交易输入代码从所述至少一个电子设备发送到所述计算机主机；以及

viii）由所述计算机主机确定所述交易代码是否与所述用户交易输入代码相匹配。

28. 如权利要求27所述的方法，其特征在于还包括以下步骤：当所述交易代码和所述用户交易输入代码相匹配时，完成交易。

29. 如权利要求27或28所述的方法，其特征在于还包括以下步骤：当所述交易代码和所述用户交易输入代码相匹配时，提供对一数据库的访问。

30. 如权利要求27到29中的任一权利要求所述的方法，其特征在于还包括以下步骤：当所述交易代码和所述用户交易输入代码相匹配时，提供对账户信息的访问。

31. 如权利要求27到30中的任一权利要求所述的方法，其特征在于还包括以下步骤：在一个交易点资金电子过户（EFT/POS）设备上传送和显示所述伪随机安全字串。

32. 如权利要求27到30中的任一权利要求所述的方法，其特征在于还包括以下步骤：在一个与所述用户关联的无线设备上传送和显示所述伪随机安全字串。

33. 如权利要求27到30中的任一权利要求所述的方法，其特征在于还包括以下步骤：在一用户计算机上传送和显示所述伪随机安全字串，其中，所述用户计算机与所述计算机主机进行电子通信。

34. 如权利要求33所述的方法，其特征在于还包括以下步骤：所述计算机主机和所述用户计算机之间通过互联网进行通信。

35. 如权利要求15所述的方法，其特征在于还包括以下步骤：将所述交易代码发送给所述至少一个电子设备，并在所述至少一个电子设备上显示该交易代码。

36. 一种安全的用户代码输入界面系统，包括：

i）一个安全的用户码输入界面，用于在一电子设备上输入用户代码，其中所述电子设备具有一个显示器；其中所述安全的用户码输入界面包含至少一个发光显示，用于使所述用户输入所述用户代码中的至少一位数字；其中所述发光显示照明或加亮所述发光显示中的至少一位显示数字，并且，当符合所述用户代码中至少一位数字的所述至少一位显示数字在所述发光显示上被照明或加亮的时候，所述用户在应答时间通过一个输入设备做出一个应答以输入所述用户代码中的至少一位数字；并且其中

ii）一个随机的连续时间被添加到所述应答时间中，以便延长所述至少一个发光显示。

37. 如权利要求36所述的安全的用户代码输入界面系统，其特征在于，所述响应是通过点击一个键盘上多个按键中的任意一个按键而被输入的。

38. 如权利要求36所述的安全的用户代码输入界面系统，其特征在于，所述响应是通过点击一鼠标的多个按键中的任意一个而被输入的。

39. 如权利要求36所述的安全的用户代码输入界面系统，其特征在于，所述响应是通过一触摸显示上的任意区域而被输入的。

40. 如权利要求36到39中的任一权利要求所述的安全的用户代码输入界面系统，其特征在于，所述安全的用户代码输入界面程序包含所述至少一个发光显示的多个循环，用以输入所述用户代码中的各位数字。

41. 如权利要求36到40中的任一权利要求所述的安全的用户代码输入界面系统，其特征在于，所述随机的连续时间少于三（3）秒钟。

42. 一种身份验证安全交易系统，包括：

i）一台计算机主机，用于保存一个与用户关联的用户代码；

ii）一个电子设备，它与所述计算机主机进行电子通信，其中，所述电子设备具有一个显示器和一个用户输入设备；以及

iii）一个安全的用户代码输入界面，它在所述至少一个电子设备的用于输入所述用户代码的所述显示器上是可视的，其中，所述安全的用户代码输入界面包含至少一个具有用于输入所述用户代码的发光显示的循环；其中，当符合所述用户代码中所述至少一个用户代码数字的显示数字在所述发光显示中被照明或是被加亮的时候，所述用户在应答时间使用所述用户输入设备做出一个响应以输入所述用户代码中至少一个用户码数字；

iv)其中所述至少一位用户代码数字中的所述各位数字是在所述至少一个循环的各个循环中被输入的，并且一个随机的连续时间被添加到所述应答时间，以延长所述至少一个循环的每个循环；以及

v）其中，输入的所述用户代码被发送到所述计算机主机，以便用保存的所述用户代码来加以验证。

43. 如权利要求42所述的身份验证安全交易系统，其特征在于，所述响应通过点击一键盘上多个按键中的任意一个而被输入。

44. 如权利要求42所述的身份验证安全交易系统，其特征在于，所述响应是通过一触摸显示上的任意区域而被输入的。

代码识别方法及系统

本发明涉及一种用于识别用户或设备的系统和方法，这种系统和方法还能够被可选地用于例如经由电话连接或是互联网这类电子计算机系统在用户或设备与第三方之间进行交易。

各种系统由于在电信链路或其他链路上使用程度不同的安全方式来执行电子交易而闻名。一种有名的系统称为销售点资金电子过户（EFTPOS），在这种系统中，用户获得一张带有唯一识别代码的信用卡或借记卡，该识别代码通常以个人可读的形式印在卡上，并且还被编码在卡背面的机器可读磁条中。出于进一步识别的目的，卡上通常还包含有使用户在其中永久包含他或她的签名的空间。在使用中，例如用户希望在零售店购买物品时，他或她把借记卡或信用卡交给商店雇员。然后该卡由一个读卡器刷取，涉及卡身份、零售店身份和所购买商品或服务价格的信息通过电话连接被发送到由发卡方（通常是银行或类似机构）操作的远程计算机服务器上。远程计算机服务器证实用户卡账户包含足以支付所提出的交易的资金或信用，并且检查用户卡账户当前是可以使用的（举例来说，检查卡没有被挂失），然后，远程计算机服务器向读卡器发回一个证实信号，指示可以允许交易。之后，商店雇员必须获取用户签名样本，并将其与磁卡背面的签名比较，以便检查用户身份。如果签名看上去匹配，那么商店雇员操作读卡器来完成交易，然后，支付交易费用所需要的资金被从用户卡账户电子过户到零售店。如果签名看上去不匹配，那么在许可交易之前，商店雇员可以要求附加的证据鉴定，也可以简单地直接拒绝交易并且保留可能是被盗的用户卡，由此防止了任何未经许可的资金过户。这个系统很容易受到欺诈性滥用，因为对失窃卡和窃贼来说，有可能伪造授权用户的签名。

在一个对上述系统的改进方案中，持卡用户可被分配一个个人识别号（PIN），该识别号通常是一个四位编码，并且理论上只有用户和发卡

方知道这个识别号。代替在销售点提供他或她的签名样本，或是除了在销售点提供他或她的签名样品之外，持卡用户还需要将其PIN输入读卡器，这个信息与卡和零售店识别数据以及涉及交易价格的数据一起被发送到远程计算机服务器。通过使用PIN来提供附加的识别验证，这个系统有助于防止通过伪造签名实施的欺诈行为，但是该系统仍然不是完全安全的，因为PIN在几次交易之间并未改变，因此，当PIN在读卡器与远程服务器之间被传送时，PIN有可能与卡识别数据一起被截取。此外，对窃贼来说，有可能看到用户将他或她的PIN输入读卡器并记住PIN。如果窃贼也能通过例如丢弃的现金收据、或是与商店雇员合谋而得到卡识别资料、或者甚至抢劫已授权卡的用户的卡，那么制造一张包含所有适当识别信息的伪造卡以用于以后的欺诈性使用将是一件非常简单的事情。

根据本发明的第一方面，它提供了一种经过编码的识别系统，该系统包括一台电子计算机；一个特定电子通信设备，该设备可被操作而与电子计算机通信；以及至少一个电子通信设备，该设备可被操作而与电子计算机通信，其中，电子计算机包含与所述特定电子通信设备有关的数据，该数据包括一个永久识别码、一个掩码以及一个允许实现所述电子计算机和所述特殊通信设备之间电子通信的识别码，其中永久识别码被输入至少一个电子通信设备并被发送到电子计算机，电子计算机产生一个伪随机字串并将其发送到所述特定电子通信设备，所述掩码被应用于该伪随机字串以便根据预定规则产生一个易失性识别码，该易失性识别码由所述特定电子通信设备或是至少一个电子通信设备回送到电子计算机，电子计算机根据预定规则将掩码应用于伪随机字串，从而获取一个易失性识别码，并对照该易失性识别码来检查发送到其自身的易失性识别码，其中，当这两个易失性识别码相互匹配的时，电子计算机将做出一个肯定的识别结果。

根据本发明的第二方面，它提供了一种用于将特定电子通信设备或是其用户识别给电子计算机的方法，该电子计算机中保存有与所述特定电子通信设备或是其用户有关的信息，其中包括一个永久识别码、一个掩码和一个允许实现电子计算机和特定电子通信设备之间通信的识别码，其中，所述永久识别码被输入至少一个电子通信设备，由此被传送

到电子计算机，电子计算机将永久识别码与允许实现电子计算机与特定电子通信设备之间通信的识别码相关联，并且在将该识别码发送到所述特定电子通信设备之前产生一个伪随机字串，掩码根据预定规则而被应用于所述伪随机字串，以便产生一个易失性识别码，该易失性识别码被输入所述特定电子通信设备或至少一个电子通信设备，并被传送到电子计算机，在电子计算机中，所述易失性识别码被与一个通过将掩码应用于伪随机字串而产生的易失性识别码进行比较，当这两个易失性识别码相互匹配时，电子计算机将得出一个肯定的识别结果。

所述特定电子通信设备可以是一个独立于所述至少一个电子通信设备的设备，也可以是同一设备。举例来说，该特定电子通信设备可以是移动电话、寻呼机、陆线电话、个人数字助理或是由特定人员拥有或专门操作的计算机。所述至少一个通信设备可以是一个资金电子过户（EFT）终端或是一个销售点资金电子过户（EFTPOS）终端，也可以是与上面相同，是移动电话、寻呼机、陆线电话、个人数字助理或是由特定人员拥有或专门操作的计算机。

所述永久识别码可以按照持卡人和/或机器可读数据的卡的形式提供给用户。

在所述特定电子通信设备是移动电话、寻呼机或个人数字助理的情况下，实现电子计算机和特定电子通信设备之间电子通信的识别码可以是移动电话号码或寻呼机号码，识别码还可以是电子邮件地址或是任何允许与给出的特定电子通信设备之间进行特定通信的类似代码。

在特定电子通信设备是移动电话或类似设备的情况下，伪随机字串可以按照基于短信服务（SMS）协议的文本消息形式发送。根据特定电子通信设备的性质，在合适情况下，也可以采用其它公知的通信协议。

本发明的实施例以多种方式提供了附加的识别安全性。首先，除了要求个人使用永久识别码之外，系统还要求个人拥有一个适当的特定电子通信设备。其次，由于系统需要用户将其掩码作用于伪随机字串以在不同时传送掩码以及永久识别码的情况下根据预定规则产生一个易失性识别码，因此，对非授权人员来说，要对电子计算机、特定电子通信设备和/或至少一个电子通信设备之间的通信进行截取以确定掩码和永久识

别码将是非常困难的。

可以预见，本发明能够扩展到这样一种情况，其中有必要建立特定电子通信设备的安全识别，而不是个人安全识别。举例来说，本发明可被用作远程计算机之间安全“握手”协议的一部分，确实并可靠地用于将特定电子通信设备识别给电子计算机，其中特定电子通信设备自身就可能是一台电子计算机。电子计算机和特定电子通信设备都把掩码保存在自己的存储器中，但是除了经由安全连接之外，它们不会相互交换掩码，理论上，安全连接与它们的正常通信装置是完全分离的。

掩码可以采用多种形式。在一个当前的优选实施例中，一个人被配备或选择一个四位数字串，例如 3928，该数字串类似于当前在操作自动柜员机（ATM）时使用的公知 PIN 码。不过，如果恰当的话，也可以使用不同长度的掩码。响应于至少一个电子通信设备发送的信号而被发送到特定电子通信设备的伪随机字串（可以是数字、字母或是其它任意字符组合）能以预定形式被显示出来，其中组成伪随机字串的字符最好被显示成一个线性阵列。然后，操作特定电子通信设备的个人选取其掩码的第一位数字，本实例中为 3，并将该字符记录在伪随机字串的第三个位置上（假定从左往右）。之后，该人员选取掩码中的第二位数字，在本实例中为 9，并将该字符记录在伪随机字串的第九个位置上，依此类推再记录掩码中的数字 2 和 8。从伪随机字串中选出的字符形成了易失性识别码，该易失性识别码随后被输入至少一个电子通信设备，并被发送到电子计算机进行验证。另外，该易失性识别码也可以通过特定电子通信设备被发送到电子计算机。如果电子计算机接收的易失性识别码与电子计算机通过将掩码应用于伪随机字串而计算出来的一个预期的识别码相对应，则一个肯定的识别结果将被产生。这种机制的主要安全特征在于，掩码从未在电子计算机、特定电子通信设备或是至少一个电子通信设备之间被传送，由此防止了未授权第三方的截取。其辅助安全特征在于，人员必须拥有他或她自己的特定电子通信设备，因为电子计算机只向该设备发送伪随机字串。

对于其它的安全性来说，在易失性识别码被发送到电子计算机进行验证并且被发现与电子计算机生成的易失性识别码相互匹配之后，电子

计算机可以向特定电子通信设备发送一个消息，要求个人确认识别是正确的。只有当个人从特定电子通信设备向电子计算机发送一个确认消息以对该消息做出肯定的应答时，验证过程才最终结束。

在本发明的某些实施例中，对操作特定电子通信设备的人员来说，没有必要查看伪随机字串以及手动将掩码应用于该字串。取而代之的是，可以在特定电子通信设备的存储器中配备一个计算机程序，该程序能使个人在被提示的时候输入他或她自己的掩码，然后自动将掩码应用于伪随机字串，并返回恰当的易失性识别码，从而将该易失性识别码输入特定电子通信设备或是至少一个电子通信设备。

在另一个改进中，伪随机字串中至少一个位置可被选择以用于包含一个代表预定参数或是条件的字符。比较有利的是，该字符的位置和它所代表的意义仅仅为电子计算机和操作特定电子通信设备的个人所知。例如，在电子计算机由银行操作并且永久识别码是个人银行账号的情况下，伪随机字串中的一个位置，假设是第七位，该位置可被选择用于代表个人银行账户的余额，例如0表示资金为零，9表示余额超过1000英镑，数字1到8表示其间呈线性比例的余额。另外，为了实现更好的安全性，伪随机字串中至少有一个位置可被选择用于包含一个标记字符，该字符假定数字1到5中的任意一个表示低于500英镑的余额，而数字6到9则代表余额超过500英镑。很明显，其它许多代表性模式也可被采用以用来传送伪随机字串中的信息。由于伪随机字串中至少一个代表性字符的位置和意义最好能由个人选择，而不是遵循一种可能被非授权第三方得知的固定格式，因此，在传送过程中，要想提取伪随机字串中的有意义的信息，那将是非常困难的。此外，在接收到伪随机字串之后，可以要求个人识别至少一个代表性字符的位置和/或意义，由此在识别处理中提供了一个附加的安全层。

很明显，在上文描述的实施例中，伪随机字串必须达到至少十个字符的长度，因为由数字0到9组成的掩码要求伪随机字串中至少有十个位置是有用的。然而，普通技术人员可以了解，通过选择恰当的编码模式，不同的掩码和字串长度可以根据需要而被选择。需要强调的是，电子计算机响应于一个来自至少一个电子通信设备的识别请求而给出伪随

机字串，对每个请求来说，伪随机字串各不相同，因此，要想对一连串有可能被截取的伪随机字串和易失性识别码的给定掩码加以确定，这将是极为困难的。实际上，在特定电子通信设备独立于至少一个通信设备的实施例中，例如它们分别是移动电话和 EFTPOS 终端，伪随机字串和易失性识别码永远不会沿着相同路由（例如一个指定的临时电话连接）发送。在特定电子通信设备与至少一个电子通信设备是同一设备的实施例中，例如适于安全连接到电子计算机的远程计算机终端，伪随机字串可以沿着相同路由发送，但是不会在同一时间发送。在以后的实施例中，可以只对一个用于登录到电子计算机的初始请求加以考虑，如果该请求从关联个人的预定电话号码经由直接调制解调器链路发出，那么伪随机字串将沿着该调制解调器链路回送到远程终端，易失性识别码也经由相同的直接调制解调器连接传送到电子计算机。

在一个特别优选的实施例中，电子计算机由借记卡或信用卡的发卡方操作，特定通信设备是一个移动电话，至少一个电子通信设备是一个由零售商操作的 EFTPOS 终端，永久识别码是个人借记卡或信用卡账号，掩码是一个如上所述的四位数字，用于实现电子计算机和特定电子通信设备之间电子通信的识别码是一个移动电话的电话号码。需要理解的是，借记卡或信用卡的发卡方可以是一个银行，它发行能以个人当前账户资金来购买物品的标准借记卡，也发行能以信用账户来购买物品的信用卡，发卡方还可以是一个向用户发行专用借记卡的专家服务提供商，在这种情况下，用户必须准备资金，根据需要将其过户到服务提供商，从而保持与其专用借记卡账户关联的最小正平衡。

当个人首次从发卡方申请一个账户时，他或她将被分配一个账号和一张卡，卡上以通常方式记有持卡人的账号和姓名，例如将个人可读的标记印在卡上并在卡背面的磁条上提供机器可读的数据。个人必须向发卡方提供普通资料，例如姓名和家庭住址，以及他或她的移动电话号码。发卡方还有必要提供掩码或者就掩码与个人达成一致。掩码最好与卡分开发行，例如通过单独的邮政递送，并且掩码永远不与账号和/或电话号码一起传送。当个人希望使用借记卡或信用卡购买物品时，他或她把卡交给零售商。零售商通过 EFTPOS 终端刷卡，该终端然后与发卡方操作

的一台主机接通。卡/账户号以及包含购买价格的交易资料经由调制解调器链路发送到主机。然后，主机将卡/账户代码与个人的移动电话号码相关联，如果账户中有足以支付预期购买的资金，那么主机产生一个伪随机字串，该字串在蜂窝电信链路上经由例如 SMS 消息发送到移动电话。如前文所述，个人将掩码应用于伪随机字串，然后把由此产生的易失性识别码交给零售商。接下来，零售商将该易失性识别码输入 EFTPOS 终端，然后，该终端把这个数据返回至主机。在主机中，该数据被与个人的账户资料相关联，并与主机中产生并临时保存的一个易失性识别码相比较，该临时保存的识别码是通过将掩码应用于与个人无关的伪随机字串而产生的。如果这两个易失性识别码匹配，那么主机将一个确认信息发送到 EFTPOS 终端以授权交易，然后，支付购买所需要的资金被自动过户到零售商，并从个人卡的账户中记入借方。

在个人账户上的资金不足以支付购买所需要的费用的情况下，主机将向 EFT 终端发出一个交易未被批准的信号，并且可以向移动电话发送一个建议个人向账户中添加资金的消息。如果发现易失性识别码不匹配的情况下，主机可以向 EFTPOS 终端发送一个信息，以便通知零售商，然后零售商可以要求个人检查正确的易失性识别码已被生成，并提供正确的易失性识别码以便传送到主机。如果个人给出错误易失码的次数超出了预定次数，例如三次，那么主机可以因为怀疑盗用而临时中止个人的账户。然后，在账户被重新激活和/或发行新账号及新卡之前，个人必须携带其身份的适当证明来向发卡方提出申请。

在某些实施例中，个人可以通过他或她的移动电话而与中心计算机直接通信。这么做是有可能的，因为移动电话的传输中包含了移动电话的电话号码资料，并且主机能够将电话号码与卡的账号相关联。由此可以提供的一个有用特征，即，在信用卡或借记卡乃至移动电话被盗的情况下，可以激活一个紧急账户锁定。这种锁定可以通过向主机发送一个预定的锁定码来激活，例如 9999。作为替换或是附加，锁定码也可以用掩码格式来发布，这在个人遭到抢劫或是被用暴力威胁，以至于要交出其卡号、电话号码以及掩码的情况下是非常有用的。

还有一个更为有用的安全特征可以被提供，其中，在易失性识别码

发送到电子计算机进行验证并被发现它与电子计算机产生的易失性识别码相匹配之后，电子计算机可以向移动电话发送一个消息，请求个人确认该交易是被认可的。这个消息可以采用 SMS 或语音邮件形式发送，并且可以包含交易资料。只有当个人用移动电话向电子计算机发送一个确认消息以对电子计算机发送的消息做出肯定应答的时候，交易才最终得到授权。

根据本发明这个实施例所述的信用卡或借记卡也可被用于在互联网上进行安全采购。在这种情况下，至少一个电子通信设备可以是互联网零售商操作的计算机服务器。当个人希望进行安全采购时，他或她借助电子邮件或是通过零售商网站向服务器提交账号，然后如先前那样，服务器将账户资料以及采购资料发送到发卡方操作的主机。之后，包含伪随机字串的 SMS 消息被发送到个人的移动电话，随后，个人产生一个易失性识别码并把它提交给零售商服务器，在许可交易和放出资金之前，该易失性识别码被从零售商服务器传送到主机进行验证。

个人在发卡方也可以具有不止一个账户，并且由此可以选择或被分配以一个以上的掩码，每个账户都有一个掩码。作为替换或是附加，每个账户可以被分配以一个以上的掩码，主机可以通过伪随机字串的一个或多个字符来指示它期待个人把从多个预定的掩码中选出的某个掩码应用于伪随机字串，并由此提供一个附加级别的安全性。

可以预见，本发明并不局限于信用卡或借记卡交易，它提供了一种在很多情况下进行识别的安全方法和系统。举例来说，可以通过提供一台中心计算机来控制对建筑物或交通工具的访问，该计算机拥有授权进入建筑物或交通工具的所有人员的资料，并且可以为每个授权进入建筑物或交通工具的人配备一张条卡，该条卡带有一个唯一识别码或磁编码格式的代码。在建筑物或交通工具的入口处可以提供连接到读卡器和电子键盘的电子锁，该读卡器和键盘能与中心计算机通信。当授权用户希望进入建筑物或交通工具时，他或她通过读卡器刷卡，该读卡器然后将唯一识别号或编码发送到中心计算机。中心计算机把唯一识别号或编码与个人的个人资料（其中包括预定掩码）关联起来，然后中心计算机把伪随机字串发送到键盘，以便在其上所具有的显示器中显示。然后个人

必须把他或她的掩码应用于伪随机字串，并将由此产生的易失性识别码输入键盘，之后，键盘将易失性识别码发送到中心计算机，以便如前所述，与计算机中产生的易失性识别码相比较。如果这两个易失性识别码匹配，那么中心服务器发出一个信号解开电子锁。这种系统所提供的一个显著的优点在于，它比通过键入预定编码来操作的现有电子锁更为先进，因为在个人每次进入建筑物或是交通工具的时候，他或她都必须输入一个不同的易失性识别码。这意味着潜在的窃贼或其他人无法通过观察被授权的个人键入入口代码并随后输入相同的入口代码来进入建筑物或交通工具。

此外，没有必要为每个被允许进入建筑物或交通工具的人员提供一张条卡。取而代之的是，每个人都配备一个唯一并且可存储的永久识别号或识别码，在需要进入建筑物或是交通工具的时候，该永久识别号或识别码可以通过电子键盘输入。然后，唯一永久识别号或识别码在中心计算机中与恰当的掩码相关联，并且一个伪随机字串被发送到电子键盘，以便如前文所述显示在电子键盘的显示器上。

可以预见，在以上实施例中，电子键盘和可选的读卡器形成了至少一个电子通信设备以及特定电子通信设备。对附加的安全性来说，虽然包含了额外的不便之处，但是准许进入建筑物或交通工具的个人可以拥有作为特定电子通信设备的移动电话，伪随机字串被发送到移动电话而不是被发送到电子键盘的显示器上。

对于本发明的方法和系统来说，其可选的应用包括任何在电子通信环境中需要个人安全识别的情况。例如，该系统和方法可用于保护远程登录计算机，并且用于保护普通电信（例如企业对企业的电子商务交易、空中交通管制通信等等），该系统和方法还可以被应用于交通工具的固定器和/或报警器上，由此交通工具的授权用户必需将一个掩码应用于伪随机字串，以便解除固定器或报警器。

本发明的另一个用途是充当一个安全的检票系统。旅行车票、音乐会入场券、电影票和戏票、体育比赛门票等等的供应商可以发行“虚拟”门票，该门票是以一个永久用户识别码和一个从主机传送到特定电子通信设备的伪随机字串作为形式。一旦到达集合地点或是应检票员的要求，

拥有该“虚拟”门票的个人需要将其掩码应用于伪随机字串并将由此生成的虚拟识别码连同永久用户识别码一起提供给检票员。检票员可以配备一个电子通信设备，借助于此设备，该信息被回送到主机进行验证，如果个人被认定是一个许可的持票人，那么主机向电子通信设备发送一个确认信号。

本发明还可被用于承运包裹的车站或是邮件库房，例如邮局、目录商店或是仓库等等，人们前往那些地方领取包裹、邮件或其它物品，在移交包裹、邮件或其他物品之前，绝对有必要对个人进行识别。领取物品的个人会被分配一个伪随机字串，在收取的时候，他将被要求提供一个易失性识别码，该识别码是通过将其掩码应用于伪随机字串而产生的。

根据本发明的第三个方面，它提供了一种身份验证安全交易处理系统，该系统包括：

i）一台计算机主机，它用于存储与用户关联的用户码，为交易提供一个伪随机安全字串，其中所述主机通过将所述用户码应用于所述伪随机安全字串来确定一个一次性交易码；

ii）至少一个电子设备，该设备通过接收并显示所述伪随机安全字串来与管理所述交易的所述主机进行电子通信，并且接收一个用户交易输入码，其中所述用户交易输入码是通过将所述用户码应用于显示在所述至少一个电子设备上的所述伪随机安全字串来确定的，所述用户交易输入码被发送到所述主机；其中：

iii）所述计算机主机证实所述用户输入码与所述一次性交易码的匹配。

用户通过将他或她的用户码应用于显示在电子设备上的伪随机安全字串来确定交易输入码。用户把交易输入码输入到显示出伪随机安全字串的电子设备中或是与计算机主机通信的设备中。所输入的用户交易码被发送到主机，以便用一次性交易码来验证。伪随机安全字串可被显示出来，并且用户输入的交易码可以被输入到具有包括以下设备在内的任何组合形式的设备中，这些设备包括销售点资金电子过户（EFT/POS）设备、与用户关联的无线设备、经由互联网与主机相连的计算机或是任何能够与计算机主机进行电子通信的设备。此外，计算机主机可以传送

一次性交易码，以便显示在电子设备上，通过与计算机主机以及用户计算机或设备相连的商家计算机或网站，系统可被用于完成与商家的交易。该系统可以用于向数据库或账户信息提供安全的或规定的访问。

根据本发明的第四个方面，它提供了一种用于验证身份以便实施安全交易的方法，该方法包括以下步骤：

i）存储涉及与计算机主机关联的用户 PIN 的信息；

ii）由所述计算机主机产生一个伪随机安全字串；

iii）通过将所述用户 PIN 应用于所述伪随机安全字串来确定一个交易码；

iv）将所述伪随机安全字串传送到至少一个电子设备；

v）在所述至少一个电子设备上显示所述伪随机安全字串，以便所述用户通过将所述用户码应用于所述伪随机安全字串来确定一个用户交易输入码；

vi）在所述至少一个电子设备上输入所述用户交易输入码；

vii）将所述用户交易输入码从所述至少一个电子设备发送到所述计算机主机；以及

viii）所述计算机主机确定所述交易码是否与所述用户交易输入码匹配。

电子设备显示出伪随机安全字串，从而使用户可以通过将其用户码应用于伪随机安全字串来确定一个用户交易输入码。该用户在一个与主机进行电子通信的相同或不同电子设备上输入交易输入码。用户输入的交易码被传送到计算机主机，以用于验证计算机主机确定的交易码与用户输入的交易输入码相互匹配。根据本发明这个方面所述的方法完善了这个交易，当主机确定的交易码与用户输入的交易输入码相匹配时，该方法允许对数据库或账户信息进行访问。

根据本发明的第五个方面，它提供了一种安全的用户码输入界面系统，该系统包括：

i）一个安全用户代码输入界面，用于在电子设备上输入用户码，其中所述电子设备具有一个显示器；其中所述安全用户代码输入界面包含至少一个发光显示，用于由所述用户输入所述用户代码中的至少一位数

字；其中所述发光显示照明或加亮所述发光显示中的至少一位显示数字，并且，当符合所述用户码中至少一位数字的所述至少一位显示数字在所述发光显示上被照明或加亮的时候，所述用户将在应答的时间上使用输入设备做出一个应答，以输入所述用户代码中至少一位数字；并且其中

ii）一个随机的连续时间被添加到所述应答时间中，用以延长所述至少一个发光显示。

所述用户码输入界面保存并运行于一个具有显示器的电子设备上。在该显示器上可以看到上述安全的用户码输入界面，其中包含至少一个发光显示，用以使用户在界面的每个循环中输入一位用户码。该界面的发光显示照明或加亮界面上的至少一个显示数字，当被照明或加亮的数字与用户代码中将被输入的那个数字相匹配时，用户点击辅助键盘或鼠标上的任意按键或是接触触摸显示屏上的任意区域。当用户敲击按键时，一个随机的连续时间将被添加，这样，发光显示将保持激活，由此与输入的数字相关的信息就无法被确定。该安全用户界面为用户代码中的每一个数字都包含一个循环。

根据本发明的第六个方面，它提供了一种身份验证安全交易系统，该系统包括：

i）一台计算机主机，用于保存一个与用户关联的用户代码；

ii）一个电子设备，它与所述计算机主机进行电子通信，其中所述电子设备具有一个显示器和一个用户输入设备；以及

iii）一个安全用户代码输入界面，它在所述至少一个电子设备的所述显示器上可视，用于输入所述用户代码，其中所述安全用户代码输入界面包含至少一个具有发光显示的循环，用于输入所述用户码；其中，当符合所述用户代码中的所述至少一个用户码数字的显示数字在所述发光显示中被照明或是被加亮的时候，所述用户在应答时间使用所述用户输入设备做出一个响应，以输入所述用户代码中的至少一个用户码数字；

iv)其中所述至少一位用户代码数字的所述各位数字是在所述至少一个循环的各个循环中被输入的，并且一个随机的连续时间被添加到所述应答时间，用以延长所述至少一个循环的各个循环；以及

v）其中，输入的所述用户代码被发送到所述计算机主机，以便利用

保存的所述用户代码进行验证。

所述计算机主机中保存有涉及用户的信息，其中包括账户和用户代码信息。所述至少一个电子设备与计算机主机进行电子通信，并且显示用于输入用户代码的安全用户输入界面。所述至少一个电子设备具有至少一个显示器和一个用户输入设备。安全用户代码输入界面包含至少一个循环以用于用户代码的各位数字，并且包含一个用于输入用户代码的发光显示。当符合用户代码中恰当数字的显示数字被在所述界面的发光显示中照明或是加亮的时候，用户在应答时间使用一个用户输入设备来做出一个应答，以输入用户代码中的各位数字。当每个数字记录在一个循环中被输入之后，一个随机的连续时间被添加到用户响应时间中，以便延长发光显示的各个循环，这样，任何人都无法通过查看用户界面来确定哪个数字被选。

在输入完全部用户代码之后，输入的用户代码被发送到计算机主机，以便用计算机主机保存的用户码来加以验证。用户可以通过敲击键盘或鼠标上的按键来输入应答，也可以通过接触触摸显示屏上任意区域来做出应答。

为了更好的理解本发明并显示本发明是如何实现的，现在将以举例的方式并参考附图对本发明进行说明，在以下的附图中：

图 1 是本发明一个优选实施例的示意图；

图 2 是双信道模式的一个优选实施例的示意图；

图 3 是当用户与本发明所述系统进行交互时将会采取的步骤的流程图；

图 4 是本发明所述单信道模式的一个优选实施例的示意图；

图 5 是本发明所述单信道模式的一个附加实施例的示意图；

图 6 是本发明所述单信道模式的一个附加实施例的示意图；

图 7 是本发明所述单信道模式的一个附加实施例的示意图；

图 8 是一个结合本发明各个方面和特征的附加实施例的示意图；

图 9 是一个本发明所述安全数据访问系统的示意图；

图 10 是一个用于检索银行账户信息的安全系统的示意图；

图 11 是一个伪随机字串的图示;

图 12 是用户临时性或交易性修改和集中处理的示意图;

图 13a 是本发明所述用户界面的一个图形表示;

图 13b 是本发明所述用户界面的一个图形表示;

图 13c 是本发明所述用户界面的一个图形表示;

图 13d 是本发明所述用户界面的一个图形表示;

图 13e 是本发明所述用户界面的一个图形表示;

图 13f 是本发明所述用户界面的一个图形表示;

图 13g 是本发明所述用户界面的一个图形表示;

图 13h 是本发明所述用户界面的一个图形表示;

图 14 是本发明所述 PIN 安全界面的启动屏幕的图形表示;

图 15a 是 PIN 安全用户界面的第一循环的图形表示;

图 15b 是 PIN 安全用户界面的第二循环的图形表示;

图 15c 是 PIN 安全用户界面的第三循环的图形表示;

图 15d 是 PIN 安全用户界面的第四循环的图形表示;

图 15e 是用符号或字符取代数字后的 PIN 安全用户界面的图形表示;

图 16 的示意图示出了应用于以互联网为媒介的数据库访问系统之中的本发明的特征;

图 17 的示意图包含有应用于以互联网为媒介的多数据库访问之中的本发明的特征;

图 18 是一个描述经由互联网通信的本发明的各种特征和组成的示意图;

图 19 是一个描述经由互联网通信的本发明的各种特征和组成的示意图;

图 20 是一个描述经由互联网通信的本发明的各种特征和组成的示意图;

图 21 是根据本发明一个附加实施例所述的访问和数据通道的示意图;

图 22 示出了一个结合有本发明各个方面的通用服务器网关模式的示意图;

图 23 示出了一个根据本发明所述的通用集成平台的示意图。

图 1 显示了一台由信用卡或借记卡的发卡方操作的主机 1，一个拥有移动电话 3 的用户 2，以及一个 EFTPOS 终端 4。用户 2 配备一张卡（未示出），其上印有一个唯一的 16 位账号，该账号被磁性编码在卡上。在主机 1 中，这个 16 位账号被与涉及该用户的账户资料、用户在信用卡/借记卡方初始登记时选择或被分配的一个 4 位掩码、以及移动电话 3 的一个唯一的电话号码相关联起来。选择 16 位账号是为了兼容现有的信用卡/借记卡协议，选择 4 位掩码是为了兼容现有的 PIN 协议。当用户 2 希望从操作 EFTPOS 终端 4 的零售商（未示出）处购买物品时，他或她会出示卡，然后该卡被 EFTPOS 终端 4 扫描。关于一次购买的资料也被零售商输入 EFTPOS 终端 4，这些信息与账号一起通过一个调制解调器链路 5 被发送到计算机主机 1。然后，计算机主机 1 将该账号与包含移动电话 3 的电话号码的用户 2 的资料相关联，并且产生一个 13 位的伪随机字串，该伪随机字串通过 SMS 或语音邮件协议 6 的方式被发送给移动电话 3。伪随机字串的前三位并不是随机的，它们被保留以便向用户指示：接收到的 SMS 消息来自计算机主机。例如，这前三位可以是“T1：”或“T2：”等等，用于表示计算机主机 1 希望用户 2 将第一或第二掩码应用于该伪随机字串。伪随机字串中接下来的 10 位为任意 4 位掩码提供了足够的冗余度，以便如上文所述方式对其产生作用。通过为伪随机字串选择一个 13 位的字串长度，就可以保证与现有移动电话显示和 EAN13（欧洲商品编号）条形码协议的兼容性。

当移动电话 3 接收到伪随机字串后，那么如上文所述，用户必须将掩码应用于该字串，以便产生一个易失性识别码，然后，该识别码被传递（8）到零售商那里，并且被输入 EFTPOS 终端 4，以便传送到计算机主机 1。另外，该易失性识别码也可以通过移动电话 3 的方式被用户 2 返回给计算机主机 1。

当计算机主机 1 接收到易失性识别码时，它把该识别码与计算机主机 1 中通过将掩码应用于伪随机字段而产生的易失性识别码相比较，如果发现这两个掩码相同，那么计算机主机 1 向 EFTPOS 终端 4 发出一个

信号以授权购买，并且还将必要的资金过户到零售商。作为可选项，在授权资金过户之前，计算机主机 1 还可以用 SMS 或语音邮件的格式 6 来向移动电话 3 发送一条消息，该消息中最好包含交易资料，并且计算机主机 1 要求用户 2 返回一个信号 7，以便最终确认交易。此举可以为数额非常大的交易提供内心的平静（peace-of-mind），并且可以在用户卡正被盗用的情况下向用户 2 发出警告。

本发明既能以双通道模式实施，也可能以单通道模式实施，这些模式将结合图 2－10 而得到公开和说明。

双通道协议适于所有拥有 G2 移动电话的用户。交易类型可以包括：（1）销售点资金电子过户（EFT/POS）以及（2）电话定购。EFT/POS 是这样一种交易，其中用户在商家那里以正常方式购买物品，当使用读卡器刷取信用卡/借记卡时，商家将被提示索取顾客的交易确认码（TAC）或掩码。用户回忆起他或她的四位 PIN 代码，该代码用于从销售点给出的伪随机字串中确定 TAC。如果用户想要在短时间或是在移动电话接收质量较差的地方进行多次购买，那么用户可以预先选择将同一 TAC 用于单独的一天。电话定购交易基本上采用与上文相同的方法，只不过商家在被提示索取 TAC 之前会以通常方式人工地输入卡片的资料。

双通道模式的其它特征在于：顾客能够选择其它的用户友好方法来从伪随机安全字串中识别出 TAC，例如谜语界面或语音识别系统。谜语界面在制造过程中只包含对电话或寻呼机中 SIM 卡的较少修改，但是它可使用户避免自己去计算 TAC。用户可以键入他们的 PIN 并点击他们选择的一个附加键，电话或寻呼机会自动算出作为结果的 TAC，而用户甚至不用看到安全字串。这种计算完全是在内部发生的，由此确保只有 TAC 被显示出来，而 PIN 不会保留在移动电话或寻呼机中。语音识别界面可以在由语音激活的电话中实施，并且基于来源于已核准语音的简单命令“TAC！”，该界面能够计算出合适的 TAC。

当顾客申请一张被允许使用的卡片时，他也可以选择下文中将要详细讨论的一个几何图形，安全字串始终在该几何图形中被传递。顾客只需要登记屏幕上显示的他或她选择的几何图形，然后直观选择他或她的 PIN 图形，就可以确定出相应的 TAC 结果。这个显示可以通过 WAP 移

动电话、G3 移动电话、互联网站点的显示提示或是销售点上的辅助专用终端而被连接。

本发明的协议可以被"栓接"在一个现有数据库服务器上，并且至少可以在未经修改的 EFT/POS 硬件上运行，这些硬件如：（1）AMEX；（2）分离拨号的 EPOS；以及（3）VESA SVS3。此外，双通道协议可用于提高 Mondex 系统的安全性（这些系统在 POS 端已经使用了 4 位 PIN 数字）。

双请求模式可以使用标准的 G2 移动电话、G3 以及 WAP 设备来接收安全字串。如果这些设备包含一个经过修改的 SIM 卡界面以用于这个安全字串，那么该设备还可以包含一个 GUI 或是谜语界面，以便简化对 TAC 的推导过程。

图 2 示出了应用于销售点环境中的本发明的协议。图 2 显示了涉及这个交易的主要部件及步骤，并且显示了两个不同的选择。第一种选择是使用一个分离拨号的销售点资金电子过户机（EFT/POS），其中交易资料直接通过授权服务器 207 发送。第二种选择使用了商业受让方（acquirer）的网络。

在直接拨号的方案中，用户 201 从位于设备 202 的授权服务器 207 接收一个安全字串 210。在用户准备购买物品之前，该安全字串 210 存在于诸如移动电话的设备 202 上。当用户 201 准备进行购买时，在步骤 220，他或她会把自己持有的被允许使用的信用卡 204 交给商家 205，以便进行销售点资金电子过户（EFT/POS）。卡 204 照例在商家 205 的 EFT/POS 终端被刷取。用户 201 检查驻留在设备 202 上的安全字串 210，并确定出该次交易的 TAC。四位数字的 TAC 230 被用户 201 提供给商家 205。用户 201 可以口头告知 TAC，也可将其输入 POS 终端，还可以在移动设备 202 上输入代码。信用卡 204、TAC 230 以及交易金额随后将通过直接拨号网络 240 被发送到授权服务器 207。授权服务器 207 与发卡方 209 一起证实账户中具有足够资金，并且 TAC 与用户的 PIN 代码以及所给出的安全字串 210 相关联。如果账号、交易金额以及 TAC 都通过验证，那么授权服务器 207 将允许交易继续进行。

在称为商业受让方网络方案的第二种方案中，相同的初始步骤被应用。用户 201 接收一个安全字串 210，这个安全字串驻留在例如移动电话

的设备 202 上，当用户 201 准备从商家 205 那里购买一件物品时，在步骤 220 中，他或她把已经登记的信用卡或借记卡 204 交给商家 205。卡 204 在 EFT/POS 终端被刷取，并且用户 201 再次通过移动电话或设备 202 上留有的安全字串 210 来确定他或她的四位 TAC 230。在这个方案中，包含卡 200 账号以及购买金额的交易信息经由路径 250 被发送到系统（scheme）252。标准的信用卡交易资料和预先授权的 PIN 则被发送到发卡方的计算机主机服务器 209。系统 252 将卡 204 的信息和预先授权的 PIN 经由通信路径 256 发送到发卡方的计算机主机 209 上。同时，系统 252 与授权服务器 207 通信并且验证预先授权的 PIN 与用户 PIN 相关。发卡方 209 继续对交易进行处理，一旦通过验证，则允许交易继续进行。

除了上述双通道方案之外，本发明还允许采用单通道模式，利用这种模式，用户能够将本发明用于这样的交易，例如，通过互联网网站进行在线购物。在安全字串被接收并且 TAC 在相同设备上被传送的情况下，单通道模式和协议经由计算机、WAP 设备、智能卡、专有系统或是 G3 移动电话而被执行。这个协议并不需要辅助通道来实施安全交易。

单通道协议借助用户下载到其计算机、WAP 设备或 G3 移动电话上的一个 applet （一种 java 程序）而得到实现。安全字串和 TAC 只能由一个许可的服务器接收，并且经由一条 SSL 链路传送。由于商家（无论是否具有资格）只拥有用户的“用户姓名和卡的 ID”而没有相关的 TAC，因此本发明能够抵抗在其中用户并不知道与自己做生意的站点是不具有资格的“幽灵（ghost）”网站。

单通道解决方案指示用户的 ISP（Web 浏览器）只把用户姓名发送到商家，而把相关 TAC 传送到许可的服务器/数据库，从而解决了在互联网上发送相关 TAC 和安全字串时所遇到的问题。

图 3 显示了在用户注册并使用单通道模式的处理中将会采取的各个步骤。该过程始于步骤 300，在步骤 310 中，用户通过一个单通道设备接通本发明的服务器主机，该单通道设备可以是个人计算机、连接到互联网络的手持设备、蜂窝电话或无线电话、或是任何可以经由单一通信通道支持网络浏览器的设备。一旦与本发明的服务器或计算机主机接通，那么包含界面 applet 的登录网页将被发送到用户设备。在步骤 320 中，

用户被要求通过适当的输入方法来输入其用户ID以及预先授权的信用卡或借记卡代码。该用户界面可以包括屏幕上的下拉菜单或是其他各种用户友好的应用程序，用以增强用户ID和信用卡或借记卡代码的输入处理。用户ID被发送到服务器进行验证。如果服务器核实用户身份，那么服务器将使用低处理开销协议（LPO 协议）而把一个安全字串发送到客户网页，同时发送一个提示来启动Applet。该Applet根据LPO协议提取和重装TAC代码，并且启动PIN安全界面。

在步骤330中，能够使用户安全输入一个PIN或TAC的PIN安全界面被启动。LPO协议提取是使用一个自动系统识别数字（SID）和产生系统输出数字（SOD）来执行的。如在下文将要详细描述的那样，TAC代码被从安全字串中提取出并根据LPO协议重装，然后该TAC代码被发送到服务器主机进行验证。在步骤340中，Applet被终止并被破坏，所有数值都被清零，并且驻留在设备上的安全字串被清除。用户会看到一个对设备正在等待一个服务器响应进行识别的界面。在步骤350中，根据用户ID和TAC码的响应，登录到服务器受到确认或拒绝。如果通过验证，那么一个其后跟随着被请求的服务访问或交易的确认信息将被发送到客户浏览器。在步骤360中，会话或交易完成，这使得用户能够关闭会话或进程，或者，也可以使用一定长度的空闲时间来触发会话自动关闭。在步骤370中，采用单通道模式的用户信息被终止。

图4示出了本发明所述单通道模式的一个优选实施例的主要组件。用户401访问本发明的服务器407，该服务器407提供下载到用户设备403上的applet 470。用户401经由路径421下载470，该程序被保存在设备403上以作为用户applet 422。网络商家405将通过路径450访问授权服务器407，并经由路径451下载applet 470，该程序470被保存在商家站点405上以作为商家的applet 452。使用设备403的用户401经由路径430访问商家网站405，并且选择他或她希望购买的物品，这种选择是通过将物品放入购物篮406并选取适合的信用卡或借记卡407来实现的。商家站点405然后对购物篮406中的物品和涉及卡407的信息加以累计，并且使用商家的applet 452而把该信息沿路径431发送到授权服务器407。

授权服务器407启动验证处理，并且使用通信路径432通过商家applet

452将适当的信息回送给驻留于用户设备403中的用户applet 422。用户401被要求输入TAC。一旦用户输入了TAC，那么TAC将沿着路径433经由商家被送回授权服务器407以使响应生效。此外，在步骤434中，授权服务器407确认账户中具有足够资金，并且在步骤435中，授权服务器407确定出与卡407、TAC以及账户资金可用性有关的信息通过验证。授权服务器407沿路径436把一个"接受"通知发送到商家网站405，后者则将该通知通过路径437转发到用户设备403。

图5－7还涉及使用不同方面和安全协议的单通道模式。在图5中，用户501访问一个商家互联网站点505并且选择所要购买的各种物品。在结账的时候，商家网站505经由路径510向用户501要求付费。个人计算机或设备503包含一个与网站505通信的applet 522，并且还包含恰当的软件或applet 522，以便沿路径520将需要进行一次授权交易的信息告知授权服务器507。商家域名、交易金额、用户ID以及交易验证码（TAC）从用户设备503沿路径530被传送到授权服务器507。个人计算机或用户设备503上已经有用于使用户确定其TAC码的安全字串。

授权服务器507经由路径540而与商家互联网站点505进行通信，用以对卡和交易金额的信息加以确认。授权服务器507还将交易ID经由路径541并通过用户个人计算机503转发给用户501。交易ID从用户个人计算机503沿路径542转发到商家的互联网站点。授权服务器507验证出购买金额、卡片信息以及TAC是合适的，并且将卡和金额的资料沿着路径550发送到商家的互联网站点505。交易资料从商家互联网站点505通过路径560发送到发卡方509，最终发卡方509把支付费经由路径570发送到商家的互联网站点505。

图6显示的单通道模式与图5显示的单通道模式相似，只不过图6中包含了一个无线设备604，它用于从用户个人计算机603中消除安全字串。在图6显示的模式中，安全字串被省略，只有用于交易的四位TAC 620被从授权服务器607传送到用户的无线设备604。

图7是一个与图5、图6所示的单通道模式相类似的单通道模式，但其不同之处在于：一个十三位的安全字串被发送到无线设备704，而不是在上文中结合图6所描述的那样，将四位TAC从授权服务器707发送到无

线设备704。在图7所公开的模式中，当用户701从商家的互联网站点705选定将要购买的物品时，付费请求沿路径710并经由用户个人计算机703发送给用户。然后，applet 722提示用户输入TAC码，该TAC码是由用户通过从授权服务器发送到无线设备704的安全字串而确定的。applet 722沿着路径730把商家域名、交易金额、用户ID以及TAC转发给授权服务器707。授权服务器707沿着路径740证实交易，并将用户账号和金额沿着路径750转发给商家的互联网站点705。交易资料从商家的互联网站点705沿着路径760发送到发卡方709，然后，支付费从发卡方709沿着路径770转发给商家的互联网站点705。

如图2－7所示，在各种使用单通道或双通道模式的在线商务方案中，可能会存在因商家库存中没有某件物品而不能立即完成整个交易的情况。在这些情况下，商家通常在发货之后才会结束交易。然而，用户可能已经输入了他或她的TAC，并且系统想要向用户发送一个新的伪随机安全字串。

本发明通过让服务器接收付费请求和有效的TAC来克服这个障碍。商家服务器通常会在额定的一分钟时限之内将定购请求发送到授权服务器。然而，如果商家已经接收了一个涉及无现货商品的购货单，那么这个定购请求将被延迟。直到接收到商品并且商品即将发送给顾客的时候，延迟的定购请求才被发送到授权服务器。一旦接收到用户TAC和交易资料并且在一分钟期限内没有收到此次定购的商家传输，那么授权服务器将默认执行一个延期支付程序。

该延期支付程序在授权服务器保留有效TAC，并且作为一个说明用户已经定购商品的证据。然后，一个新的安全字串将被发给用户，以便在下次交易中使用。授权服务器程序将立即向用户发送一个电子邮件，用以说明他或她从商家那里所要求的商品的资料。每个星期或是在某个其他预定的时间间隔内，授权服务器将向用户提醒其定购请求。用户由此得知任何未决交易，这些交易最终将通过其账户而被清除。

当商品抵达商家仓库并且即将发货的时候，商家资料被发送到授权服务器，并且交易完成。如果这个时候用户资金不足以支付交易金额，那么交易将被拒绝，这与标准的信用卡交易一样。

图 8 描述了使用本发明特征的一个附加模式，其中用户具有一个预先授权的或是借记的账户804。用户看到一个真实的设备805，例如一个自动售货机，并且通过路径810选择物品，由此触发真实的设备805以要求支付费用。该付费请求将通过预先授权的流动账户804而被发送，这个处理是在步骤840中使用一个刷卡设备806刷取预先授权的账户804（例如信用卡或借记卡）来完成的。此外，小额付费请求还把将要请求一个TAC的消息通知给刷卡设备806。用户可以具有诸如无线电话这样的个人设备803，该设备包含一个TAC或是安全字串，由此用户可以确定TAC并将TAC 830输入刷卡设备806。用户还可以将TAC 830输入无线设备803，后者会将TAC 830无线发送到刷卡设备806或授权服务器807。交易资料从刷卡设备806沿着路径850发送到授权服务器807。授权服务器807包含涉及流动账户的信息，并且，如果通过验证，那么它将会沿着路径860通知小额付费计算机主机808以授权支付费用。然后，小额付费主机808沿着路径870把支付数额过户到上述真实的设备805。

图9描绘了一种数据控制模式，利用这个模式，本发明的部件可用于将一个安全层和预先授权添加到数据库中，以便对访问数据库加以控制。在图9中，用户901通过他或她的计算机或笔记本计算机903来访问数据库909。该访问是从授权服务器907沿着路径910请求的。一个安全字串经由路径920被从授权服务器907发送到计算机903，由此使用户确定出他或她的TAC。用户输入TAC，该TAC沿着路径930传送到授权服务器907。如果用户提供的TAC与已被用户901验证的适当PIN向匹配，则授权服务器907将允许沿着路径940来访问数据库909。

另外，该系统可以只简单地发送TAC，而不发送安全字串。然后，访问数据通过授权服务器907并经由路径950被传送到用户计算机903。此外，安全字串可以通过另外一条路径921（例如通过使用一个无线设备904）而被发送到用户901。

图10描述了一种远程银行存款余额查询模式，通过这种模式，用户可以检查账户的余额。在图10所给出的模式中，通过使用蜂窝电话、寻呼机或无线设备1004，用户1001可以要求查询银行1008中的账户余额。该用户通过路径1010被提供一个安全字串或TAC，该安全字串或TAC驻

留在无线设备1004中。用户确定他或她的TAC代码，并且向银行出纳员提交其TAC代码，或是将其输入至无线设备1004。TAC代码被发送到授权服务器1007，并由该服务器验证出TAC代码适于安全字串并且对应于用户PIN。然后，授权服务器1007沿着路径1020与银行1008通信以检索账户信息，由此为用户提供被请求的信息。

本发明的两个重要方面（即低处理开销协议和安全字串操作）在结合图2－10所描述的双通道和单通道模式中得到了应用。某些无线设备，例如web设备，它们由于自身的低处理开销，因而无法运行高级别的加密程序。本发明引入了一种低处理开销协议，该协议能使这类设备运行高度安全的交易，也可以在不使用大容量存储内核（footprint）的情况下进行下载。低处理开销协议的一个额外好处在于：在处理信息时，现有的交易数据提供服务器要快于传统的加密系统。通过同时使用多个安全字串,低处理开销协议避开了TAC与安全字串之间相互关联的可能性。在多个安全字串中，实际上只有一个字串是相关的，剩余字串只是用于隐藏该相关字串。安全字串包含相同的数字，但是它们以不同的随机顺序排列。用户applet接收多个安全字串，并且利用一个系统识别数字（SID）来识别哪一个字串相关。识别数字的系统知道哪一个安全字串是真实的并且立即清除不相关的字串，而只对正确和相关的字串加以处理。举例来说，如果识别数字的值为4，那么本发明将把第四个安全字串识别为相关的安全字串。

在交易过程中，如结合图11和12将要描述的那样，用户输入他或她的PIN，并且TAC是在无线设备、个人计算机以及EFT/POS的applet中内部算出的，或者如图11所示，一个十三位的安全字串1100被从授权服务器发送到用于识别一个行随机数字的用户设备，在这个实例中为十三（13）。安全字串1100可以始于两个字母识别前缀1101，该前缀标识出是哪一个服务器发出了安全字串1100。举例来说，在图11中，如果用户的PIN是2468并且用户将PIN代码应用于安全字串1100中的数字位置。那么用户将查看第二点、第四点、第六点和第八点上的数字，以便为该次交易确定其交易验证码或TAC。在这个例子中，数值为2468的用户PIN将产生一个数值为7693的TAC。因此，用户将会输入7693作为TAC，用以

通知授权服务器继续验证处理。

关于在被传送的保密安全字串中使TAC受到保护的方式的进一步描述将结合图12加以说明。如图12所示，用户或顾客1201具有一个已知的PIN 1202（即1234）。保存在用户设备上并从服务器1207下载的信息是十三位伪随机字串1203。在个例子中，数值为"1234"的顾客PIN在与伪字串1203相关联的时候将会指示一个数值为"6891"的TAC代码1204。当用户被要求验证TAC 1204或是将其输入以授权服务器1207证实顾客1201实际上是已被授权和注册的用户时，TAC1204可被操作并以无数种方式反转，以便在沿着通信路径到达服务器1207的传送过程中保护该代码。一种用于为顾客PIN 1202和TAC代码1204提供安全层的方法是：将TAC代码合并入多个字串中的一个十三位字串，就像先前所述的那样。

为了识别适当的字串，运行在顾客设备上的applet将通过一个系统识别数字1205来识别相关的字串。SID 1205被用于识别哪一个安全字串是相关的。该SID 1205可以用无数种方式确定，其中包括：使用用户PIN1202的某些数字或数字组合、由用户设定SID 1205以及由系统服务器设定SID 1205。在图12所示实例中，系统将SID的值设定为3。因此，九个字串中的第三个字串就是相关字串。十三（13）个数字中的九个（9）字串经由一个数据连接（例如数据流1230）被发送到用户或顾客1201的设备。该设备上的applet知道SID 1205的值并且提取出相关的字串1203。

顾客检查驻留在其设备上的相关字串1203，并且确定他或她的TAC 1204。然后，TAC 1204被编结到一个输出的相关字串中，该字串被分成八（8）个非相关字串组。输出数据流1240包含九个十三位数字的输出字串。相关输出字串的位置通过一个系统输出数字（SOD）1209而被识别，它也可以用无数种方式来确定，例如，使用或添加一定数量的用户PIN 1202或是由用户或系统服务器来选择SOD 1209。

在这个例子中，系统将系统输出数字（SOD）1209的值设置在2上。因此，TAC 1204将被合并入字串1240的数据流内九个字串中的第二个字串。TAC代码1204也可以被倒置和操作、被增加一个自动数字（即每个数字都增加1），或是采用其中PIN代码可以在传送之前得到修改的其他任何方式。在图12所示的例子中，TAC代码1204被翻转，以用于确定相

关输出字串中TAC数字的位置。例如，由于在这个实例中，TAC 1204的值为“6891”，其翻转值“1986”将规定位于第一点的是TAC码的第一位数字，位于第九点的是TAC的第二位数字，依此类推，直到TAC被并入相关的安全字串为止。

含有九个十三位字串的输出安全字串的数据流1240被发送到服务器1207，该服务器具有一个执行验证的applet。服务器1207还具有一个applet，该程序知道SOD 1209的值，并且可以识别出用于对用户PIN进行验证的相关的输出安全字串。因此，服务器1207上的applet知道用户的PIN 1202为“1234”，并且可以基于所建立的协议确定出SOD 1209的值为2，进而确定出相关字串为第二个字串。服务器1207根据用户保存的PIN来分析第二个字串，并且等待响应，以便验证该响应与来自初始字串1230的TAC 1204代码相匹配。

当接收到九个载体字串后，服务器1207知道相关的TAC载体字串的输出数字位置，并且立即清除不相关的字串，同时对正确选出的TAC载体字串进行处理。然后，服务器1207上的验证过程对正确的TAC与所给出的安全字串和用户PIN号进行比较。如果所有三个都相关，则完成授权，并且一个新的安全字串被发送到用户的applet。

尽管在这个例子中，所述数字被限制为九行十三个数字加上每行三个（3）系统数字（总计144个数字）。但是它并不意味着是对可被使用的行或数字的限制。对许多160个字符的设备来说，九行十三个数字总计144个数字是有意低于总的全球分组标准。因此，将数字长度保持在160以下将会使处理开销最小，以便顾及WAP应用和无线设备的低处理能力。此外，这个低处理开销将产生非常快的验证时间。验证过程还采用了一个过滤步骤，其后跟随的是一个单维阵列处理过程，而该过程并不是一个需要更多处理时间的密集型算术计算体系。

除了各种单和双通道模式、低处理开销协议以及使用多个安全字串的安全层以外，本发明还可以在用户界面内部提供一个安全层。图13a－13h示出了各种用户界面的例子，这些界面都可以提供给用户以用于输入用户TAC。在图13a－13h所提供的例子中，用户把他或她的个人PIN记忆成一个图案，而不是一个数字序列。举例来说，如果用户选择使用形状

1301并且出示图13e中的显示，那么他们只须记住他们创建了一个PIN，该PIN在图13c公开的形状1301的内部创建了一个小方块1303。当该显示被随机数填充时，则用户可以应用他或她所选择的设计（也就是小方块1303）。在这个实例中，来自方块1303的用户PIN将是"2389"。因此，知道PIN为"2389"并且察看了随机显示1302内部随机产生的数字，用户将会了解，数字"7538"对应于他或她的PIN数字位置。因此，用于完成交易或是输入数据库的用户TAC将是"7538"。图13a-h中所公开的用户界面仅仅是示范性的，各种显示、以及颜色和图形符号也可以被合并到用户界面中。因此，用户能够创建他或她的PIN的图形表示，而不需要记住四位PIN数字。

本发明另一个用于处理系统的用户界面的特征涉及到一个PIN安全阻碍界面的使用。任何带有键盘或是触摸界面（它可被连接到一个网络上或是能够下载数据或机器码）的设备都会需要含有一个口令或按键输入安全系统以实现完整性。一种构成该系统的方法是使用一个特洛伊木马（Trojan）程序。该程序是一个小程序，它收集键盘信息以便以后使用。还有其它程序也可以收集口令或键输入信息，然而在登录输入最后一位数字的时候，该程序会伪造一个登录失败的提示，并且在不为实际用户知晓的情况下，该程序将通过猜测最后一位数字（称为一个"嗅觉"程序）来尝试继续登录。这些技术都需要来自设备键盘或辅助键盘以及其他输入设备的实际数据。尽管数据可以通过加密或其他方式递送，并被安全的重传到设备处理单元进行的实际处理中，也可以从该处理中被重新发送，但是，如果安全系统需要输入有意义的用户数据以访问和操作安全系统，那么该数据可能被截取和转运，从而极大地降低了系统安全性。

虽然键盘或少量其他输入数据可以被重定向，或是在很少或没有用户指示或者系统性能影响的情况下被保存，但是对于具有高吞吐量输出和特定于设备的输出的图形显示来说，这种情况则不再适用。虽然有可能进行屏幕抓取或屏幕捕捉，但是由于系统资源集中，因此这很有可能会被用户发现，尤其是在处理能力相对较低的设备上。由此可以通过一个界面来提供良好的对抗性，该界面把信息提供给一个安全系统，这些信息只对那些在处在自身时间界面参数范围内的系统有意义，并且在那

些系统中，所获取的任何键盘信息都不具有外部意义。与之相似，任何可能的屏幕抓取或屏幕捕捉信息都不会危及系统的登录安全性。

当前，在计算机、PDA、2.5G或3G移动设备上输入用户名、口令或PIN代码是存在缺陷的，这是因为：（1）旁观者可能看到用户将他或她的PIN代码输入设备（称作"肩窥"）；（2）键盘有可能包含一个特洛伊木马程序，该程序记录输入的用户名、口令或PIN代码（特洛伊木马程序在未曾告知用户的情况下被下载到计算机，并且该程序可以无限期的驻留在那里）；（3）PKI验证可以证实该交易是在一台经过验证的计算机上实施的，但是它们不能有效验证计算机背后的用户；以及（4）运行微软视窗系统的计算机存在一个问题，因为视窗系统会记忆用户名、口令或者PIN代码，这将会产生一种情况，即，设备将用户的I/D保存在计算机内部。

"雷达"阻碍或本发明的PIN安全用户界面实现了一种良好的用户I/D，因为在每次交易过程中，用户都必须在场。PIN安全用户界面可以防止特洛伊木马程序，因为任何按键都可被用于输入PIN或TAC，而所述PIN或TAC则可使任何被特洛伊截获的按键信息都没有用处，就像屏幕上显示的信息一样。

此外，该用户界面是防肩窥的，因为观察屏幕或是观察按键输入并不能收集到什么信息，这使得肩窥成了一种毫无意义的行为。另外，当系统使用双通道和单通道（applet）协议时，它能够防止PIN被截取。本发明所述的协议是唯一的，因为它在每次交易时都会发送一个易失性TAC。即使截取/解密这个信息的尝试获得成功，也不会导致用户的真实PIN受到危及。

本发明的另一个特征在于，它是一个多平台系统。由于PIN安全用户界面具有低存储内核以及简单的通用用户界面，因此它可以工作在多种计算机和应用上。作为一个整体，协议和系统并不特定于某种设备，而是可以运行在诸如公用计算机的任何设备上。系统并不需要运行在一个程序历史纪录已知的可信计算机系统上。在不需要为计算机进行数字认证的情况下，用户可以在全世界任何一台计算机上进行交易。

另外，该用户界面很容易使用，因为用户无须了解协议、TAC以及

安全字串。PIN安全用户仅需将他或她的不变PIN经由PIN安全用户界面输入即可。另外，PIN安全用户界面是"搅乱"的证据，因为该界面并不将用户PIN或TAC（伪PIN）显示在屏幕上，因此也就不会受到来源于VDU的电磁辐射的影响，而这方面的内容是经由搅乱技术进行监测的一个主题。通过使用本发明的PIN安全用户界面所得到的强有力的保护允许将安全的单个PIN应用在多种具有不同安全体系的账户上，这可以通过使用一个中心PIN授权服务器来实现。即使安全字串存在于设备上也不会产生问题，因为本发明并不需要数字认证，因此，如果计算机落入不合适的人的手中，计算机存储器中也不会存在可能危及用户I/D的信息。

PIN安全用户界面包含一种将PIN代码输入计算机、ATM、PDA、2.5G或3G移动设备的独特方法。图14和15a－15e是这种PIN安全用户界面屏幕的典型实例。当用户希望进行在线交易时，PIN安全applet将激活，该程序提供如图14所示的"开始"用户界面。点击用户计算机屏幕上的任意按键，激活TAC或PIN的输入界面屏幕。该界面可以使用键盘、鼠标或触摸显示屏来激活。

如图15a－15e所示，PIN安全界面现在将开始依次显示（本实例中采用顺时针方向的方式）12个数字（从1开始，结束于12）。在这个显示循环中，当用户希望登记的数字被照亮时，用户只要按下其键盘、鼠标上的任意按键或是点击触摸显示屏上任意一点，就可以登记他或她的PIN或TAC。该PIN安全显示将会循环4次，每次用于4个PIN代码中的一位数字。

在第十二个位置上存在一个停留时间，以使用户准确地响应下一个循环的启动。当用于第一个PIN代码的第一个循环结束时，该显示将重新开始另一个循环。该循环也可通过改变照明颜色而被识别。这个处理过程被重复4次，直到所有4个数字都被输入，以便组成用户的4位PIN。

举例来说，如图15a－15d所示，如果用户的PIN是"2468"，那么在第一个循环，参见图15a，当第二个数字被照亮时，键盘应被按下。在第二个循环，当第四个数字被照亮（参见图15b）时，键盘应被按下，在第三个循环，当第六个数字被照亮时（参见图15c），键盘应被按下，在第四个循环，当第八个数字被照亮（参见图15d）时，键盘应被按下。在任一时刻，屏幕上只能看到一个显示，由此防止旁观者判定哪一个PIN正被输

入。另外，背景颜色以及所显示数字的变化可以是伪随机的。

当用户点击键盘以注册其第一位PIN TAC数字之后，一个随机的连续周期（run on period）时间将被激活。该连续处理能够防止旁观者对被注册的数字进行仔细查看。举例来说，如结合图15a所示的那样，当用户想要注册第一个数字（例如数字2）时，在数字2或第二个数字被照亮时，他们将会按下键盘上的任意按键，然而，该显示将继续照亮循环中2以后的代码或数字。在加速照亮所有数字直到结束循环之前，系统也可以只照亮被选数字之后的一部分数字，例如被选代码之后的0到4位数字。旁观者只能看到该循环在数字2、3、4、5或6被照亮之后加速，但是无法判定已经注册的是哪一个数字。在这个连续周期之后，系统可以提高循环速度以便结束循环，这样用户无须捱到整个循环时间结束，这有助于快速输入PIN。所述连续周期通常要短于从点击按键到用户开始怀疑是否已经给出一个明确选择所经过的时间。对人类的短期视觉记忆来说，这个时间最多是三秒钟。

连续周期和提高的循环速度可应用于所有4个周期和显示。处于数字照亮与循环中的变化之间的停顿时间是伪随机的，由此可以防止特洛伊木马程序通过将显示与键盘和用户计算机的时钟速度相关联来确定正被输入的数字。

如图15e所示，PIN安全用户界面还可以使用字符、字母或符号来代替显示器上的数字，这使得用户代码或PIN可以是符号或构成单词的字母的任意组合。此外，如上所述并且结合图9，本发明可被应用于利用双通道或单通道模式或协议以及PIN安全界面来实现的数据的远程访问。

通过配备一台授权服务器计算机，就可以使现有的数据库具有根据本发明所述的PIN安全界面，该计算机能够记录用户的PIN代码，提供并保存安全字串，并且能还对接收到的TAC进行关联，从而对用户的身份加以验证。

此外，PIN安全或雷达（Radar）界面可以在计算机自身处理器的内部、局域网结构的内部以及互联网上工作。在计算机自身处理器内部操作的PIN安全界面可以作为一个防黑客的屏幕保护程序，这意味着当用户首次启动他或她的计算机时，他或她将被给出这个界面。因此用户必须

输入PIN，如果用户决定短时间离开计算机，对罪犯来说，这时有机会使用他或她的计算机，那么用户可以按下一个功能键，该功能键将会激活PIN安全界面。当用户返回到他或她的计算机时，他或她只要点击鼠标或是任意按键并且通过该PIN安全界面输入PIN即可。

此外，如果一个用户未能在4个扫描循环中的任何一个循环内输入其PIN数字，那么本发明将允许在任意扫描中输入PIN数字（假如它们处于正确的顺序）。这意味着不需要按下"复位"按键，除非用户有意犯错误。

使用本发明所述安全特性、措施、协议、界面以及外层的其它模式将结合图16-23而得到讨论。

如图16所示，授权服务器1607直接连接到一个客户的主机网关服务器1609。该主机网关服务器1609是数据库1611与互联网1613之间的连接装置，它被放置于围绕在主机数据库1611四周的防火墙1615的外部（这样可以确保任何黑客活动都无法在数据库1611内部发生）。远程数据访问结构也可以连同用户1601和用户设备1604一起来使用PIN安全界面1623。系统还可以使用一个备份服务器或数据库1630。

授权服务器1607可以被配置成充当双通道或单通道系统。其结构使得主机网关服务器1609能够经由本发明或是现有访问程序来访问数据库1611。这意味着在安装完成之后，可以在不影响原始配置的情况下进行允许访问测试。

图17显示了如何利用一个PIN代码从一个用户1701访问多个客户机1740、1750。此举是通过安装一个中心PIN授权服务器1707来实现的，该服务器把接收到的TAC与从任意被激活的客户机1740、1750给出的安全字串结合在一起。

PIN安全界面可以通过各种方式得到应用，包括双通道和单通道：瘦（thin）客户机和多个单通道Applet实施例。在图18所示的双通道应用中，用户的TAC通过PIN安全界面1823而被输入，并且通过互联网1813被直接发送给授权服务器1807。在双通道应用中，没有安全字串被发送给用户计算机1822，取而代之的是，安全字串经由SMS被发送到移动设备1804。

如图18所示，安全字串被从授权计算机1807发送到用户移动设备1804。用户通过PIN安全界面1823输入TAC，授权服务器1807通过互联网

1813接收TAC。

在单通道瘦客户机的应用中，如图19所示，PIN安全界面的applet 1923驻留在授权服务器1907上。用户1901从任意计算机1922远程访问这个applet 1923，并且不需要通过预先下载的任何程序形成而对计算机1922进行"设置"。如图19所示，用户经由互联网1913访问授权服务器1907和applet 1923。用户1901输入他或她的PIN，该PIN在源头或授权服务器1907处被相关。

在单通道Applet应用中，如图20所示，PIN安全界面的applet 2023驻留在用户计算机2022上。该applet 2023只需下载一次，并且会在注册过程中被自动发送到用户计算机2022。PIN安全界面被特别设计成具有极小的存储器内核，此举使下载和使用过程都很快。

如图20所示，用户经由互联网2013访问授权服务器2007。用户2001输入他或她的PIN，applet 2023将该PIN转换成一个TAC（该转换通过利用驻留于applet 2023中的易失性安全字串而被自动完成），然后，该TAC经由互联网2013被发出，以便在授权服务器2007那里进行关联。

图21显示了一个典型的数据访问应用，其中授权服务器2107已被安装在一个访问数据库2111的网关服务器2109上。图21假设用户2101已经在系统中进行了注册，并且其计算机上装有PIN安全界面的applet 2123。要从数据库2111中访问信息，授权服务器2107将一个新的安全字串经由互联网2113或无线链路2151发送到用户计算机或G2移动电话。该安全字串2151驻留在设备2104上，直到用户2101希望访问数据库2111为止。

用户2101将他或她的易失性TAC发送至授权服务器2107用以确认他/她的身份。在双通道方案中，用户从G2移动设备2104获取他或她的TAC，这个获取可以经由可视提取（将其PIN用作一个序列发生器）、智能PIN或是SIMM来完成，其中用户2101将他或她的PIN输入设备2104，并且相关的TAC数字被显示在设备2104的屏幕上。然后，TAC被输入用户计算机（未示出）。在单通道方案中，用户只将他或她的PIN输入PIN安全界面2123。之后，该PIN在applet 2123内部被转换成一个TAC，并且经由路径2120被发送给授权服务器2107。

只有当用户的身份通过将接收到的TAC与用户PIN相关联而被肯定

地证实并且先前发出的安全字串是通过网关服务器2109并经由路径2130初始化的数据请求2130时，被请求的数据才可以经由路径2140被传递到用户计算机。

如果安全字串的递送和TAC的提取是在一个第二设备（例如通过双通道协议）上实施的，则不需要PIN安全界面。用户可以使用G2移动电话来接收一个安全字串，并且提取独立于数据存取计算机的TAC。这意味着TAC可以被输入数据存取计算机，而不需要经过PIN安全界面，因为对于肩窥、特洛伊木马程序、搅乱技术以及在线用户身份窃取来说，TAC是具有内在安全性的。

图22显示了一个结合本发明所述各个方面的通用服务器/网关模式。该通用安全服务器模式还可以引入UPS（不间断电源）、二重冗余、磁盘镜像、Linux的WEB服务器2245以及内部防火墙2215、PIN安全applet 2223、用户数据库2207以及一个内部维护的任何报告功能2211。

图23示出了通用集成平台，其中显示了防火墙2315内部的授权服务器2307。该授权服务器2307被连接到一个网络服务器2317和一个主机数据库2311。主机数据库2311也可以位于自身防火墙2316的内部。

另外，授权过程通过一个响应而不是一个识别账户及其参数来对用户加以识别，其中该参数能够防止由在线欺诈性保证的滥用所产生的所谓的“友好欺诈”（Friendly Fraud）。一个附加的好处在于，对于数据库文件存取来说，还存在着一个审计追踪过程。

本文中所述的计算机指得是任意的个人计算机、ATM、PDA、G2.5移动设备、G3移动设备，或是任何具有CPU的设备。本文中所述的交易指得是任何财务交易、远程数据存取程序，或是任何用户与系统之间的接口交易。各种用户界面和显示上的数字只是示范性的，并且字符、字母、颜色等可以被独立使用，也可以被结合在一起使用，但它们仍然包含在本发明的意图范围内。

虽然在这里已经通过实例而对本发明的优选实施例和各种备选实施例进行了详细描述和公开，但是对本领域技术人员来说，很明显，在不脱离本发明范围的情况下，可以对本发明进行各种形式和细节上的改动。本发明的范围仅由以下权利要求限定。

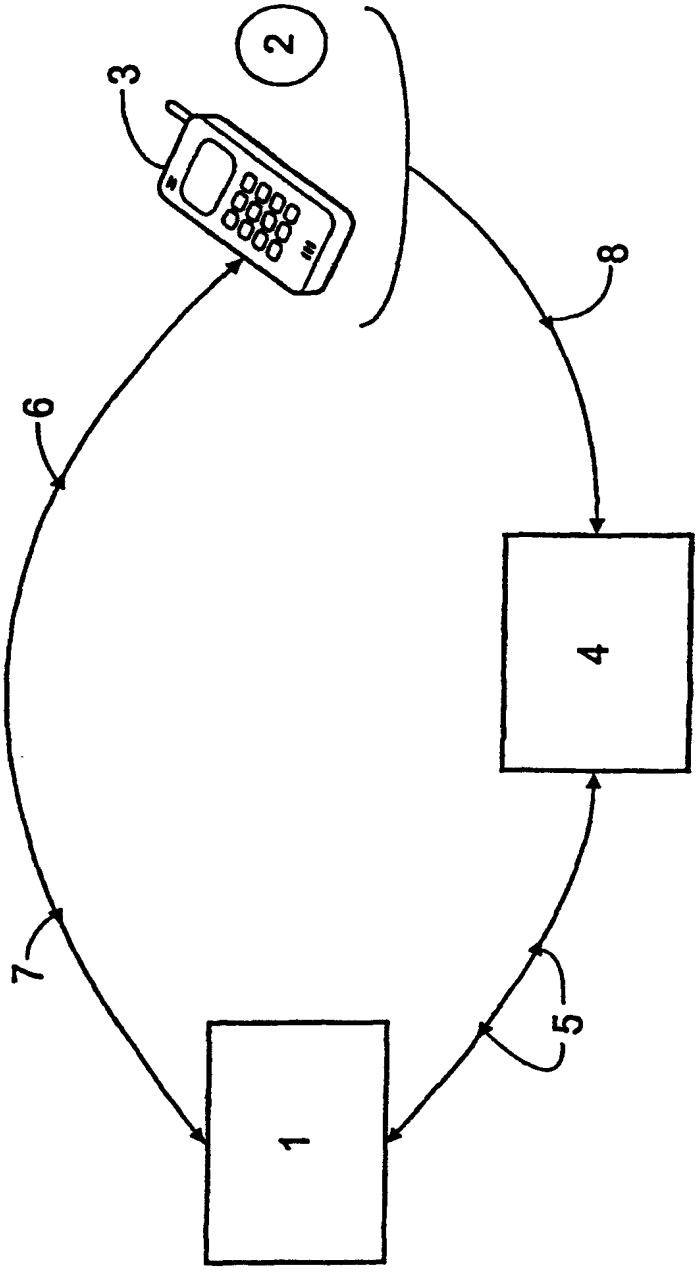


图1

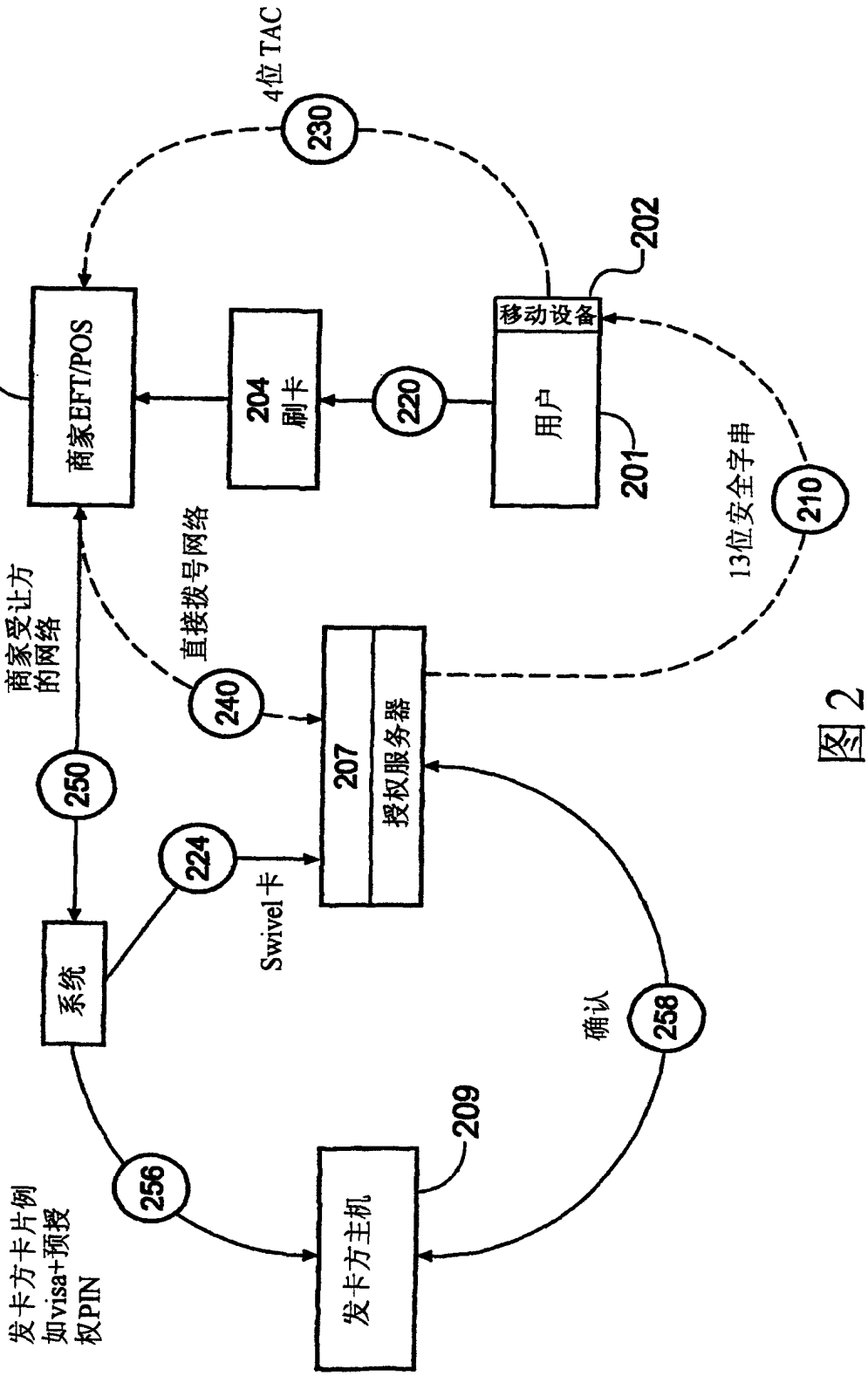


图 2

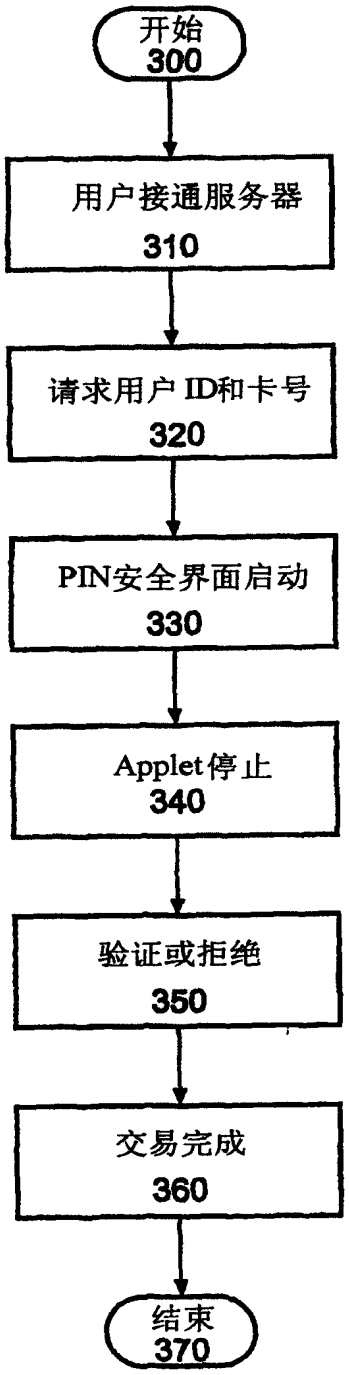


图3

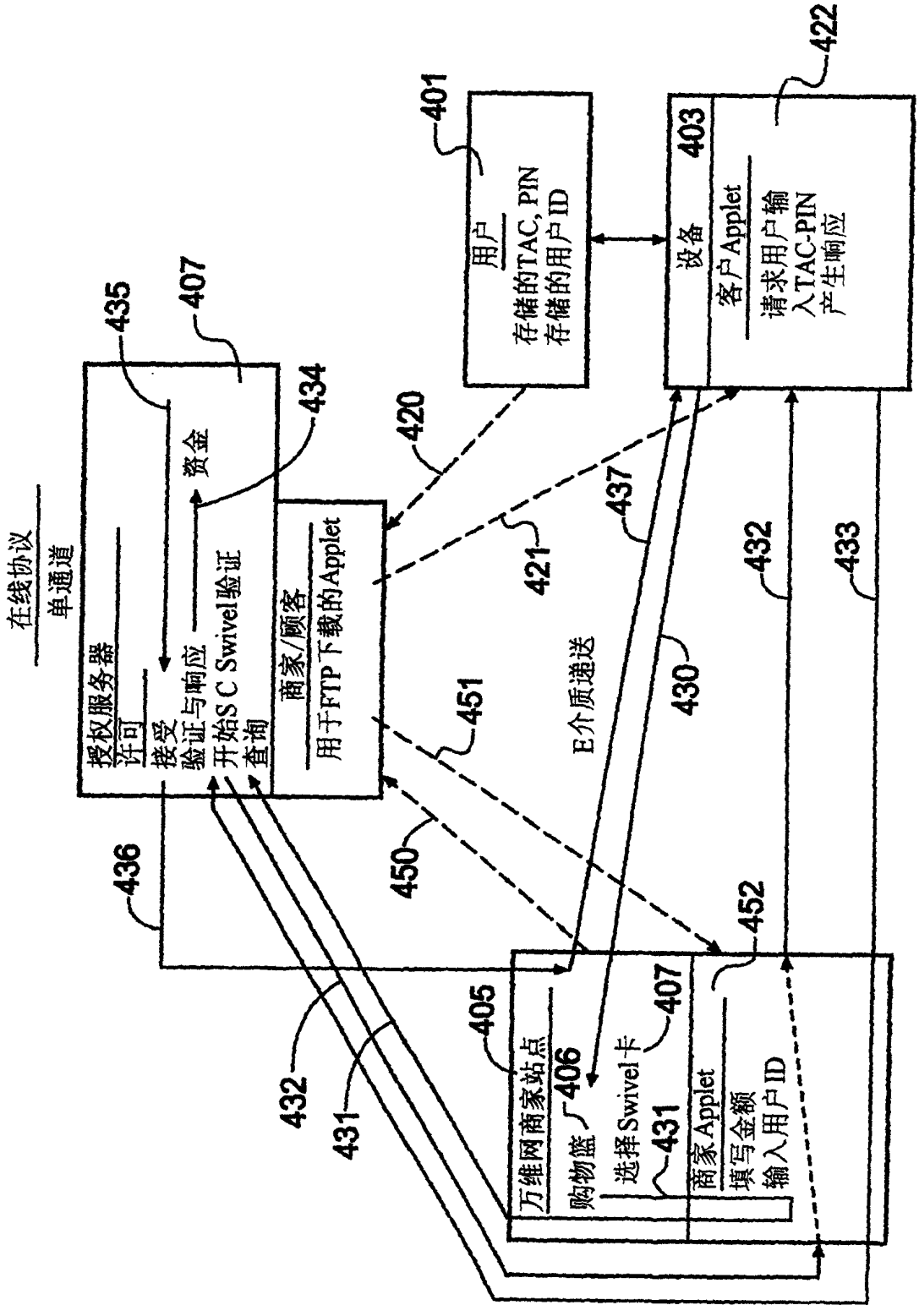

在线协议
单通道
授权服务器
许可
接受
验证与响应
开始SC Swivel验证
查询
资金
商家/顾客
用于FTP下载的Applet
用户
存储的TAC, PIN
存储的用户ID
设备
客户Applet
请求用户输入TAC-PIN
产生响应
E介质递送
万维网商家站点
购物篮
选择Swivel卡
商家Applet
填写金额
输入用户ID
401
403
405
406
407
420
421
422
430
431
432
433
434
435
436
437
450
451
452

图4

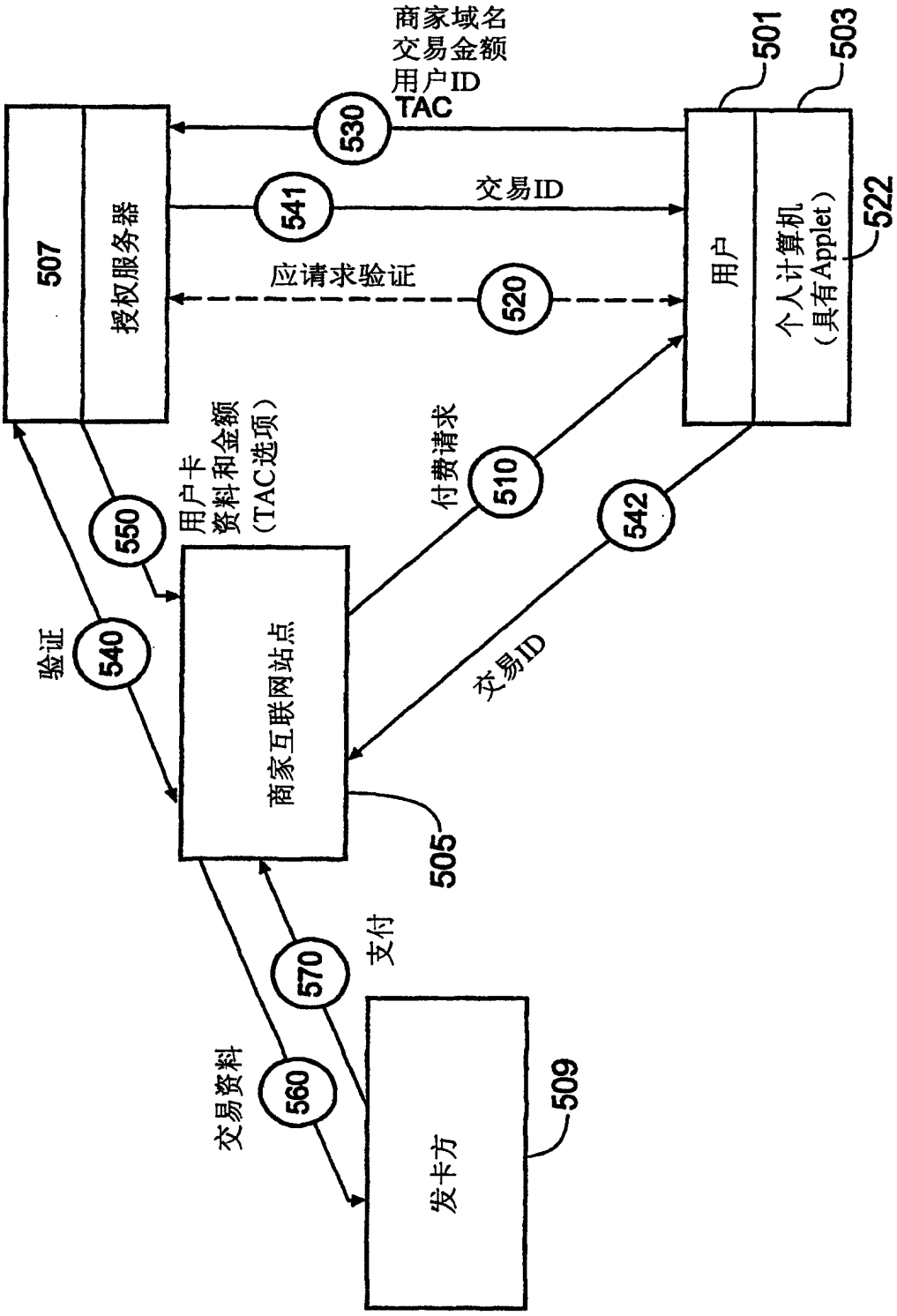


图5

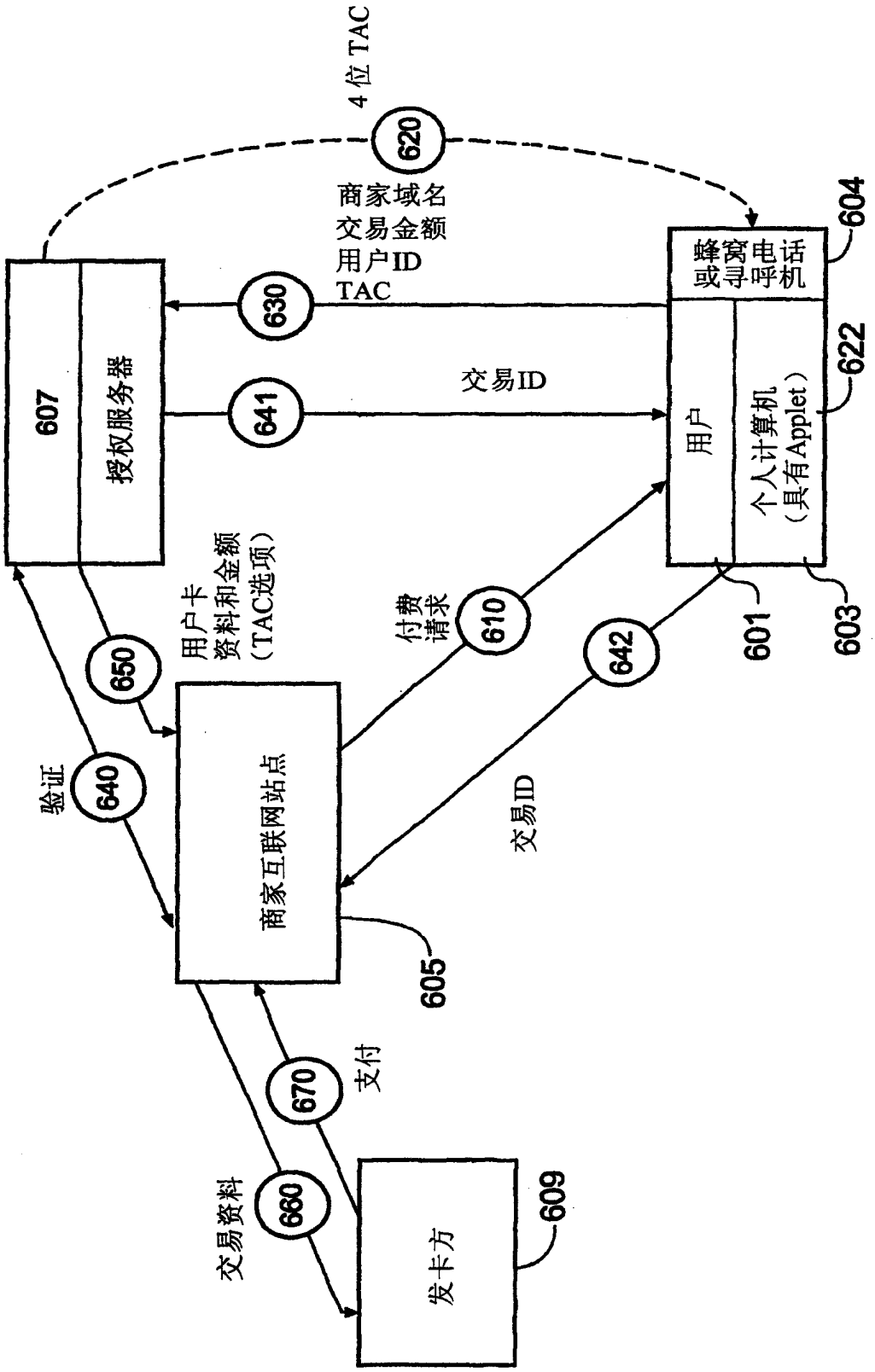


图6

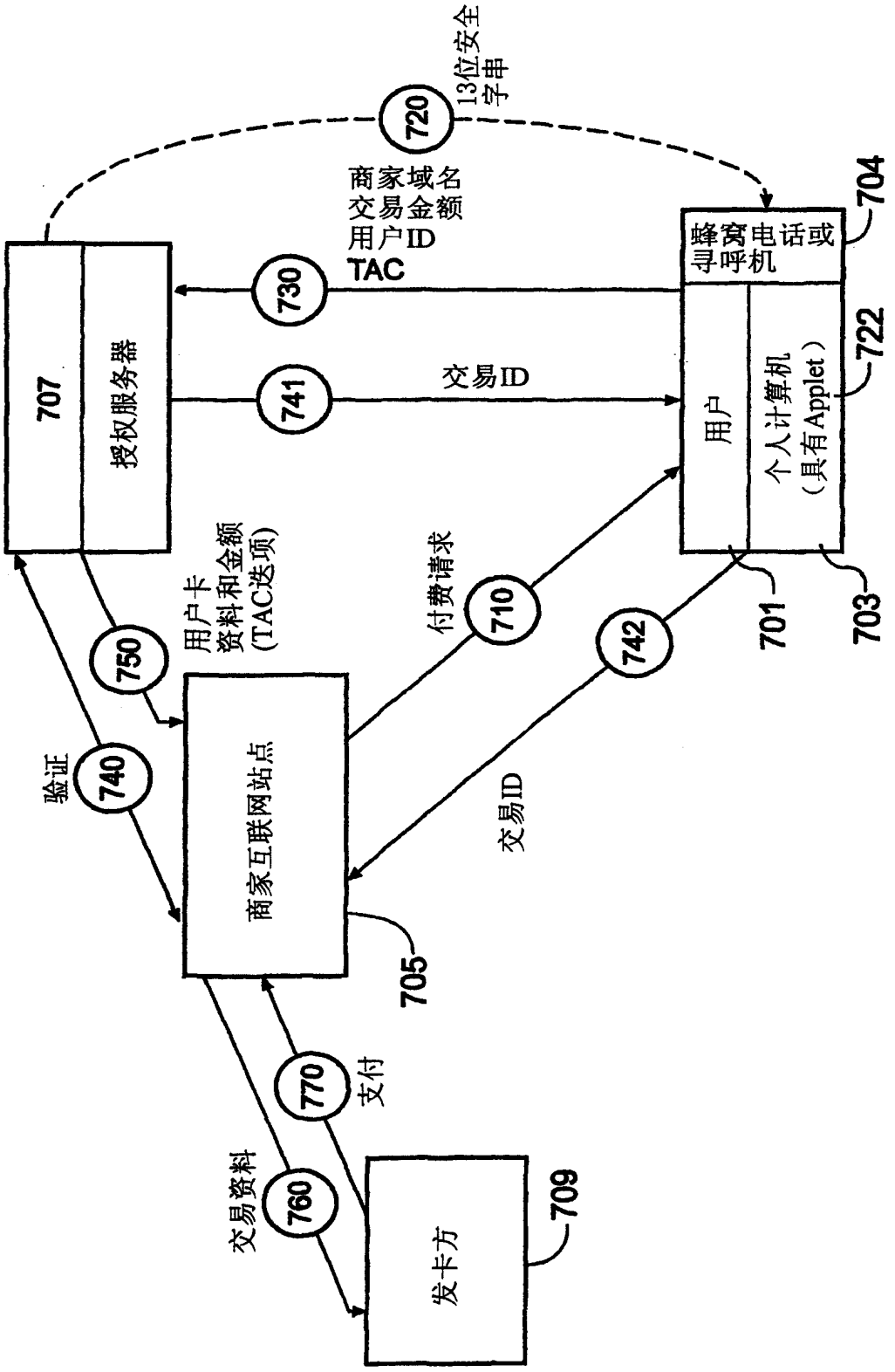

720
13位安全字串
商家域名
交易金额
用户ID
TAC
730
704
蜂窝电话或寻呼机
707
授权服务器
741
交易ID
722
用户
个人计算机（具有Applet）
用户卡资料和金额(TAC选项)
750
付费请求
710
742
701
703
验证
740
商家互联网站点
交易ID
705
770
支付
交易资料
760
709
发卡方

图 7

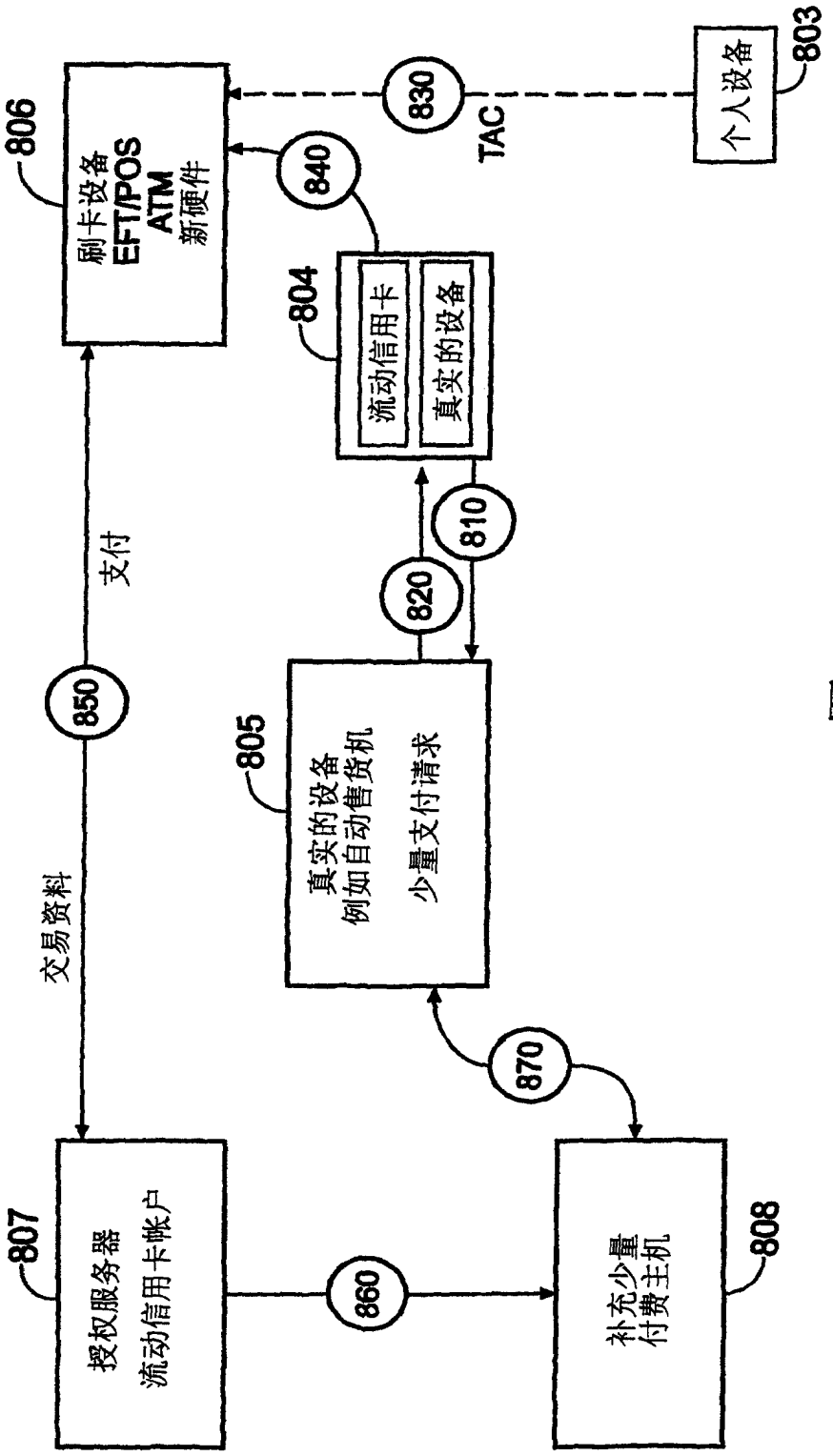


图 8

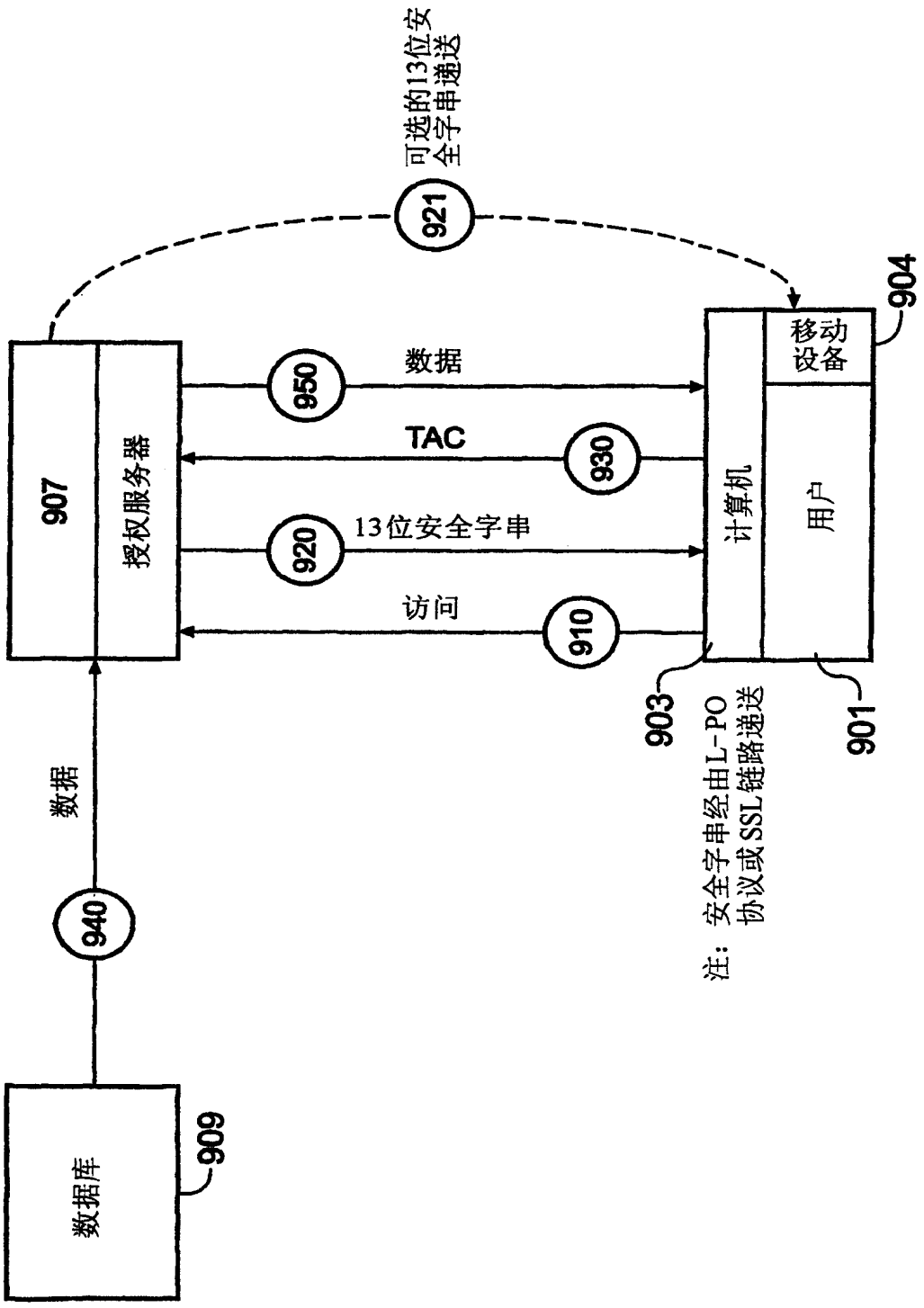

可选的13位安全字串递送
921
904
移动设备
907
授权服务器
950
数据
TAC
930
920
13位安全字串
计算机
用户
访问
910
903
901
注：安全字串经由L-PO协议或SSL链路递送
数据
940
数据库
909

图 9

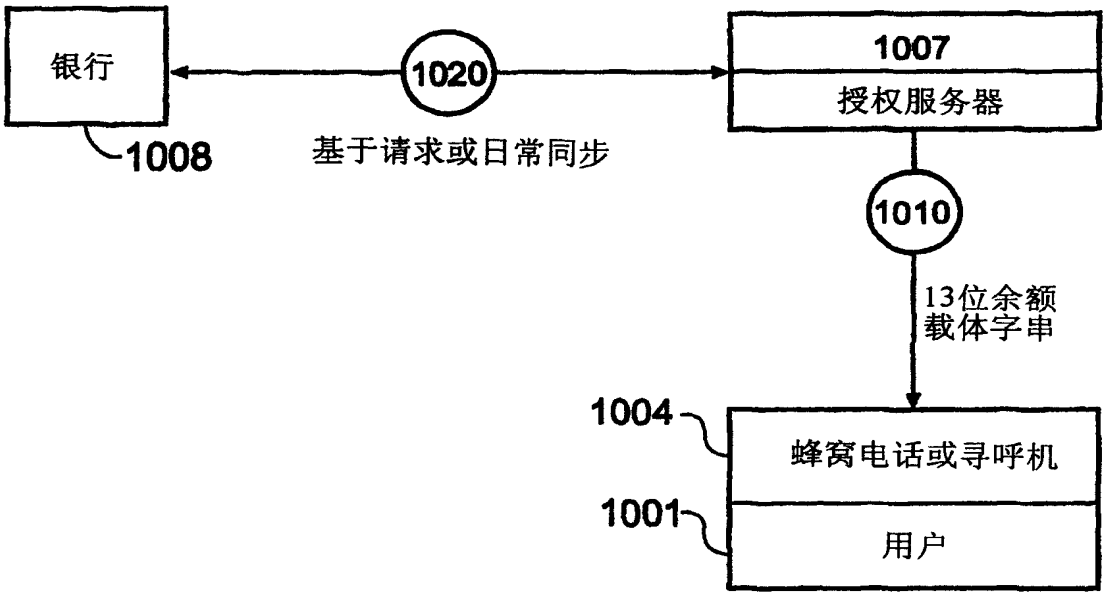


图 10

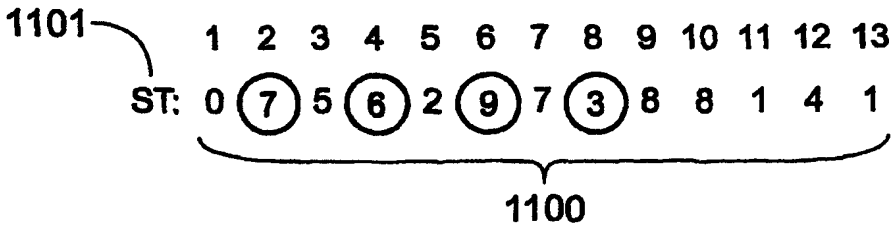


图 11

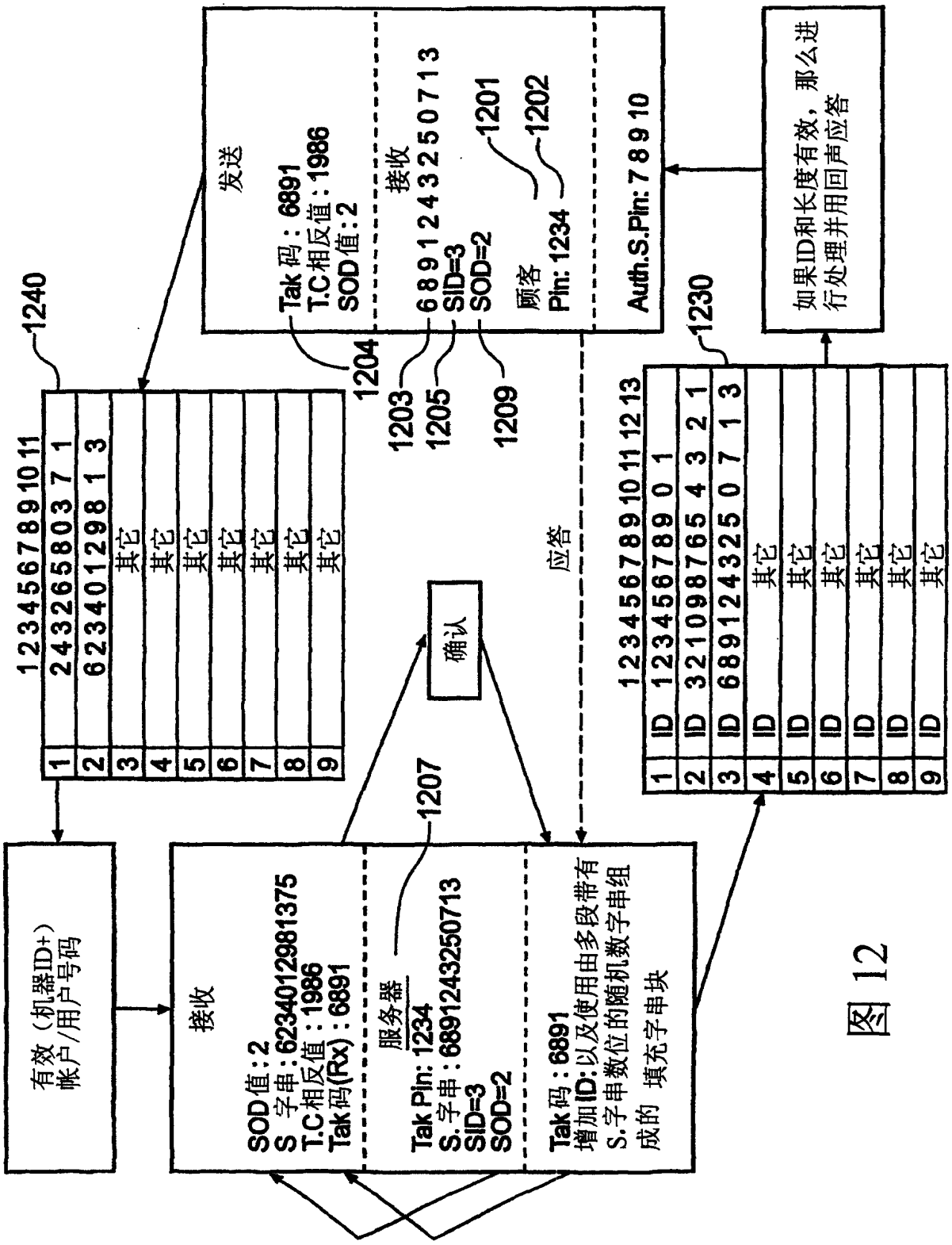


图 12

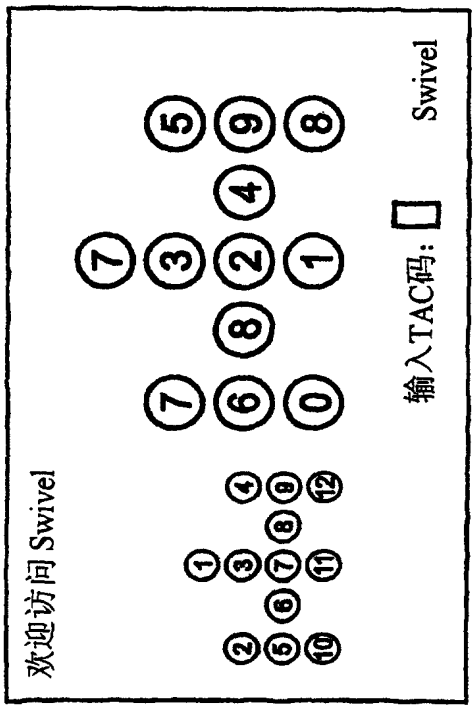


图13a

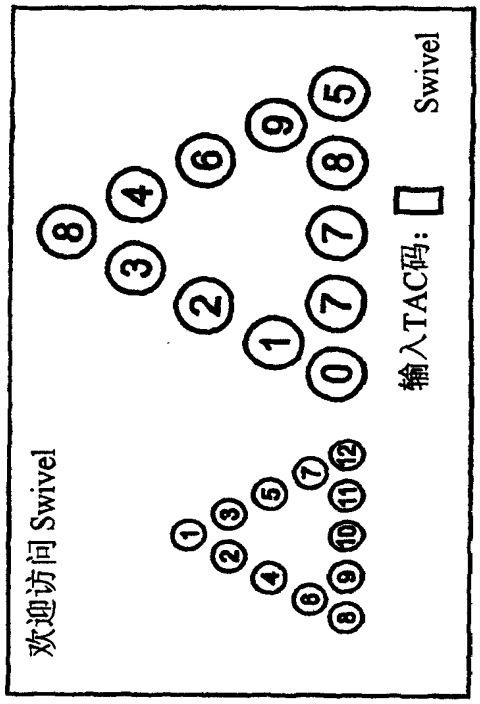


图13b

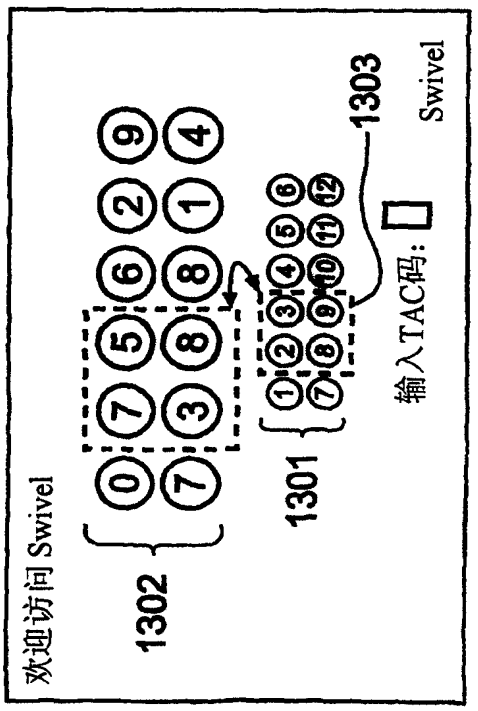


图13c

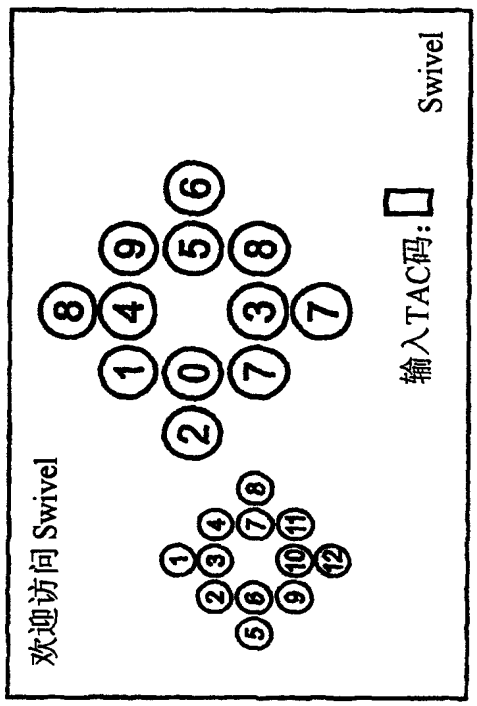


图13d

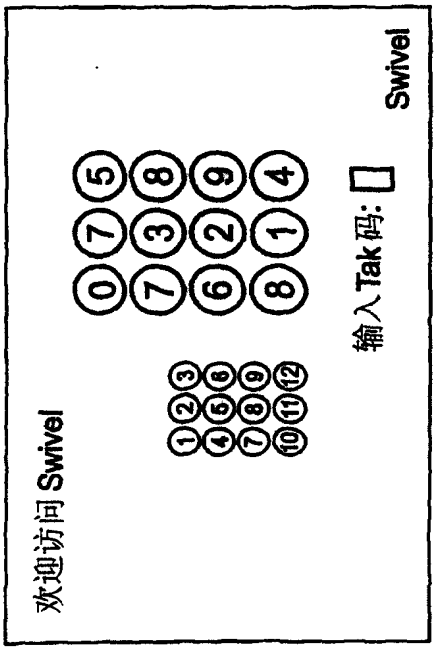


图 13e

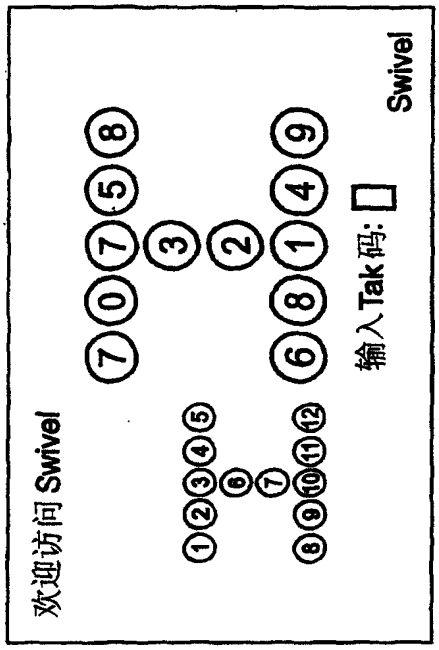


图 13f

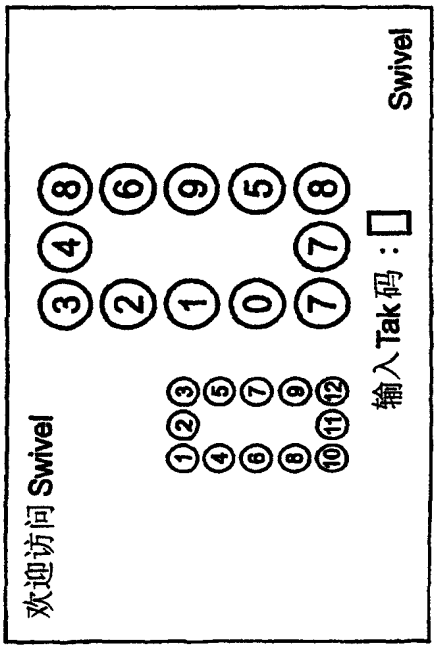


图 13g

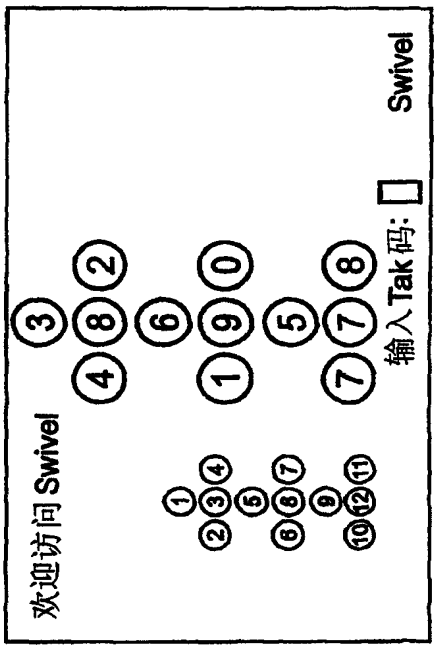


图 13h

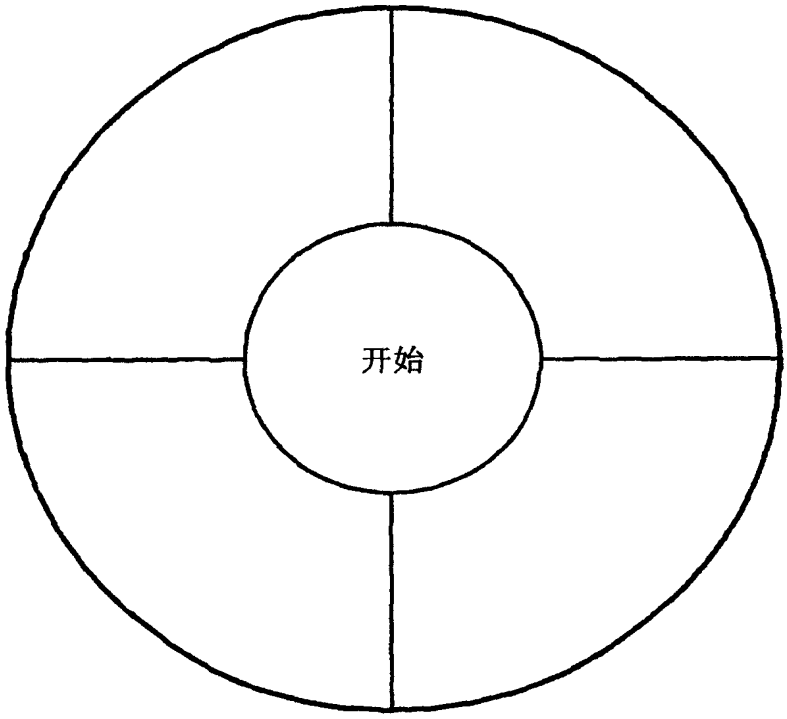


图14

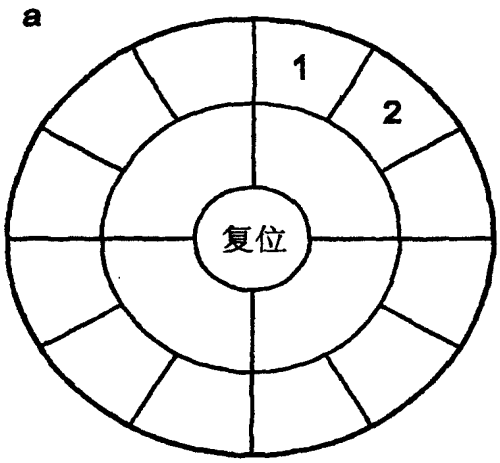


图15a

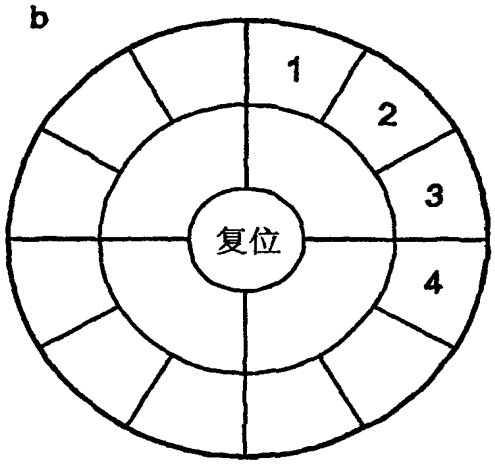


图15 b

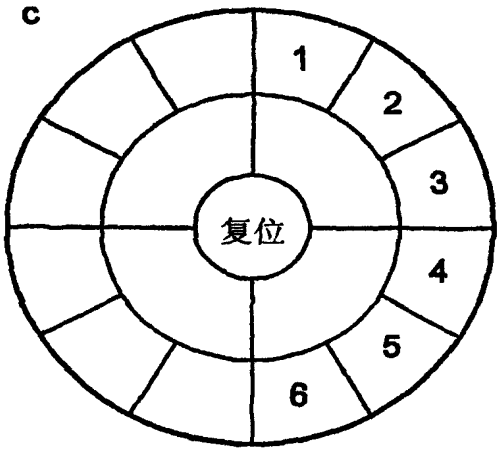


图15 c

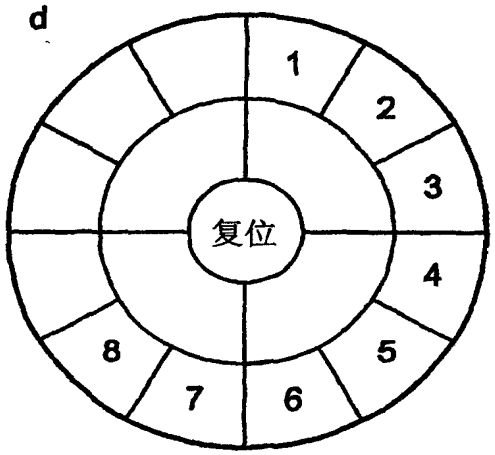


图15 d

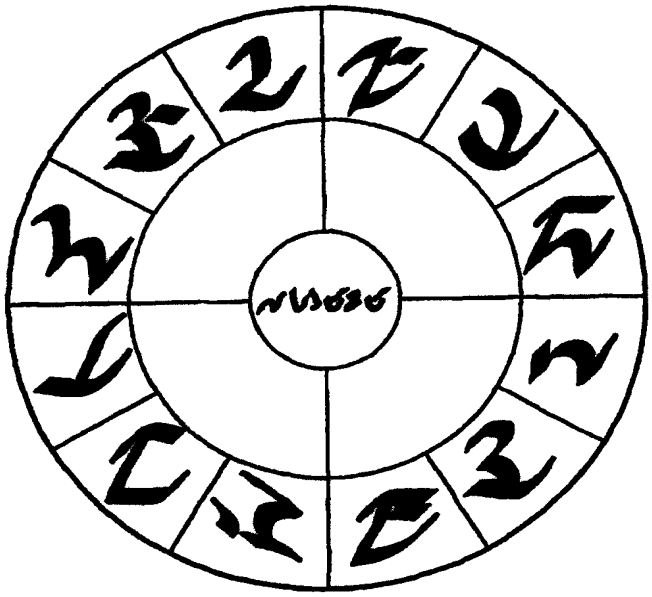


图15e

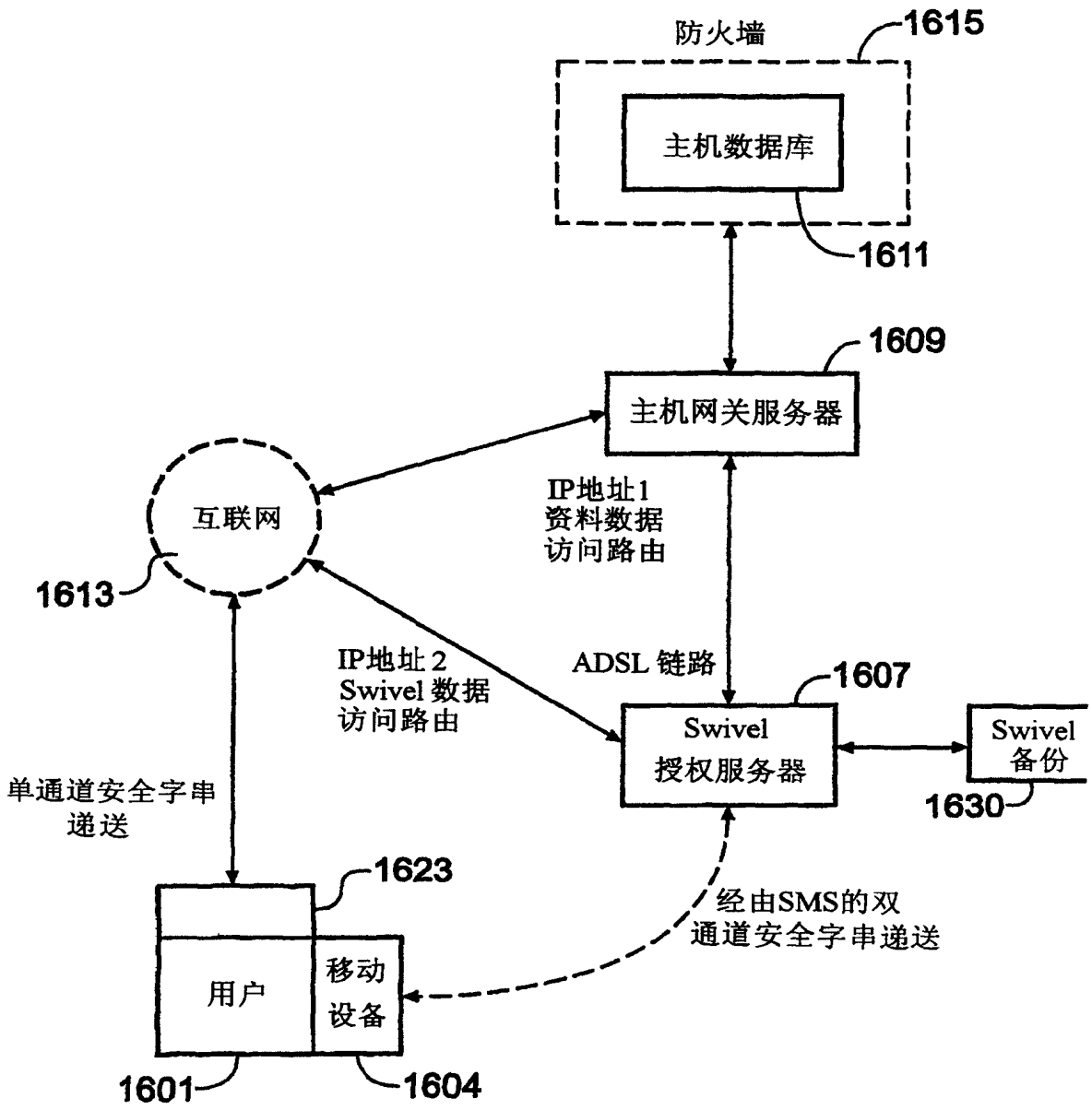


图16

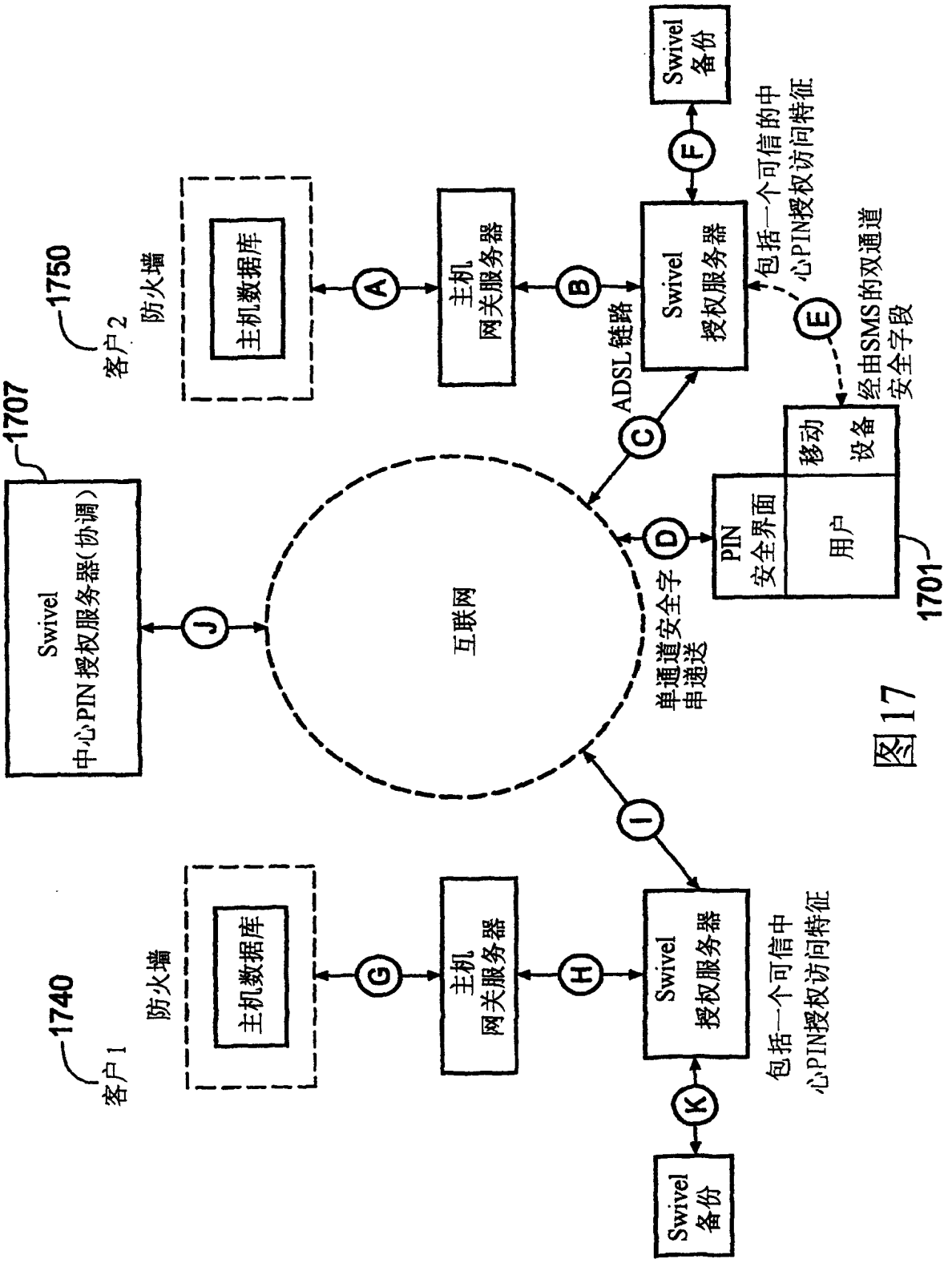


图17

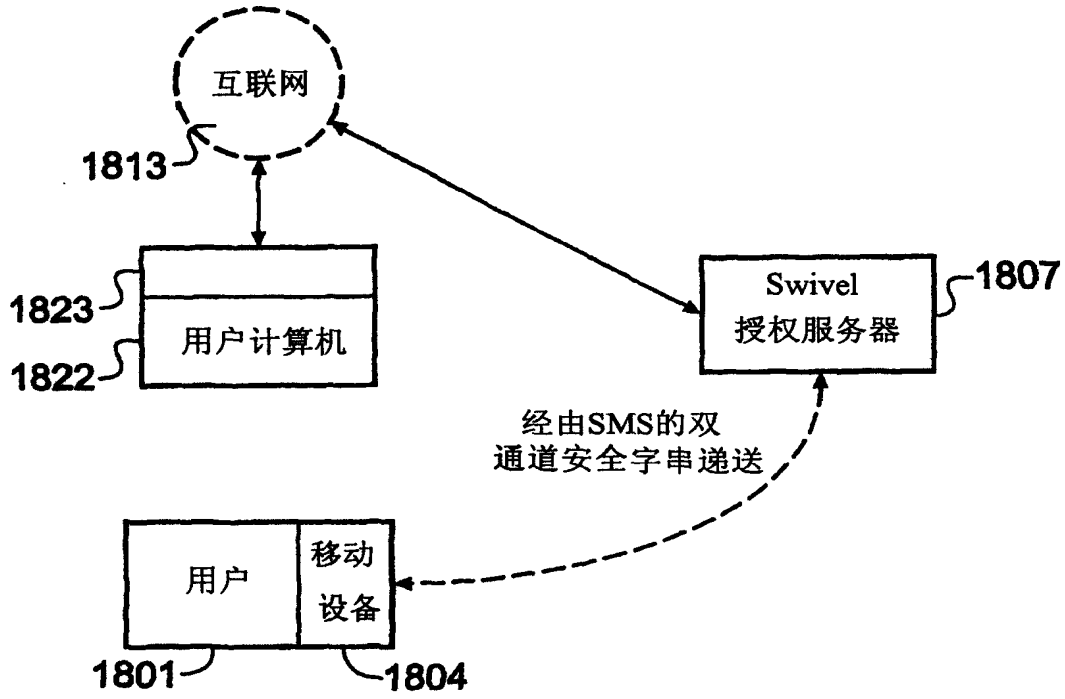


图18

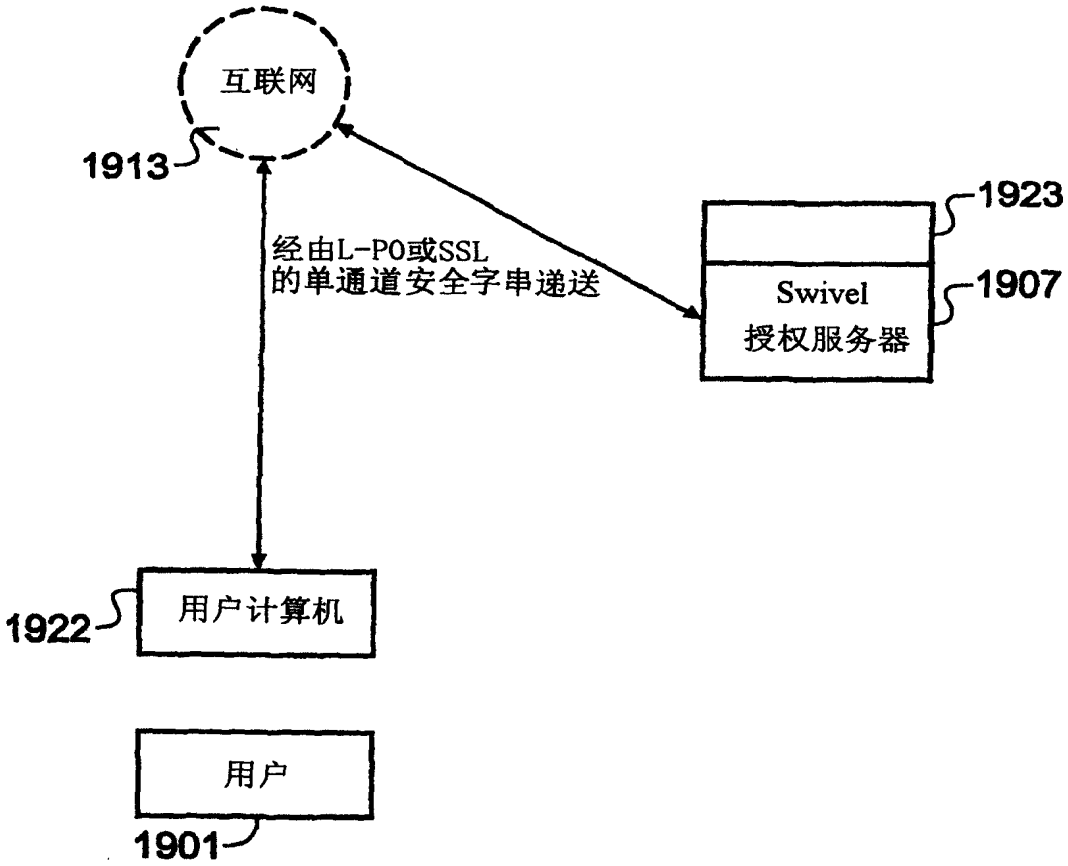


图19

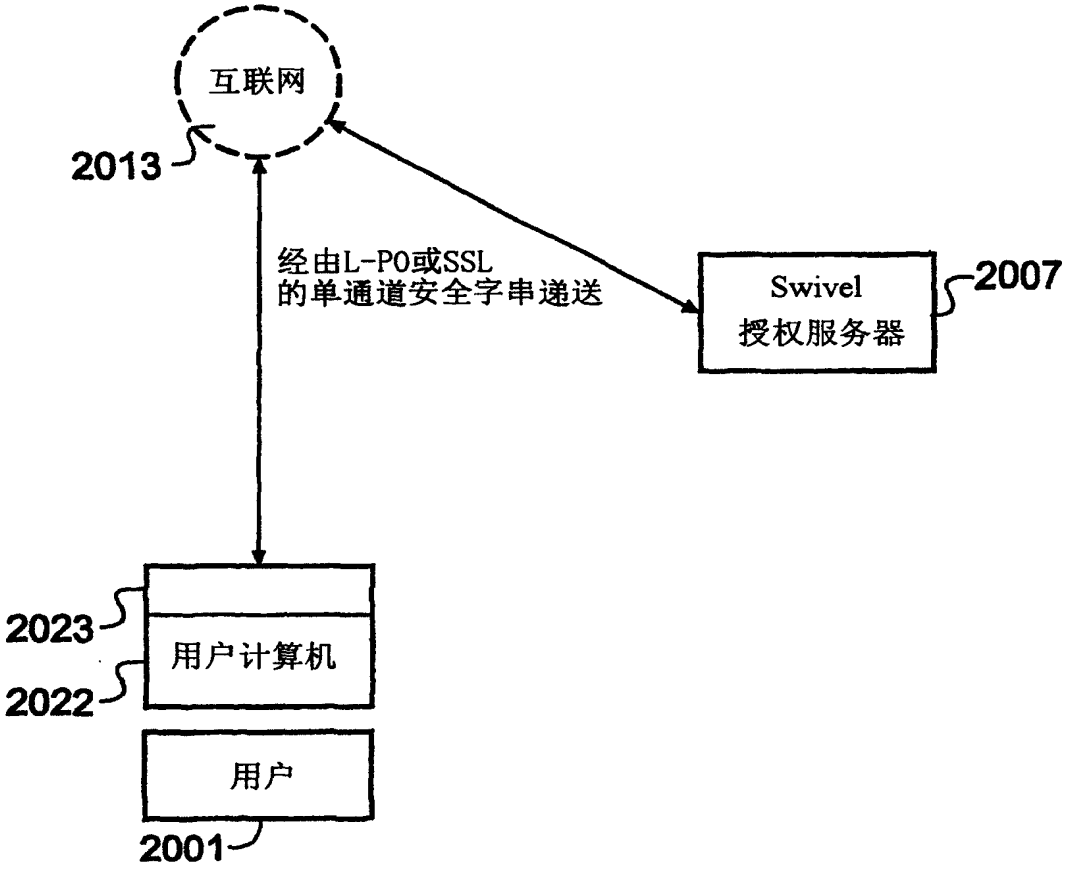


图20

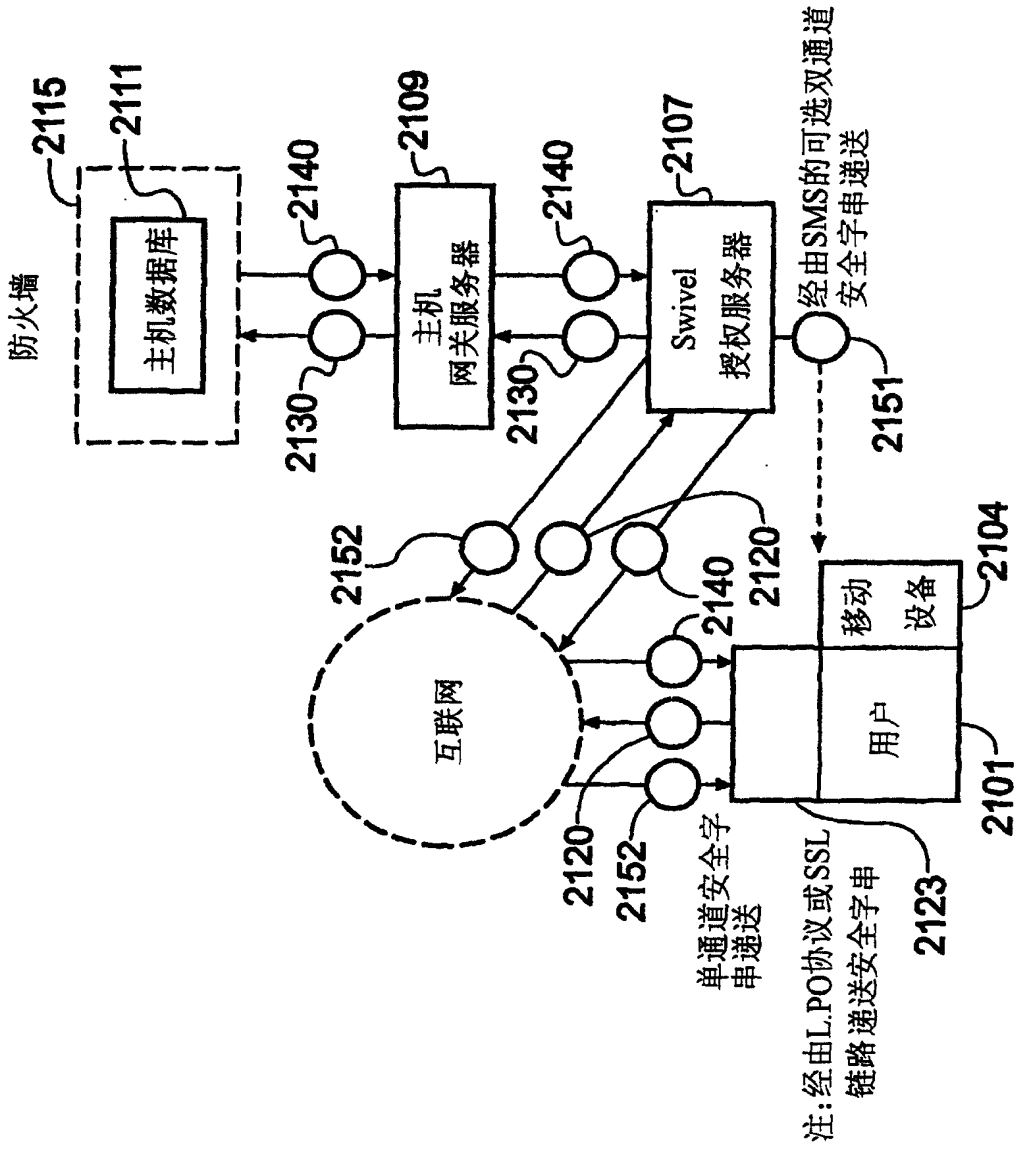


图 21

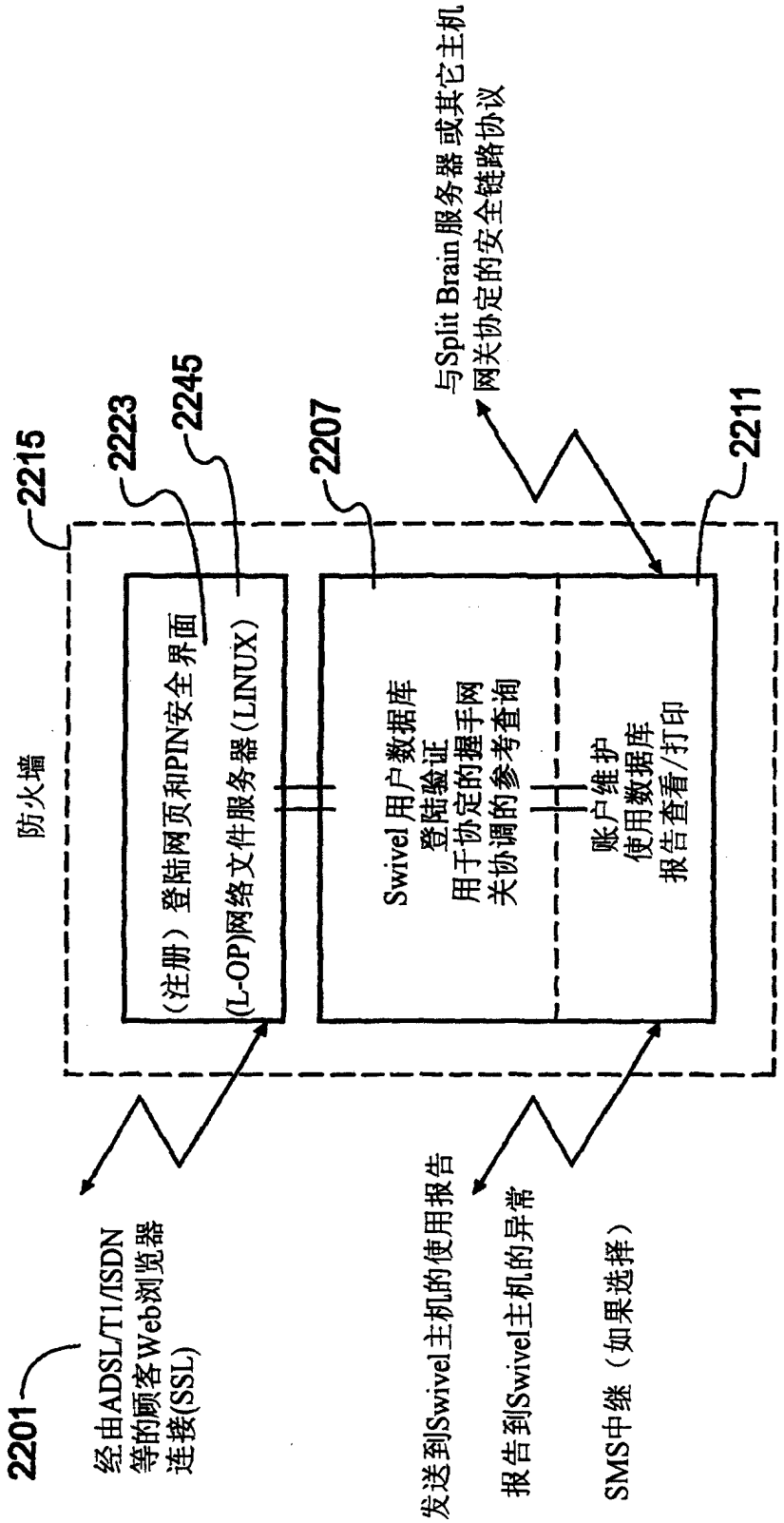


图 22

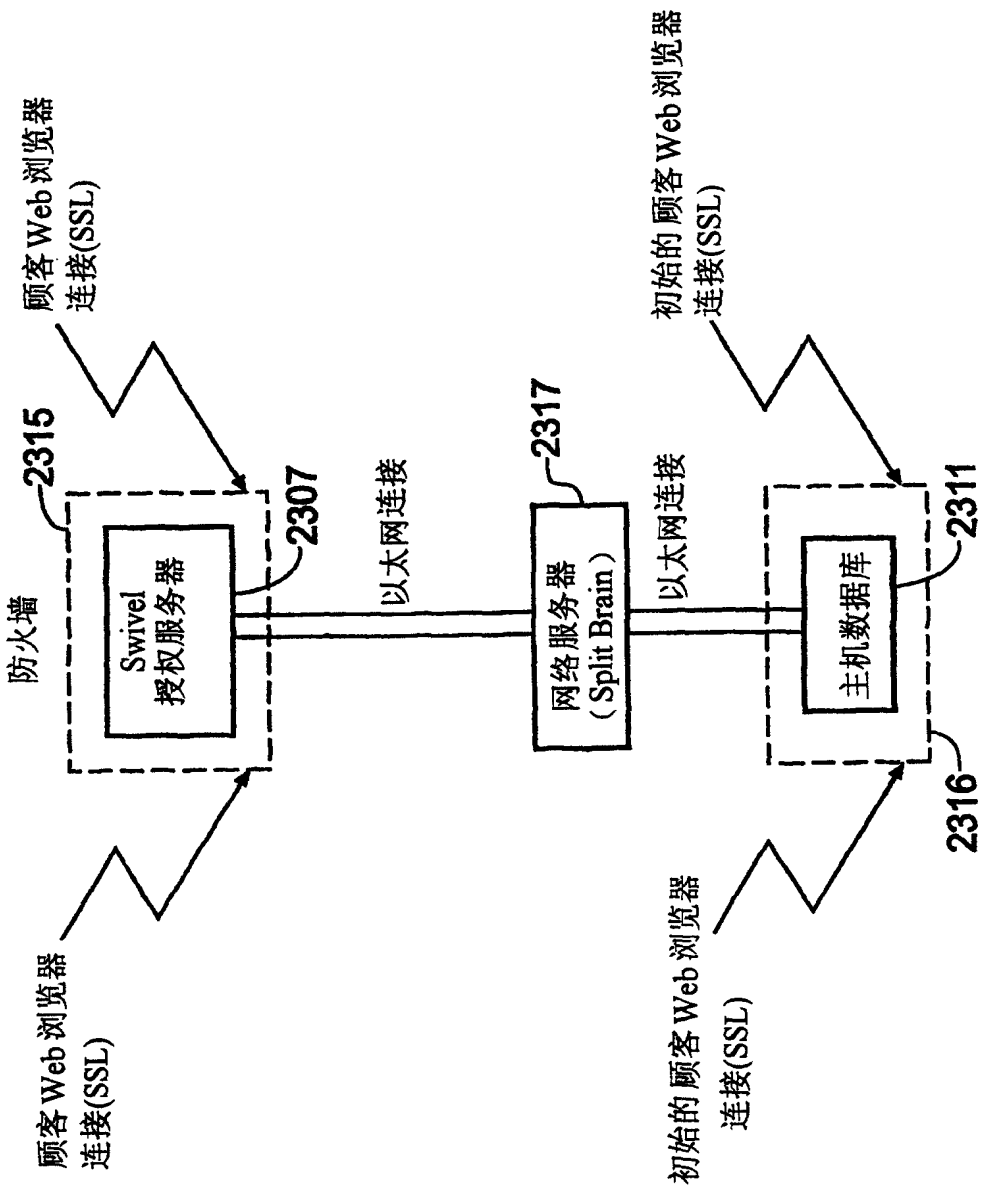


图 23

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 04/10/2023
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

DATE MAILED: 04/10/2023

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

TITLE OF INVENTION: REFUND CENTERS FOR PROCESSING AND DISPENSING VENDING MACHINE REFUNDS VIA AN MDB ROUTER

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	07/10/2023

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.

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 04/10/2023
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.
15/893,514	02/09/2018	Paresh K. Patel	104402-5026-US	4668

TITLE OF INVENTION: REFUND CENTERS FOR PROCESSING AND DISPENSING VENDING MACHINE REFUNDS VIA AN MDB ROUTER

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	07/10/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS
OUSSIR, EL MEHDI	3685	705-050000

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 1002-1546

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 04/10/2023

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

EXAMINER	
OUSSIR, EL MEHDI	
ART UNIT	**PAPER NUMBER**
3685	

DATE MAILED: 04/10/2023

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.

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.

Notice of Allowability	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--

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 01/30/2023.
   ☐ 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 See Continuation Sheet . 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 _____.

/EL MEHDI OUSSIR/
Primary Examiner, Art Unit 3685

Continuation of 3. The allowed claim(s) is/are: 11,16,18-19 and 21-28

Detailed Action

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.

This communication is in response to Applicant's response filed on January 30, 2023 in response to Examiner's Non-Final Office Action filed on September 30, 2022.

The information disclosure statements filed on September 16, 2022 and October 19, 2022 have been considered.

Claims 11, 16, 18-19, and 21-28 are pending. All other claims are cancelled.

Reasons for allowance

Claims 11, 16, 18-19, and 21-28 are allowed.

Applicant's arguments filed on January 30, 2023, pages 6-8, regarding claim rejections under 35 U.S.C. 112 have been fully considered and are persuasive. The claim rejections are withdrawn.

All previous rejections and response to arguments are incorporated entirely herewith.

The claims overcome all objections and rejections.

The claims are novel over prior art because the claims are not obvious in light of the prior art. Although the claims capture different limitations that can be found in various references individually; the limitations as a whole would not be deemed obvious.

Some of the closest art related to the claims include U.S. Patent Application Publication 2015/0235202 to Zabala, U.S. Patent Application Publication 2015/0154579 to Teicher, U.S. Patent 9547859 to Patel et a., and U.S. Patent Application Publication 2016/0086145 to Tsutsui.

Zabala teaches a device in communication with a vending machine to perform cashless payments. A user can utilize a mobile device to establish a connection with the vending machine and purchase a product from the phone and have the vending machine dispense it.

Zabala teaches receiving a request for a cash payment; transmitting the request to an authorizing server distinct from the mobile device; 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… payment accepting machine- dependent conditions, wherein a first of the one or more… payment accepting machine-dependent conditions comprises a… button or control at the payment accepting machine must be engaged; Abstract, at least Paragraphs 0004, 0042 and Figures 1, 8, 11, and 16.

Zabala does not explicitly disclose time dependent condition for the transaction; however, a transaction that is completed is understood that it is completed within a predetermined time otherwise the transaction is not processed. Zabala does not specifically disclose that the button must be activated within a predetermined time; however, because Zabala teaches a button is pressed in order to allow for the item to be dispensed, it is understood that said pressing is done within a predetermined time.

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.

Patel does not teach 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.

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.

The references relied upon throughout prosecution, cited, and the newly cited references fail to disclose:

A method, comprising: at a mobile device:

receiving a request for a cash payment; transmitting the request to an authorizing server distinct from the mobile device;

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.

Dialog®

STIC
Scientific and Technical Information Center

Report Information from Dialog

July 14 2023 11:33

Table of contents

1. Are mobile payments the smart cards of the aughts?..... 1

Bibliography..... 7

Are mobile payments the smart cards of the aughts?

Author: Jacob, Katy

Publication info: Chicago Fed Letter 240: 1-4. Federal Reserve Bank of Chicago. (Jul 2007)

Abstract (summary): During the 1990s, payment industry analysts, policymakers, and academics predicted an eminent "smart card revolution" as providers began to use closed-loop trials and focus groups to test different types of cards. In the current decade, a new payment revolution is being hyped that combines two subsets of mobile commerce -- mobile payments and mobile banking. Today, smart cards and mobile payments are gaining popularity simultaneously as payment providers seek to capitalize on the information-sharing capabilities of mobile and chip-based payments that are not available in paper or magnetic stripe payments. Due to the many ways that mobile phones are integrated into consumers' daily lives, there is potential to avoid the pitfalls of the past experience with smart cards in developing a robust business model around mobile payments. It is important to note that while the mobile phone might be the most obvious initial channel for large-scale adoption of a new payments infrastructure, it need not be the only channel.

Full text:

Headnote

This article compares the much anticipated but ultimately stalled smart card revolution of the 1990s with the current expansion of mobile payment platforms, and asks how mobile payments fit into the larger payment system.

In the past few years, payment networks and banks have begun to follow in the footsteps of start-up companies and offer mobile platforms, meaning in-person or remote payments via a mobile phone or other mobile device. Is this just another overhyped trend (like smart cards in the 1990s), a real payments revolution, or something in between? In short, are mobile payments the smart cards of this decade?

During the 1990s, payments industry analysts, policymakers, and academics predicted an eminent "smart card revolution" as providers began to use closed-loop trials and focus groups to test different types of cards. Smart cards look like credit cards but utilize a microchip to store identification and transaction information. The most famous smart card trial was the 1996 Olympic Games, when Visa developed a smart card for use at 1,500 merchants inside Atlanta's Olympic stadium. Consumers were not inclined to embrace smart cards, given the other payment options available, especially because they were accepted in only a limited number of locations. Smart cards never took off in the general marketplace during the 1990s, and they remained in the trial phase because of ongoing challenges related to infrastructure, marketing, standardization, and profitability.

A decade later, we are just beginning to see the adoption of contactless chip cards using radio frequency identification (RFID) technology. All of the major card networks and many large financial institutions have rolled out contactless products. Some very large merchants, such as McDonald's and Wal-Mart, have invested in RFID infrastructure. More than 40,000 U.S. merchant locations accept contactless payments. Analysts estimate that there are 27 million contactless cards in the U.S. today.1 Eleven years after the first major trial, smart cards finally seem to be gaining some traction.

In the current decade, a new payments revolution is being hyped that combines two subsets of mobile commerce-mobile payments and mobile banking. Mobile payments are defined as "any payment where a mobile device is used to activate and/or confirm the payment."2 A variety of solution providers, payments processors, and other institutions can offer mobile payments. Mobile banking, on the other hand, remains the exclusive domain of financial institutions that have a deposit relationship with a consumer. While mobile banking

services can enable mobile payments, the reverse is not true.

Each subset of mobile commerce is predicted to grow exponentially in the marketplace. Some analysts predict that, globally, mobile payments will be worth $55 billion in 2008.3 But as with smart cards, while mobile payments have gained ground in Asia and Europe, they have not in the U.S. There are a number of reasons for this, including regulatory, market, technological, and cultural differences. First of all, the existing electronic payments infrastructure in the U.S. is expensive to replace, especially for merchants. In some cases, countries with less developed electronic payment systems have been able to move more quickly into mobile payments. Moreover, in some developing economies, such as those in the Caribbean and South Africa, the lack of telephone land lines brought more consumers into the mobile market faster.

At the same time, the U.S. wireless market is fairly atypical in the world in its complexity. There is no one set of standards for the high number of firms and networks involved in the wireless market, which can impede innovation and interoperability in different areas of the country. In Japan, on the other hand, NTT DoCoMo is dominant in the mobile market and was able to use its very large market share to influence merchants and financial services companies. Further, this telecommunications company also directly owns its own payment platforms to facilitate commerce, which would generally be a more difficult proposition within the regulatory environment in the U.S. In addition, largely because of legacy pricing structures, American consumers have been slower to adopt short messaging service (SMS) communication (mobile phone text messaging) than their counterparts overseas, and SMS is a critical part of many mobile payment systems.

How do mobile payments work?

There are two ways to think about mobile payments. One involves the phone as a chip carrier, wherein a computer chip using near field communication (NFC) technology is built into the phone.4 The other option integrates payments into the phone's software, enabling a consumer to use the phone as a virtual "mobile wallet." For in-person or proximity payments, consumers use the phone to make a purchase at a point-of-sale terminal that is equipped to handle the payment. Remote payments utilize SMS, wireless application protocol (WAP) ,9 or a proprietary solution integrated into the phone's software to initiate payments that do not require a point-of-sale terminal.

Many mobile trials in the U.S. have focused on remote payments, and some financial services companies have begun to relay financial information to customers using SMS. Some trials have utilized a chip-based model. In order to provide banking functionality, such as account balance checks, consumer alerts, and payment verification, most providers use an Internet-browser-based solution or proprietary software to connect to the bank's network. Depending on the structure, both proximity and remote payments might require a consumer to be connected to the financial system in some way, through a deposit account, credit card account, or debit card account. The advent of prepaid cards, however, enables some consumers to access these types of mobile payments without having bank accounts or credit histories.6

The promise of mobile payments

The number one reason given for the predicted rise of mobile payments is the prevalence of mobile phones coupled with consumers' willingness to adopt new mobile functionality. Globally, there are over 2.5 billion mobile phone users, surpassing Internet or personal computer users. In the U.S., there are more than 230 million wireless subscribers, and there are high users of mobile phones across all income levels.

To be successful, any new payment form needs a large customer base and a high volume of transactions. The mere prevalence of mobile phones does not necessarily mean that enough consumers will embrace them as payment instruments. Mobile payments are in their infancy, and while consumers currently see their potential value, it is difficult to gauge their inherent value. Research suggests that consumers need more exposure to mobile payments possibilities before we can understand the factors driving adoption. Because of its high mobile phone usage, the youth market has been touted as the cohort that will catapult mobile payments into the financial mainstream. One survey found that, in the past year, more than 10% of respondents made a purchase

with a mobile phone, while a slightly higher number made a personto-person (P2P) payment with a mobile device. The same survey found that those aged under 25 purchase digital content for their phones, while those aged 25-34 are more likely to use phones to transfer funds.7

Importantly, although mobile payments represent another payment choice for consumers-who are estimated to make 58 individual payment choices each month-these payments often rely on traditional funding and settlement systems.8 In fact, many current U.S. mobile payment trials, especially those focused on proximity payments, are dependent on the existing magnetic-stripe-card-based infrastructure. In these cases, the mobile phone becomes a device through which consumers access payment card accounts, and arguably, no real payment substitution takes place. On the other hand, at some point in the future, a chip placed in a phone or another device could become the primary way that consumers access credit or prepaid accounts, eliminating the need for a physical card.

Payment trials and tribulations

There is a parallel between today's mobile payment trials and the smart card trials of the 1990s. Analysts agree that our legacy payments infrastructure represents one of the biggest obstacles to mobile payments. Because these new payment systems have had limited exposure, there is a lack of large-scale data sets to facilitate comparisons with other payment forms. It is also difficult to infer U.S. usage from international experience because of market differences, as discussed earlier. Understandably, companies involved in limited trials are unwilling to make significant infrastructure investments when it is not clear how consumers will react. Payment providers also typically assume that merchants will bear the costs of the new infrastructure, while merchants need to be convinced of the benefits accruing to them before making such investments.

Ironically, it is in part due to the ways that the smart card and mobile payment trials have been developed that it is difficult to gauge consumers' adoption of the new payment methods. Most of these trials have occurred in closed-loop or limited-scope systems and, by definition, test only one distribution method (phone or card) rather than several simultaneously. When consumers are out of the "trial zone" or away from areas that allow remote payment functionality, they are not able to use the payment devices. In the 1990s, limited consumer appetite, infrastructure costs, and uncertainty over issues such as standards, security, and customer relationships kept companies from moving forward with their smart card plans.

There is now a synergy between the mobile and chip worlds. As multiple mobile payment trials are in process, there are also an increasing number of chip-based card trials among major firms. Thus, mobile payments are not rising up in a vacuum-RFID/NFC chip platforms are simultaneously gaining ground as the networks and large financial institutions tentatively accept the possibility of moving to chip-based payments. For example, Wal-Mart's decision to require its top suppliers to put RFID tags on shipping crates has been influential, even though some suppliers balked at the $0.25 to $0.30 cost per tag. Further, the existing RFID infrastructure at the merchant level, while small, reduces a key initial hurdle for mobile payments adoption.

Multiple industries are needed to make a new mobile payments infrastructure a reality. Obviously, telecommunications firms have a significant role to play, as do software and hardware companies, banks, merchants, and networks. Because of the large number of players, analysts question who will be "in charge" of mobile payments in the future: Who will deal directly with the customer, absorb the risk, pay for the infrastructure, and foster innovation? And how will revenues be divided to ensure that the cost to the consumer is sufficiently attractive?

Some analysts argue that banks play the most crucial role in the equation and that mobile payments will never truly take off without an effective mobile banking platform. But this is one payment form that banks can't exclusively dominate. They need the cooperation of phone companies that are looking for new ways to differentiate themselves in a crowded market. As banks compete with each other for similar customers, so do phone companies. However, they are not necessarily vying for the same set of customers. Mobile companies have high penetration rates among unbanked and lower-income households whom banks find hard to reach,

while phone companies might be able to lure higher-income customers who would be willing to switch from Internet payments to mobile payments.

Is there a "killer" mobile application?

Mobile holds a significant advantage over contactless cards in the area of paperless two-way communication. Card-based models do not allow for the sending, receiving, and presenting of information, as mobile devices do. Internet payments made via personal computer are most similar to mobile payments in this regard, but currently require more cumbersome hardware. As we enter the age of the Apple iPhone and similar devices, it becomes clear that mobile phones now have the ability to operate as small-scale computers. Some mobile payment platforms involve specific downloaded software, and NFC chips can carry a substantial amount of data. Moreover, as technology advances with innovations such as WiMAX,9 Internet connections through mobile devices will become faster and more readily available.

Because of the efficient electronic payment mechanisms in the U.S., mainstream consumers might be interested in mobile payments for reasons beyond payments per se. It is not always necessary to be able to pay for anything from anywhere anytime, but consumers might find great utility in being able to send and receive financial information from the same device that they use to make payments. As behavioral economists are quick to point out, many consumers like to budget their purchases. One of the benefits of using mobile payments is that it facilitates recordkeeping to help consumers stay within budget. For example, some prepaid card companies have begun offering a text message service to consumers who would like to be notified of each transaction. This type of real-time account recordkeeping can be especially beneficial for consumers with low balances or those who are sharing accounts with family members.10 Moreover, merchants can derive value from the information exchange made possible through the mobile phone or device by developing loyalty programs and targeted marketing campaigns.

It is this interconnected functionality that makes mobile payments unique. A mobile payments platform can integrate payments, banking, and real-time two-way data transmission. The same cannot be said of cash, checks, or cards. However, most mobile trials have been siloed into remote payment pilots that direct consumers through existing payment networks and utilize SMS to relate information or chip-based trials that enable proximity payments. A "killer" application might allow consumers to use both, as well as provide recordkeeping software for budgeting purposes and other appealing features that consumers would embrace. Unfortunately, the very aspect of mobile payments that makes them appealing carries risk. While firms can use twoway authentication and other security measures, consumers and merchants might be wary of mobile payments in a system where data are broadcast over airwaves and are at risk of interception. Surveys show that consumers would prefer to receive mobile payment offers from banks rather than third party processors or phone carriers, perhaps because of security concerns or familiarity.11 The incorporation of successful security measures that are not burdensome will be important to mobile payment business models. Companies that can capitalize on a "trusted source" reputation might ultimately be more successful in this space.

Conclusion

Today, smart cards, which debuted unsuccessfully in the 1990s, and mobile payments are gaining popularity simultaneously as payment providers seek to capitalize on the information-sharing capabilities of mobile and chip-based payments that are not available in paper or magnetic stripe payments. Due to the many ways that mobile phones are integrated into consumers' daily lives, there is potential to avoid the pitfalls of the past experience with smart cards in developing a robust business model around mobile payments.

It is important to note that while the mobile phone might be the most obvious initial channel for large-scale adoption of a new payments infrastructure, it need not be the only channel-unless the infrastructure that is eventually built is specific to one form of payment. In the future, we may look back and see that the specific focus on mobile phones or smart cards was limited in scope. A new payments evolution may be realized by a nexus of networks, financial institutions, and technology providers that can ensure a safe, reliable, convenient,

and ubiquitous chip-based payment platform-be it via a mobile phone, RFID tag, contactless card, or another, as yet unforeseen, payment instrument.

Sidebar

Mobile commerce is predicted to grow exponentially in the marketplace. Some analysts predict that, globally mobile payments will be worth $55 billion in 2008.

Sidebar

Research suggests that consumers need more exposure to mobile payments possibilities before we can understand the factors driving adoption.

References

1 Packaged Facts, 2007, Smart Cards in the U.S.: Contactless Payment Cards, report, Rockville, MD, May 1.
2 S. Karnouskos and F. Fokus, 2004, "Mobile payment: A journey through existing procedures and standardization initiatives," IEEE Communications Surveys and Tutorials, Vol. 6, No. 4, pp. 44-66.
3 Celent LLC, 2006, "Mobile commerce: Dealing with the devil in the details," report, San Francisco, CA, February 13.
4 Some solution providers have also placed RFID tags on the phone's memory card to enable proximity payments.
5 WAP is an open, international wireless communication standard, whose principal application is to enable Internet access from a mobile device.
6 Prepaid cards are prefunded, with monetary value recorded on a magnetic stripe. In the case of open-system cards, such prepaid cards can be used on the existing card networks in the U.S. and elsewhere.
7 Financial Insights, 2007, Financial Insights 2007 Consumer Payment Survey, report, Framingham, MA, April.
8 American Bankers Association and Dove Consulting, 2005, 2005/2006 Study of Consumer Payment Preferences, report, Washington, DC, October.
9 WiMAX is defined as Worldwide Interoperability for Microwave Access and aims to provide wireless data over long distances, in a variety of ways. J. Van, 2007, "Taking wireless to the WiMAX," Chicago Tribune, April 12, p. 1.
10 K. Jacob and C. Boyd, 2007, "Mobile financial services and the underbanked: Opportunities and challenges for mbanking and inpayments," Center for Financial Services Innovation, report, April.
11 CheckFree Corp. and Firethorn Holdings LLC, 2006, "CheckFree and Firethorn partner to deliver mobile banking and bill payment services for financial institutions," press release, Atlanta, GA, November 9.

AuthorAffiliation

by Katy Jacob, research specialist

Subject: Cellular telephones;Electronic banking;Payment systems;Smart cards;Software;Service introduction;Mobile commerce;Infrastructure

Location: United States--US

Classification: 9190: United States8120: Retail banking services5250: Telecommunications systems &Internet communications

Publication title: Chicago Fed Letter

Issue: 240

Pagination: 1-4

Number of pages: 4

Publication year: 2007

Publication date: Jul 2007

Publisher: Federal Reserve Bank of Chicago

Place of publication: Chicago

Country of publication: United States

Publication subject: Business And Economics--Banking And Finance, Business And Economics--Economic Situation And Conditions

ISSN: 08950164

Source type: Trade Journals

Language of publication: English

Document type: Feature

ProQuest document ID: 214565521

Document URL: https://dialog.proquest.com/professional/docview/214565521?accountid=131444

First available: 2010-06-08

Updates: 2014-05-222022-09-26

Database: ABI/INFORM® Professional Advanced (1971 - current)

Bibliography

Citation style: APA 6th - American Psychological Association, 6th Edition

Jacob, K. (2007). Are mobile payments the smart cards of the aughts? Chicago Fed Letter, (240), 1-4. Retrieved from https://dialog.proquest.com/professional/docview/214565521?accountid=131444

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.

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 1002-1568

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.

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.

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

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.

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.

Espacenet

Bibliographic data: CN106803175 (A) — 2017-06-06

Snap mobile payment apparatuses, methods and systems

Inventor(s): HAMMAD AYMAN; KARPENKO IGOR; GAVRILOV MIROSLAV; SHRIVASTAVA ABHINAV; CARLSON MARK; HARIRAMANI PRAKASH ± (A·哈曼德, ; I·卡彭科, ; M·加夫利洛夫, ; A·施里瓦司塔瓦, ; M·卡尔森, ; P·哈里拉马尼)

Applicant(s): VISA INT SERVICE ASS ± (维萨国际服务协会)

Classification: **- international:** *G06Q20/36*
- cooperative: G06Q20/20 (EP, US); G06Q20/204 (EP, US); G06Q20/326 (EP); G06Q20/3276 (EP, US); G06Q20/36 (CN); G06Q20/3674 (EP, US); G06Q20/384 (EP); G06Q30/06 (EP, US)

Application number: CN20171037081 20120216 Global Dossier

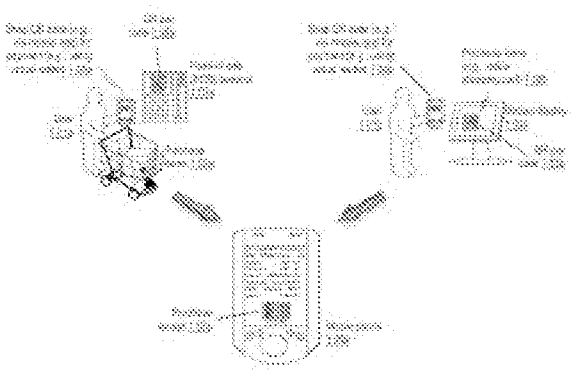
Priority number(s): US201161443624P 20110216 ; US201161512248P 20110727 ; US201161522213P 20110810 ; US201161527576P 20110825 ; CN20128018719 20120216

Also published as: CN106803175 (B) AU2012217606 (A1) AU2016204018 (A1) AU2016204759 (A1) AU2018204759 (B2) BR112013021059 (A2) CN103765453 (A) CN103765453 (B) CN109118199 (A) SG193481 (A1) US11288661 (B2) US2012209749 (A1) US2014197234 (A1) US2019034921 (A1) US2022253832 (A1) WO2012112822 (A2) WO2012112822 (A3) less

Abstract of CN106803175 (A)

The snap mobile payment apparatuses, methods and systems (SNAP) transform real-time-generated merchant-product Quick Response codes via SNAP components into virtual wallet card-based transaction purchase notifications. In one embodiment, the SNAP obtains a snapshot of a QR code presented on a display screen of a point-of-sale device from a mobile device. The SNAP decodes the QR code to obtain product information included in a checkout request of the user, and merchant information for processing a user purchase transaction with a merchant providing the QR code. The SNAP accesses a user virtual wallet to obtain user account information to process the user purchase transaction with the merchant. Using the product information, merchant information and user account information, the SNAP generates a card authorization

request, and which the SNAP provides to a payment network for transaction processing. Also, the SNAP obtains a purchase receipt confirming processing of the user purchase transaction.



Notice

DESCRIPTION CN106803175A

10 Snapshot mobile payment device, method and system

[0001]

14 This application is a divisional application based on the patent application with the application number 201280018719.7, the application date is February 16, 2012, and the invention title is "Quick shot mobile payment device, method and system".

[0002]

20 This patent application publication document (hereinafter referred to as "the specification") describes the inventive aspects leading to each new innovation (hereinafter referred to as the new invention technology and/or new method) and contains the subject matter of copyright, mask work and/or other knowledge Property Rights Protected Materials.

24 The respective owners of this intellectual property have no objection to the facsimile reproduction by anyone of the patent disclosure document as it appears in published patent office files/records, but otherwise reserve all rights.

[0003]

30 priority statement

[0004]

34 This application claims priority under 35 USC $119: Serial No. 61/443,624 filed February 16, 2011, entitled "Mobile Capture Checkout Apparatus, Method, and System," Attorney No. P-42032PRV|20270 - U.S. Provisional Patent Application for 127PV; Serial No. 61/512,248 filed July 27, 2011, entitled "Quickshot Mobile Payment Apparatus, Method, and System," Attorney No. 10US01|20270-175PV for U.S. Provisional

Patent Application ; U.S. Provisional Patent Application Serial No. 61/522,213 filed August 10, 2011, entitled "Universal Mobile Payment Platform, Apparatus, Method, and System," Attorney No. 10US03|20270-175PV2; and August 2011 The serial number of the application on the 25th is 61/527,576, the title is "Quipai mobile payment device, method and system", and the US provisional patent application number is 10US02|20270-175PV1.

43 The entire teaching of the aforementioned application is hereby incorporated by reference.

[0005]

47 technical field

[0006]

51 The present invention relates generally to devices, methods and systems for electronic purchase transactions, and in particular, to Snapshot mobile payment devices, methods and systems ("SNAP").

[0007]

56 Background technique

[0008]

60 A customer transaction typically requires the customer to select a product from a display shelf or a website and then check out at a checkout counter or on a web page.

62 Product information is usually selected from web catalogs or entered into point-of-sale terminals.

63 In a physical retail environment, product information is automatically entered by scanning item barcodes at point-of-sale registers with integrated barcode scanners, and customers are typically provided with multiple payment options, such as cash, check, credit card or debit card.

66 Once payment is made and approved, the point-of-sale recorder stores the transaction in the merchant's computer system and generates a receipt indicating that the transaction has been satisfactorily concluded.

[0009]

71 Description of drawings

[0010]

75 According to the inventive aspects of the present invention, the appendix and/or accompanying drawings illustrate non-limiting examples according to various examples of the present invention, aspects of the invention:

[0011]

81 1A-F show block diagrams illustrating example aspects of snap mobile payment based purchase transactions in some embodiments of SNAP;

[0012]

86 2A-F show application user interface diagrams illustrating example features of the Snap Mobile Payment application that facilitates Snap Mobile Payments, in some embodiments of the SNAP;

[0013]

91 3A-E show application user interface diagrams illustrating example features of the Snap mobile payment application for capturing product barcodes, protecting user data, and preventing fraud, in some embodiments of the SNAP;

[0014]

97 Figures 4A-D show data flow diagrams illustrating an example snap mobile payment process in some embodiments of the SNAP;

[0015]

102 5A-E show logic flow diagrams illustrating example aspects of implementing Snap Mobile Payments, such as Snap Mobile Payment Execution (“SMPE”) component 500, in some embodiments of the SNAP;

[0016]

107 6A-B show logic flow diagrams illustrating example aspects of processing quick response codes, such as Quick Response Code Processing (“QRCP”) component 600, in some embodiments of the SNAP;

[0017]

112 Figure 7 shows a user interface diagram illustrating an overview of example features of a virtual wallet application in some embodiments of the SNAP;

[0018]

117 8A-G show user interface diagrams illustrating example features of a virtual wallet application in shopping mode, in some embodiments of the SNAP;

[0019]

122 9A-F show user interface diagrams illustrating example features of a virtual wallet application in payment mode, in some embodiments of the SNAP;

[0020]

127 Figure 10 shows a user interface diagram illustrating example features of a virtual wallet application in history mode, in some embodiments of the SNAP;

[0021]

132 11A-F show user interface diagrams illustrating example features of a virtual wallet application in snap mode, in some embodiments of the SNAP;

[0022]

137 Figure 12 shows a user interface diagram illustrating example features of a virtual wallet application in offer mode, in some embodiments of the SNAP;

[0023]

142 13A-B show user interface diagrams illustrating example features of a virtual wallet application in security and privacy mode, in some embodiments of the SNAP;

[0024]

147 Figure 14 shows a block diagram illustrating an embodiment of a SNAP controller.

[0025]

151 The number preceding each reference number within the figure indicates the figure in which the reference number is introduced and/or elaborated upon.

153 Accordingly, a detailed discussion of reference numeral 101 will appear and/or be referenced in FIG. 1 , reference numeral 201 is introduced in FIG. 2 , and so on.

[0026]

158 Detailed ways

[0027]

162 Snapshot Mobile Payment (SNAP)

[0028]

166 The snapshot mobile payment device, method and system (hereinafter "SNAP") converts the quick response codes of merchant products generated in real time into transaction purchase notifications of card-based virtual wallets through SNAP components.

169 1A-F show block diagrams illustrating example aspects of snap mobile payment based purchase transactions in some embodiments of SNAP.

171 Referring to FIG. 1A, in some implementations, a user such as 101a-b may wish to purchase a product at a merchant store such as 103a or at a merchant website such as 103b.

173 For example, at a merchant store, a user may scan the barcodes of multiple products (eg, 102a) on a point-of-sale ("POS") terminal in the store, eg, 103a, and then indicate which scanned items the user wishes to checkout.

176 In some implementations, the POS terminal generates, via a payment network, a quick response ("QR") code, such as 105a, including information related to the scanned product item, and merchant information for processing the purchase transaction.

179 A user using a user device such as a smartphone may capture an image of the QR code generated by the POS terminal.

181 For example, the user equipment may have an application for quickly obtaining a QR code of the merchant's product.

183 The user device may use the information extracted from the QR code, along with information about a virtual wallet bound to the user device, to initiate a purchase transaction.

185 For example, the user device may use the product and merchant information extracted from the QR code and financial payment information from the virtual wallet to create a purchase transaction request and submit the request to a payment network (e.g., credit card processing network).

[0029]

191 In some implementations, the user device may use an alternative method of capturing a QR code to obtain information from the POS terminal.

193 For example, the POS terminal may communicate to the user device via Bluetooth , Wi-Fi, SMS, text messaging, email, and/or other communication methods the information required to submit a purchase transaction request to the payment network.

[0030]

199 In some implementations, the user 101b may wish to checkout items stored in a virtual shopping cart on an online store website, such as 102b.

201 For example, a user may browse the website using a secure display (eg, part of the user's trusted computing device).

203 When indicating that the user wishes to checkout items in the virtual shopping cart, the website may provide a QR code including information about the products and merchant information in the virtual shopping cart.

205 For example, in cases where the user uses a secure display, a QR code may be displayed at a random location

within the secure display for security purposes.

207 The user may take a snapshot of the displayed QR code and use payment information from a virtual wallet associated with the user device to create a purchase transaction request for processing by the payment network.

210 When the purchase transaction is complete, the payment network provides a purchase receipt, e.g. 107, directly to the user device 106, the POS terminal in the store, and/or the secure display (for a secure online shopping situation) as confirmation that the transaction processing is complete .

213 Accordingly, in some implementations the merchant can be shielded from obtaining the user's personal and/or private information while processing the purchase transaction, while securing the user's virtual wallet using a secure display presenting the merchant's product QR code. integrity.

[0031]

219 In various implementations, such payment processing can be used for a wide variety of transactions.

220 For example, a user dining at a restaurant may obtain a bill that includes a QR payment code that includes details about the cost of the meal included in the bill, as well as the restaurant's merchant ID.

222 Without disclosing any financial or personal information about the user to the restaurant, the user can use the user's smartphone to take a snapshot of the restaurant bill, and use the user's virtual wallet to pay the restaurant bill.

[0032]

228 Referring to FIG. 1B , in some implementations, eg 110 , a user 111 may wish to use the reverse snapshot mobile payment process to checkout items stored in a (virtual) shopping cart in an (online) store, eg 112 .

230 For example, a user may use a secure display, such as 113, that is part of the user's trusted computing device, or browse a website via a POS terminal in a brick and mortar store.

232 When indicating that the user wishes to checkout the items in the virtual shopping cart, the user may generate (e.g., 114) via a mobile application on the user's mobile device connected to the user's virtual wallet, a payment method, offer, reward, etc. for the user. , and/or QR code 115b for other information.

235 The user may provide the QR code displayed on the user's mobile device to a webcam (or other QR code capture device and/or mechanism) installed on the trusted computing device (or POS terminal).

237 The user's trusted computing device or POS terminal can take a snapshot, e.g., 116, of the QR code generated by the user's mobile device and create a purchase transaction request using the payment information from the user-generated QR code for the payment network to process.

240 When the purchase transaction is complete, the payment network may provide a purchase receipt directly to the user's mobile device, POS terminal in the store, and/or a secure display (for secure online shopping situations) as confirmation that transaction processing is complete.

243 Thus, in some implementations, the user will be able to use the QR code generated by the user's mobile device as a replacement for a plastic payment card (e.g., credit, debit, prepaid card), or as an alternative such as near field communication, , etc. and other financial information transmission mechanisms.

248 In some implementations, the QR code can be representative of a one-time anonymous credit card number (see, eg, description associated with FIG. 3B).

[0033]

253 In some implementations, the first user 121b may wish to pay the second user 121a some amount (or equivalent, such as virtual currency, alternative currency, rewards, miles, points, etc.), such as P2P Snapshot mobile payment 120 .

256 The second user 121a may generate a time-limited validity QR code, such as 122, including information about the amount to be transferred and a privacy token/alias linked to the second user's financial account.

258 The second user may display the generated QR code to the first user (e.g., display the QR code to the first user by holding the second user's mobile phone; send the QR code via email, social networking message, twitter, etc.) . The first user takes a snapshot of the QR code, e.g. 123, using the first user's mobile phone, and uses the amount, the second user's privacy token/alias linked to the financial account, and the QR code linked to the first user's mobile phone A first user's virtual wallet to generate a purchase transaction request for processing by the payment network. When the transaction is complete, the payment network may provide a transaction notification receipt to the user who is a party to the transaction. In an alternative implementation, the two users may share data encoded in the QR code via alternate methods of the QR code, including but not limited to: Near Field Communication (NFC), Wi-Fi , Bluetooth , Cellular Web, SMS, email, text messaging and/or other communication protocols.

[0034]

271 In general, it should be understood that such tokens, aliases and/or treatments may be used to advantage in various implementations of Stories mobile payment.

273 For example, a user wishing to participate in a reverse snapshot mobile payment process (see, e.g., FIG. 1B , element 110) may generate a QR containing information about a handle to financial payment information stored on a server of the payment network system code. For example, some implementations of QuickPay mobile payments may generate and/or process handles using a payment token process similar to that described in U.S. Application Serial No. 13/153,301, entitled "Payment Token Apparatus Method and System" Similarly, the entire content is hereby expressly incorporated by reference. Additionally, in some implementations, the handle may encode information in accordance with a compact messaging protocol, such as in Serial No. 6,837,425, entitled "Concise Protocol and Method for Solving Substantially Offline Messaging Between Portable Consumer Devices and Base Devices" described in U.S. Patents, the entire contents of which are expressly incorporated herein by reference. In some Reverse Snap mobile implementations, the user may provide the QR code containing the handle and displayed on the user's mobile device to a webcam (or other QR code) installed on a trusted computing device (or POS terminal) capture device and/or mechanism). A computing device or POS terminal trusted by the user may obtain a snapshot, e.g., 116, of the QR code generated by the user's mobile device and provide a handle extracted from the QR code to the merchant server for a purchase transaction request processed by the payment network . To process the purchase transaction using the handle, the merchant server may generate a card authorization request (such as further described in the discussion below with reference to FIG. 4A) and

provide the card authorization request to the payment network. When the purchase transaction is completed, the payment network may provide a purchase receipt directly to the user mobile device, the POS terminal in the store, and/or the secure display (e.g., for a secure online shopping situation) as a transaction using the handle Acknowledgment that processing is complete.

[0035]

297 In some implementations, a user warning mechanism can be built into the Kuaipai mobile payment purchase transaction processing flow.

299 For example, in some implementations, the merchant server may embed a URL specific to the transaction into the card authorization request. For example, in some implementations, the POS terminal, remote device, and/or desktop computer may embed the URL in optional layer 3 data in the card authorization request. The URL may point to a web page stored on a merchant server dedicated to the transaction that is the subject of the card authorization request. For example, the web page pointed to by the URL may include details about the purchase transaction, such as products purchased, cost of restocking, time expiration, status of order processing, and the like. Thus, by passing the URL of the webpage to the payment network, the merchant server can provide the payment network with details of the transaction. In some implementations, the payment network may provide notifications to the user, such as payment receipts, transaction authorization confirmation messages, shipping notifications, and the like. In such a message, the payment network may provide the URL to the user device. The user can navigate to the URL on the user's device to obtain alerts about the user's purchases, as well as other information, such as offers, coupons, related products, reward notifications, and the like.

[0036]

315 In some implementations, multiple users may participate in a group payment via Snap Mobile Payment to split a tender, eg, 130 .

317 In some implementations, one of the users 131a may obtain a snapshot (eg, 132) of a QR payment code (eg, 134) generated at a POS terminal, eg, 133 (or, eg, presented on paper such as a meal bill). The user may in turn generate a QR split payment code containing information about the amounts into which the payment has been split. The user 131a can present the decomposed payoff QR code 135 to other users 131b-c, and the user 131b-c can obtain a snapshot, e.g., 136, of the decomposed payoff QR code. In some implementations, the user 131b-c may reimburse user 131a via the payment network for payment of the original QR code, or the user 131b-c may make direct payment to the merchant via the decomposed reimbursement QR code (e.g., When the user 131a takes a snapshot of the merchant's QR code, no payment processing occurs immediately). In some implementations, the merchant may provide the split-pay QR code directly to the users 131a-c.

[0037]

330 In some implementations, group mobile payments may be enabled by using an alternative communication mechanism, rather than using QR codes.

332 For example, in some implementations, the POS terminal 133 may communicate with the users 131a-c using a communication protocol such as Bluetooth . The POS terminal can establish an independent communication session with each user serially or in parallel. Through these separate communication sessions, the POS terminal may transmit the product and/or merchant data required by the user's device to generate individual purchase transaction processing requests. Thus, through these separate communication sessions, the POS terminal can break down group reimbursements associated with users 131a-c into individual payment amounts.

[0038]

342 Referring to Figure 1C, in some implementations, for authentication/verification purposes, as well as to provide digital permission to disclose personal and/or private information, Snap Mobile Billing can be used.

344 For example, a user 142 visiting his/her doctor 143 may be required to provide formal permission to disclose personal information (eg, medical records) to the doctor. The doctor's terminal (eg, 144) may generate a QR code containing the doctor's digital credential and information about the type/content of the requested user's medical record. The user can take a snapshot of the QR code through the user's mobile device. The user's mobile device can generate a request for record release from the QR code and serve as verification that the request was obtained from a personally trusted device, such as the user's mobile device. In an alternative implementation, the user can select the personal information that the user would like to disclose to the medical provider, and the user's mobile device can generate a QR code for the doctor's terminal to take a snapshot to retrieve the user's medical information. In some implementations, the QR code can also include payment information (eg, the user's payment account information, or the doctor's acquirer information) and information about the controlled release of personal information.

[0039]

358 In some implementations, SNAP can facilitate P2P transactions by pre-populating a changeable QR payment code, such as 150.

360 For example, a first user with a public profile page (eg, 151) can place an image of a QR code in the public profile, eg, 152 . For example, the QR code may include a predetermined payment amount for a purchase transaction initiated by taking a snapshot of the QR code. In some implementations, the predetermined amount can be $0 (eg, $0 QR payment code). The second user can use the mobile device to capture a snapshot of the QR payment code, and can set the amount the second user wants to pay the first user through the second user's mobile device. The second user's mobile device can provide the payment network for transaction processing with the information encoded within the QR code and the payment amount selected by the second user.

[0040]

371 It should be understood that the various aspects of Snap Mobile Payment described herein may be used for any controlled exchange of information and/or payment.

373 For example, referring to FIG. 1D , in some implementations, a user may obtain a pay-per-view program,

such as 160 , through QuickPai mobile payment. For example, a television display may provide an advertisement including program information (eg, 162) and a QR payment code for obtaining the program content, eg, 161 . The QR code includes information identifying the program information, as well as information identifying the television subscriber account information, television address, and the like. The user can take a snapshot of the QR code and provide the information embedded in the QR code along with the user's mobile device information (eg, subscriber account number linked to the user's virtual wallet, payment account information, etc.). When the payment information is processed by the payment network, the payment network can provide an indication that the payment is complete to the television programming provider, and the television programming provider can stream the programming content to the user's television. As another example, a similar flow can be used for in-flight entertainment, such as 170, where an on-board screen can provide program information 172 and a QR payment code 171 for the user to snap for in-flight entertainment initiation. As another example, billboards, wall hangings, posters, in-store advertisements, temporary fences, etc., such as 180, may include offers for products/services, as well as QR codes including merchant information and product information identifying purchase quantities, etc. The user can snap a snapshot of the QR code with the user's mobile device linked to the user's virtual wallet to purchase the product and/or service, and, if appropriate, the product can be exchanged directly with the payment network as The purchase information specified as part of the purchase request sent by the user's mobile device is shipped to the user's address. As another example, a newspaper, such as 185, may include offers, advertisements, job postings, etc., containing QR codes, such as 186, containing information necessary for a user to initiate a purchase transaction using a payment network. It should be understood that any aspect of implementing the Snapshot mobile payment discussed in the implementations herein, and/or their equivalents, may be used in any other implementations discussed herein and/or their equivalents.

[0041]

399 Referring to Figures 1E-F, in some implementations, the data required to process a purchase transaction can be provided by methods that replace QR codes, including but not limited to: Near Field Communication (NFC), Wi-Fi , Bluetooth , Cellular Web, SMS, email, text messaging and/or other communication protocols.

403 For example, in some implementations, a user shopping online through a web browser executing on a client device, such as 190, may wish to pay for the purchase of items from an online store website (eg, 191). The website may include user interface elements that a user can activate to initiate shopping checkout and payment. When the user activates the user element, the client displaying the online shopping site may provide a message to the merchant's server to initiate a secure purchase transaction. A merchant server running the online shopping site may establish a secure connection (eg, a secure socket layer connection) to a payment network server of a payment network (eg, 192). And, the payment network server can establish a secure connection to the client. For example, the client may include a secure I/O chip that only allows a secure connection to be established between the client and the payment network server of the payment network. Through a secure connection, the payment network server may provide instructions to the client to request the user to launch the virtual wallet mobile application on the user's user device, see eg FIG. 1F, 196 . The client may thus provide a request to the user to launch the virtual wallet mobile application on the user's user device (eg 193). When the user launches the virtual wallet mobile application on the user device, the user

device and the client can establish a secure connection with each other (eg, via Bluetooth , Wi-Fi, cellular, etc.). In some implementations, the client and user equipment can be preconfigured to rapidly establish the secure communication channel with each other. Through the secure communication channel, the client can provide data to the user's mobile device, or vice versa, to facilitate initiation of the purchase transaction. The virtual wallet application on the user's mobile device (or client) can then generate a purchase transaction initiation message and provide this message to the payment network server for processing the purchase transaction. When the transaction processing is completed, the payment network server may provide a payment completion notification to the client, such as 197 in FIG. 1F, or to the user equipment.

[0042]

427 2A-F illustrate application user interface diagrams showing example features of the Snap Mobile Payment application that facilitate Snap Mobile Payments, in some embodiments of the SNAP.

429 Referring to FIG. 2A , in some implementations, a user may wish to checkout one or more items stored in a virtual shopping cart on an online merchant website. For example, a user may use a browser application, eg, 201, to visualize a checkout page, eg, 202, of the merchant website. The checkout web page can describe the details of the checkout order, such as 203, and can provide the user with one or more options to provide payment for the purchase of stored items. In some implementations, the checkout web page can include an option to pay for the purchase using the Snap Mobile Payment process, eg, 204 .

[0043]

438 Referring to FIG. 2B , in some implementations, when the option to use the snapshot mobile payment process is selected, the merchant checkout webpage, such as 206, may provide a QR code, such as 209, through the browser application 205, which includes information about the virtual Information about the items in the shopping cart and merchant information for the payment network to process the purchase (eg, a private token/alias linked to the merchant's acquirer financial account).

443 In some implementations, the web page can be displayed by a secure display of the user's trusted computing device. For example, as a security measure, the position of the QR code frame within the display, such as 207, can be randomly changed to prevent snapshots of the QR code from being obtained by fraudulent means (eg, tampering with the trusted computing device). In some implementations, a security image pre-selected by the user, such as 208, can be displayed on the screen so that the user can verify that it is accurate. In some implementations, the image can be encrypted by SNAP before the image is provided to the trusted computing device. In some implementations, the trusted computing device may be the only device holding the decryption key needed to decrypt and successfully display the image to the user on the secure display.

[0044]

454 Referring to Figure 2C, in some implementations, such merchant product information including QR codes may be used by point-of-sale ("POS") terminals, such as 210a-b.

456 For example, in a brick-and-mortar store, when the user indicates that they wish to check out for items in the user's physical shopping cart, the POS terminal may display a QR code, such as 211a-b, which includes the

payment amount for the purchase, such as 212a-b. For example, the QR code may include data formatted according to Extensible Markup Language ("XML"), such as the following example data structure:

[0046]

463 Referring to Figure 2D, in some implementations, a user can use a smartphone (eg, 213) to obtain a snapshot of the QR code displayed on a secure display or screen of the POS terminal.

465 For example, the user's smartphone can run on it to detect and capture an application, e.g., 214, of the QR code (e.g., 216a).

467 For example, the user can use a registration feature, such as 215, to register the QR code within the smartphone's display. In some implementations, the application can provide the user with the ability to zoom in (eg, 217) or zoom out (eg, 218) the QR code to ensure that the image of the QR code fits the size of the smartphone's screen. The user will be able to use a user interface element such as 219 to obtain a snapshot of the QR code when it is QR coded within the smartphone's display. The user can cancel the snap mobile payment process using the user interface element 220 on the display of the smartphone.

[0047]

476 Referring to Figure 2E, in some implementations, when a snapshot of the merchant's product QR code is obtained, the user's smartphone can extract the product and merchant data stored within the QR code and use the The account number of the user's virtual wallet is used to generate a purchase transaction request for processing by the payment network.

480 Upon completion of processing the payment transaction by the payment network using information provided by the user's smartphone, merchant website 222 (via the browser application 221) may provide the user with a purchase receipt 225 . Referring to FIG. 2F , in an implementation in which the user uses the snapshot mobile payment process in a physical store, the POS terminal can display a purchase receipt for the user. In some implementations, the payment network can provide the buyer's receipt directly to the user's smartphone.

[0048]

489 3A-E show application user interface diagrams illustrating example components of the Snap mobile payment application for capturing product barcodes, securing user data, and preventing fraud, in some embodiments of the SNAP.

492 Referring to FIG. 3A , in some implementations, an application executing on a user's device may include an application interface that provides the user with various features. In some implementations, the application can be configured to recognize a product identifier (eg, barcode, QR code, etc.), such as 301 . For example, the application can be configured to capture merchant product QR codes for Snapshot mobile payment processing, as discussed above with reference to Figures 2A-F. In some implementations, the user may be required to log in to the application to activate its features. Once activated, the camera can provide the user with an in-person one-tap-to-buy feature. For example, the client device may have a camera through which the application can acquire images, video data, stream live video, etc., eg 303 . The application may be

configured to analyze input data and retrieve (eg 301) product identifiers, eg 304 , such as QR codes 209 , 211a - b , 216a and 227 . In some implementations, the application can overlay crosshairs, target boxes, and/or similar alignment reference marks, such as 305, so that the user can use the reference marks to align the product identifier, thereby aiding in the identification and identification of the product identifier. explain. In some implementations, the application may include an interface element to allow the user to toggle back and forth between the product identification mode and the product offer interface display screen (see, e.g., 306) so that the user can research exactly what is available to the user before capturing the product identifier. transaction. In some implementations, the application can provide the user with the ability to browse previous product identifier captures (see, eg, 307) so that the user will be able to better decide which product identifier the user wishes to capture. In some implementations, the user may wish to cancel the product purchase; the application may provide the user with a user interface element (eg, 308) to cancel the product identifier identification process and return to the previous interface screen the user was originally using. In some implementations, the user may be provided with information about products, user settings, merchants, offers, etc., such as in a list form (see, eg, 309), so that the user can better understand the user's purchase options. Various other features may be provided in application (see eg 310).

[0049]

518 Referring to FIG. 3B , in some implementations, the application may include an indication of the user's location (eg, name of the merchant store, geographic location, information related to aisles within the merchant store, etc.), such as 311 .

521 The application may provide an indication, eg 312, of the amount due for the product purchase. In some implementations, the application can provide the user with various options to pay for the purchase of the product. For example, the app may use GPS coordinates to determine the merchant's store where the user is located and direct the user to the merchant's website. In some implementations, SNAP may provide APIs to directly engage merchants to assist in transaction processing. In some implementations, a tagged merchant's SNAP application can be developed with SNAP functionality that can directly connect the user to the merchant's transaction processing system. For example, a user may select from a plurality of cards (eg, credit cards, debit cards, prepaid cards, etc.) from various card providers (eg, 313). In some implementations, the application may provide the user with an option to pay for the purchase amount using funds contained in the user's bank account, such as checking, deposit, money market, current account, etc. (eg, 314). In some implementations, the user can set default options through the application to set which card, bank account, etc. to use for the purchase transaction. In some implementations, the setting of such default options may allow the user to initiate the purchase transaction via a single click, tap, swipe, and/or other corrected user input action, such as 315a. In some implementations, when the user uses this option, the application can use the user's default settings to initiate the purchase transaction. In some implementations, the application allows the user to use other accounts (eg, Google checkout, Paypal account, etc.) to pay for the purchase, eg, 316 . In some implementations, the app allows the user to pay for the purchase using reward points, airline miles, hotel points, electronic coupons, printed coupons (e.g., by capturing printed coupons in a similar manner to product identifiers), etc. Transactions, eg 317-318. In some implementations, the application provides an option to provide quick authorization, eg, 319, before initiating the purchase transaction. In some implementations, the application can provide a progress indicator to provide an indication of the

progress of the transaction after the user has selected an option to initiate the purchase transaction, eg, 320 . In some implementations, the app can provide the user with historical information, eg, 321, about the user's previous purchases made through the app. In some implementations, the app can provide the user with options to share information about the purchase with other users (e.g., via email, SMS, wall post on , tweet on Twitter , etc.) and/or Controlling information shared with merchants, acquirers, payment networks, etc., to process the purchase transaction, e.g., 322.

549 In some implementations, the application may provide the user with an option to display product identification information captured by the client device (eg, to display the product information to a customer service representative upon leaving the store), such as 324. In some implementations, the user, application, device, and/or SNAP may encounter errors in processing. In this case, the user will be able to chat with a customer service representative (eg VerifyChat323) to resolve difficulties during the purchase transaction.

[0050]

557 In some implementations, the user may choose to use a one-time anonymous credit card number for the transaction, see eg 315b.

559 For example SNAP may use a set of pre-specified anonymous card details (see eg "AnonCard1", "AnonCard2"). As another example, a SNAP might generate a set of one-time bearer card details, eg in real time, to securely complete a purchase transaction (eg Anon It 1X). In such an implementation, the application may automatically set the user profile settings so that any personally identifying information of the user will not be provided to merchants and/or other entities. In some implementations, the user is required to enter a username and password to activate the bearer feature.

[0051]

568 Referring to FIG. 3C , in some implementations, the user interface elements of the Stories mobile payment application may advantageously be configured to provide the user with the ability to utilize custom payment parameters with a minimum number of user gestures applied to the user's mobile device. Ability to process purchases.

572 For example, a user may be provided with overloaded user interface elements, such as 325-326. For example, if the user has a QR payment code within the view of a camera included in the user's mobile device, the user can activate element 325 to take a snapshot of the QR code and use predetermined default settings to process the purchase based on the QR code . However, if the user wishes to customize payment parameters, the user may activate user interface element 326 (eg, press and hold continuously). In doing so, the application may provide a pop-up menu, eg, 327, that provides various payment customization options, such as those previously provided. For example, the user can drag the user's finger to the appropriate setting that the user likes, and release the user's finger from the touch screen of the user's mobile device to select that setting for payment processing. In alternative implementations, the payment settings options, such as 330, and QR capture activation buttons, such as 328a-b (such as 328b may provide even more settings than those displayed in the initial screen) may be combined with windows (such as 329) together in the user interface for capturing the QR code by the mobile device's camera. In an alternative implementation, the user's mobile

device can generate a hybrid QR code payment setup graphic, and the POS terminal (or user's trusted computing device) can capture the entire graphic for payment processing.

[0052]

589 Referring to Figure 3D, in some implementations, a user may advantageously be able to provide user settings in a device that generates a QR code for a purchase transaction, and then capture the QR code using the user's mobile device.

592 For example, a display device of a point-of-sale terminal may display a checkout screen, such as a web browser running on a client, eg 331, displaying a checkout web page, eg 332, of an online shopping website. In some implementations, a checkout screen may provide user interface elements, such as 333a-b, by which a user may indicate a desire to use Stories Mobile Payment. For example, if the user activates element 331a, the website can generate a QR code using the user's default settings and display the QR code (eg, 335) on the client's screen for the user to capture using the user's mobile device. In some implementations, the user can activate a user interface element, such as 333b, whereby the client can display a pop-up menu, such as 334, with additional options from which the user can select. For example, the website may provide the user with options similar to those discussed above in the description with reference to Figures 3B-C. In some implementations, the website can modify the QR code 335 in real time as the user modifies the settings provided by activating the user interface element 333b. Once the user has modified the settings using the pop-up menu, the user can capture a snapshot of the QR code to initiate the purchase transaction.

[0053]

607 Referring to FIG. 3E , in some implementations, SNAP can provide a user interface to the user to modify the user's snap mobile payment settings.

609 For example, the SNAP may provide a web interface, such as 341. For example, a user can use the web interface to modify the security settings, eg, 342, of the user's virtual wallet. For example, the user can browse a list of trusted devices, such as 344, through which the user can access the user's virtual wallet. In some implementations, the web interface can provide user interface elements to add trusted devices, such as 343 . The web interface may also provide users with additional security options. For example, the user can set a security password (e.g. 345), change settings regarding when the user should be asked before authorizing a purchase transaction (e.g. 346), the type/style of representation of the security feature (e.g. 347), and the Security image (eg 348) on the terminal used in Snapchat mobile payment. In various implementations, the user can access other services including modifying user profile, account number, account preferences, adding cards, getting offers and coupons, locating ATM machines, and the like.

[0054]

622 Figures 4A-D show data flow diagrams illustrating an example snap mobile payment process in some embodiments of the SNAP.

624 Referring to FIG. 4A, in some implementations, a user such as 401 may wish to purchase a product, service, offer, etc. (“Product”) from a merchant such as 403 through the merchant's online site or the merchant's

store. A user may communicate with a merchant server, e.g., 403, through a client, such as, but not limited to, a personal computer, mobile device, television, point-of-sale terminal, kiosk, ATM, etc. (e.g., 402). For example, a user may provide user input (eg, checkout input 411) into the client indicating that the user wishes to purchase a product. For example, a user in a merchant store may scan a product barcode for a product with a barcode scanner at a point-of-sale terminal. As another example, a user may select a product from a web catalog on a merchant website and add the product to a virtual shopping cart on the merchant website. The user may then indicate that the user wishes to checkout the items in the (virtual) shopping cart. The client may generate a checkout request, eg 412, and provide the checkout request (eg, 413) to the merchant server. For example, the client may provide the merchant server with a (secure) Hypertext Transfer Protocol ("HTTP(S)") GET message including product details in the form of data formatted according to Extensible Markup Language (XML). The following is an example HTTP(S) GET message for a merchant server including a checkout request in XML format:

[0056]

641 In some implementations, the merchant server can obtain the checkout request from the client and extract the checkout details (eg, XML data) from the checkout request.

643 For example, the merchant server may use a parser, such as the example parser discussed below with reference to FIG. 14 .

645 The merchant server can extract the product data as well as client data from the checkout request. In some implementations, the merchant server may query (e.g., 414) a merchant database (e.g., 404) to obtain product data (e.g., 415), such as product pricing, sales tax, offers, discounts, rewards, and/or other information to process the purchase trade. For example, the database may be a relational database responsive to Structured Query Language ("SQL") commands. The merchant server may execute a hypertext preprocessor ("PHP") script that includes SQL commands to query the database for product data. A list of exemplary PHP/SQL commands illustrating the substantive aspects of querying a database is provided below:

[0058]

655 In some implementations, in response to obtaining the product data, the merchant server may generate (eg, 416a) a QR payment code and/or secure display element according to the user's security settings (see, eg, 358).

658 The merchant server can provide the QR code to the client so that the client can display the QR code, and then the user can use the user's device to capture the QR code to obtain merchant and/or product data for generating a purchase transaction processing request .

661 In an alternative implementation, the merchant server may direct the client to communicate via an alternative communication protocol such as, but not limited to, Wi-Fi , Bluetooth , cellular network, SMS, email, and/or the like. The product and/or merchant data required to process the transaction to the user's device. For example, the merchant server may direct the client to initiate a plug-in on its system to provide an alternative communication service and transmit the product and/or merchant data to the user's device via the communication service.

[0059]

670 In implementations using QR codes, the merchant server may generate a QR code containing product information and merchant information required by the payment network to process the purchase transaction.

673 In some implementations, the QR code may include at least information required by the user device capturing the QR code to generate a purchase transaction processing request, such as a merchant identifier (e.g., merchant ID number, merchant name, store ID, etc.) and The session identifier for the user's shopping session associated with the store's website/store.

[0060]

680 In some implementations, the merchant server can generate in real-time a custom, user-specified merchant product XML data structure with a time-limited validity period, such as the exemplary "QR_data" XML data structure provided below:

[0062]

686 In some implementations, the XML data may include handles, aliases, tokens, or pointers to information stored on the payment network server, rather than encoding all the actual data needed to initiate the transaction for encoding into the QR code Information can advantageously be minimized.

689 In some implementations, the merchant can use the XML data to generate a QR code.

690 For example, the merchant server can use the PHP QR Code Open Source (LGPL) library available at http://phpqrcode.sourceforge.net/ for generating QR codes, 2D barcodes.

692 For example, the merchant server may issue PHP commands similar to the exemplary commands provided below:

[0063]

697 <?

698 PHP

[0064]

702 header('Content-Type: text/plain');

[0065]

706 //Create OR code image using data stored in Sdata variable

[0066]

710 QRoode::png(Sdata, 'qxcodeimg.png');

[0067]

714 ?

715 >

[0068]

719 In an alternative implementation, the merchant server may provide (eg, 416b) XML data with the request to the payment network server (eg, 406) to generate the QR code.

721 For example, the merchant server requests the generation of a QR code using an API call to the payment network server.

723 The payment network server may generate a QR code for the merchant server, eg, 416c, and provide (eg, 416d) the QR code to the merchant server.

725 For example, the payment network server may encode information provided by the merchant into the QR code, and may also advantageously include security information, time validity information, digital certificate information, bearer shipping messages, QR code generation/processing payment information, etc. encoded into that QR code.

[0069]

732 In some implementations, the payment network server provides the merchant server with encryption keys (eg, Rivest-Shamir-Adleman (RSA) private/public keys, digital certificates).

734 The merchant can use the encryption key to encrypt the custom, user-specific merchant product XML data structure to generate encrypted purchase data (eg, using the RSA algorithm).

736 The merchant server can then encode the encrypted data into a QR code. In various embodiments, the payment network server may advantageously employ this scheme to authenticate the merchant for any transaction processing request related to the user-merchant shopping session.

[0070]

742 In some implementations, the user device can be provided with a predesigned QR code associated with a verified, pre-authenticated merchant.

744 For example, a user may browse an online website on the user's device. The user device may generate an HTTP(S) GET request for a web page from a web server. In some implementations, the web server can generate a query for an advertisement to display on the web page in response to the user device's request for the web page. For example, a webpage server may retrieve a database or provide a request to an ad network server (eg, Akamai) to serve advertisements for embedding in the webpage. In some implementations, the ad network server may use keywords, metadata, etc. obtained from the webpage server (e.g., keywords or metadata associated with the webpage, user profile information, user ID, from the user's browsing history from cookies on that user's device, etc.). The advertising network may use the keyword to generate a query of

a database of advertisements associated with the keyword, and may obtain the advertisement to offer. In some implementations, the ad network server may provide (e.g., via an API call) information about such advertisements (e.g., merchant name, merchant ID, product name, product price information, related offers, etc.) to the payment network server . The payment network server may generate a QR code based on information provided by the ad network server so that a user device may take a snapshot of the QR code to initiate a communication with the QR code (e.g., provided to the payment network server by the ad network server) A purchase transaction of associated goods and/or services. The ad network server can provide the QR as part of the advertisement to the web server, which in turn can embed the advertisement including the QR code into the web page before serving the web page to the user device. In an alternative implementation, the ad network server/web server may transmit the URL or other identifier of the QR code (final) to the user device, and the user device may use the URL of the QR code (e.g., hosted on the payment web server) to generate a call (eg HTTP(S) GET request) to obtain the QR code and display it for the user.

[0071]

767 In some implementations, the merchant server can provide the QR code to the client, eg, 417.

768 For example, the merchant server may provide a hypertext markup language (“HTML”) page including references to the QR code image and/or secure element image, such as the following exemplary HTML page:

[0073]

773 In some implementations, the client can obtain the QR payment code (eg, 417) and display the QR code (eg, 418) on a display screen associated with the client device.

775 In some implementations, a user can use a user device, such as 405, to capture a QR code presented by the client device for payment processing.

777 For example, the user may provide a payment input into the user device such as 419. In various implementations, user input may include, but is not limited to, a single tap of a touchscreen interface (e.g., a single tap mobile app purchase embodiment), keypad entry, swiping a card, activating RFID-enabled/ Hardware devices with NFC (e.g., electronic cards with multiple accounts, smartphones, tablets, etc.), mouse clicks, button presses on joysticks/game consoles, voice commands, single taps/clicks on touch-sensitive interfaces Multi-touch gestures, touching user interface elements on touch-sensitive displays, and more. For example, a user device may obtain tracking data from a user card (e.g., credit card, debit card, prepaid card, charge card, etc.), such as the exemplary tracking data provided below:

[0075]

788 In some implementations, the user device can determine whether an image has been captured describing the QR code.

790 Depending on whether a QR code has been captured, and (optionally) also on the content of the QR code, the user device may redirect the user (e.g. via a web browser application executing on the user device) to: a product, a merchant website , products on the merchant's website, the website, and include commands to add items to the user's shopping cart associated with the website, etc.

794 For example, a user device may execute a component such as the exemplary quick response code processing ("QRCP") component 600 described below with reference to the discussion of FIGS. 6A-B .

[0076]

799 In some implementations, when user payment input is obtained and the QR code is captured, the user device can generate a card authorization request 420 for provision to the payment network server (e.g., if the QR code includes a purchase coupon, offer, send invoices, personal payments from another virtual wallet user, etc.).

803 For example, the user device may provide a card authorization request (eg 421) on behalf of the user, an HTTP(S) GET message (eg 406) including product order details for payment to the web server, in the form of data in XML format. The following is an exemplary HTTP(S) GET message for the payment network server including a card authorization request in XML format:

[0078]

810 In some implementations, the card authorization request generated by the user device may include the minimum information required to process the purchase transaction.

812 For example, this can improve the efficiency of communicating the purchase transaction request, and can also advantageously improve the privacy protection provided to the user and/or merchant.

814 For example, in some implementations, the card authorization request may include at least a merchant ID, a session ID for the user and merchant's shopping session, and a device ID of a user device (eg, a smartphone) linked to the user's virtual wallet. In some implementations, the QR code and message sent to/from the QR code capture device may include a source ID (e.g., an identifier of the device that generated the QR code), session ID, merchant ID, item ID (e.g., model number) , the checkout amount, and/or the transaction device ID (eg, the user's smart phone device).

[0079]

823 In some implementations, the card authorization request may be provided by the merchant server or point-of-sale terminal rather than the user device.

825 In some implementations, a security-desiring user may request a payment network server via the user device to dynamically generate the primary account number that will be used with the user in the purchase transaction.

[0080]

831 ("PAN", for example, a credit card number) along with the Card Verification Value Code (dCVVTM).

832 In response, the payment network server may generate a dCVV code (e.g., using random number generation, an MD5 hash of an input key, which may be generated using a user ID, merchant ID, session ID, timestamp, combinations thereof, etc.), and The user provides a session specific dCVVTM code to use with the user's PAN number. For example, session-specific dCVV codes may have an expiration time (eg,

expire within one minute from issue). The user device can communicate the PAN and dCVV (eg, via Bluetooth , NFC, Wi-Fi, cellular, QR code, etc.) to the point-of-sale terminal, which can create a card authorization request. For example, the user device may generate a QR payment code with the PAN and dCVV numbers embedded therein, and the point-of-sale terminal may snap a snapshot of an image of the QR payment code generated by the user device. The point-of-sale terminal can then generate and provide the card authorization request to the payment network server. The payment network server may then compare the dCVV obtained from the merchant to the dCVV provided to the user device before the purchase transaction was initiated to confirm the transaction. If the dCVV codes from the two sources (payment network server and merchant) correspond correctly to each other, then the payment network server can continue processing the purchase transaction.

[0081]

849 In some implementations, the card authorization request from the user device may include encrypted data extracted from the QR code, which may have been encrypted by the merchant server as part of a merchant authentication scheme.

852 In some implementations, the Pay Network Server may obtain encrypted data from a card authorization request provided by a user device and attempt to decrypt the encrypted data, for example, using an RSA private/public key that the Pay Network Server initially provided to the merchant The keys used by the server to encrypt the purchase data before embedding in the QR code are complementary. If the payment network server is able to decrypt the purchase data, the merchant is authenticated as a valid merchant. In some implementations, the payment network server can compare the purchase data decrypted from the card authorization with the data provided by the user/user device to determine whether the data from these different sources (user/user device, and merchant) are mutually correct. correspond. Thus, in some implementations, the payment network server can authenticate the merchant and associate the merchant with a particular user session or user device prior to processing the transaction.

[0082]

865 In some implementations, the payment network server may provide a notification to the user device that the transaction was verified and approved for the transaction.

867 In an alternative implementation, the payment network server may continue transaction processing. In some implementations, when the user is identified as being in a session with the merchant, the payment network server may communicate with the user device to provide the user with additional features. For example, in some implementations, the payment network server may provide communication with the user device (e.g., via an HTTP(S) POST message) to provide: the merchant's virtual storefront; A description of the merchant's aisle, a list of related items, etc. (see, eg, Figures 8E-G and the following description of additional embodiments).

[0083]

877 Referring to Figure 4B, in some implementations, the payment network server may process the transaction to

transfer purchase funds to an account stored on the merchant's acquirer.

879 For example, the acquirer may be a financial institution that maintains the merchant's account. For example, the results of transactions processed by the merchant may be deposited into an account maintained by the acquirer's server.

[0084]

885 In some implementations, the payment network server can generate a query, eg, 422, for the issuer server corresponding to the payment option selected by the user.

887 For example, a user's account may be linked to one or more issuing financial institutions ("issuers"), such as banking institutions, that issued the user's account. For example, such accounts include, but are not limited to, credit cards, debit cards, prepaid cards, checking, deposit, money market, certificates of deposit, savings (cash) value accounts, and the like. The publisher's publisher server, eg 4o8a-n, may hold user account details. In some implementations, a database such as payment network database 407 may store details of issuer servers associated with issuers. For example, the database may be a relational database responsive to Structured Query Language ("SQL") commands. The payment network server may query the payment network database for issuer server details. For example, the payment network server may execute a hypertext preprocessor ("PHP") script including SQL commands to query a database for details of the issuer server. A list of exemplary PHP/SQL commands illustrating the substantive aspects of querying a database is provided below:

[0086]

901 In response to obtaining the issuer server query, eg 422, the pay network database may provide the requested issuer server data to the pay network server, eg 423.

903 In some implementations, the payment network server can use the issuer server data to generate an authorization for each issuer server selected based on the predefined payment settings associated with the user's virtual wallet and/or the user's payment option input. request, such as 424, and provide card authorization requests, such as 425a-n, to the issuer server, such as 408a-n.

907 In some implementations, the authorization request may include details such as, but not limited to, costs to the user included in the transaction, user's card account details, user billing and/or shipping information, and the like. For example, the payment network server may provide an HTTP(S) POST message including an authorization request in XML format similar to the exemplary list provided below:

[0088]

914 In some implementations, the issuer server can parse the authorization request and based on the request details can query a database, such as user profile database 409a-n, for data associated with the account linked to the user.

917 For example, the publisher server may issue PHP/SQL commands similar to the examples provided below:

[0090]

921 In some implementations, after obtaining the user data, eg, 427a-n, the issuer server can determine whether the user can pay for the transaction with funds available on the account, eg, 428a-n.

923 For example, the issuer server may determine whether the user has sufficient balance remaining in the account, sufficient credit associated with the account, and the like.

925 Based on this determination, the issuer server may provide an authorization response to the payment network server, eg, 429a-n.

927 For example, the issuer server may provide an HTTP(S) POST message similar to the example above. In some implementations, if at least one issuer server determines that the user cannot pay for the transaction with available funds in the account, see, e.g., 430-431, then the payment network server may again request payment options from the user (e.g., by providing an authorization failure Message 431 to user equipment and request user equipment to provide new payment options), and retry the authorization of the purchase transaction. In some implementations, if the number of failed authorization attempts exceeds a threshold, the payment network server can exit the authorization process and provide an "authorization failed" message to the merchant server, user device, and/or client.

[0091]

938 Referring to Figure 4C, in some implementations, the payment network server may obtain an authorization message including notification of successful authorization, see eg 430, 433, and parse the message to extract authorization details.

941 When it is determined that the user has sufficient transaction funds, the payment network server may generate a transaction data record, such as 432, according to the authorization request and/or authorization response, and store details of the transaction and authorization regarding the transaction in the transaction database. For example, a payment web server could issue PHP/SQL commands similar to the following example listing to store transaction data in a database:

[0093]

949 In some implementations, the payment network server can forward the authorization success message, eg, 433a-b, to the user device and/or the merchant server.

951 The merchant can take this authorization message and determine from it that the user has sufficient funds in the card account to carry out the transaction.

953 The merchant server may add transaction records for the user to a batch of transaction data regarding authorized transactions. For example, the merchant may append XML data about the user's transactions to an XML data file, e.g., 434, including XML data for transactions that have been authorized for each user, and store the XML data file in a database (e.g., merchant database 404) , for example 435. For example, a batch XML data file could be of a structure similar to the sample XML data structure template provided below:

[0094]

961 <?

962 XML version="1.0" encoding="UTF-8"? >

[0095]

966 <merchant_data>

[0096]

970 <merchant_id>3FBCR4INC</merchant_id>

[0097]

974 <merchant_name>Books&Things, Inc.</merchant_name>

[0098]

978 <merchant_auth_key>lNNF484MCP59CHB27365</merchant_auth_key>

[0099]

982 <account_number>123456789</account_number>

[0100]

986 </merchant_data>

[0101]

990 <transaction_data>

[0102]

994 <transaction 1>

[0103]

998 . . .

[0104]

1002 </transaction 1>

[0105]

1006 <transaction 2>

[0106]

1010 . . .

[0107]

1014 </transaction 2>

[0108]

1018 .

[0109]

1022 .

[0110]

1026 .

[0111]

1030 <transaction n>

[0112]

1034 . . .

[0113]

1038 </transaction n>

[0114]

1042 </transaction data>

[0115]

1046 In some implementations, the server may also generate a purchase receipt, such as 434, and provide the purchase receipt to the client, such as 436.

1048 The client may render and display the purchase receipt for the user, eg 437a.

1049 In some implementations, the user device 405 may also provide a notification of successful authorization to the user, eg, 437b.

1051 For example, a client/user device may render web pages, electronic messages, text/SMS messages, buffer voicemails, sound ringtones, and/or play audio messages, etc., and provide output including, but not limited to: sound, music , audio, video, images, tactile feedback, vibration alerts (e.g., vibration-enabled client devices such as smartphones), and the like.

[0116]

1058 Referring to Figure 4D, in some implementations, the merchant server can initiate clearing of a batch of authorized transactions.

1060 For example, the merchant server may generate a batch data request, such as 438 , and provide the request, such as 439 , to a database such as merchant database 404 .

1062 For example, a merchant server may query a relational database using PHP/SQL commands similar to the examples provided above.

1064 In response to the batch data request, the database can provide, eg, 440, the requested batch data.

1065 The server may generate a batch clearing request, eg, 441, using the batch data obtained from the database, and provide (eg, 442) the batch clearing request to the acquirer server, eg, 410.

1067 For example, the merchant server may provide the acquirer server with an HTTP(S) POST message that includes batch data in XML format in the message body.

1069 The acquirer server may use the obtained batch clearing request to generate a batch payment request, such as 443 , and provide the batch payment request to the payment network server, such as 444 .

1071 The payment network server may parse the batch of payment requests and extract transaction data, eg, 445, for each transaction stored in the batch of payment requests.

1073 The pay network server may store transaction data, such as 446, for each transaction in a database, such as pay network database 407.

1075 For each extracted transaction, the pay network server may query a database, such as pay network database 407, eg 447-448, for the address of the issuer server.

1077 For example, a payment web server may use PHP/SQL commands similar to the examples provided above.

1078 The payment network server may generate a single payment request, eg, 449, for each transaction for which transaction data was extracted, and provide the single payment request (eg, 450) to the issuer server (eg, 408).

1081 For example, a payment web server may provide an HTTP(S) POST request similar to the following example:

[0118]

1086 In some implementations, the issuer server generates a generateable payment command, eg, 451.

1087 For example, the issuer server may issue a command to debit funds from a user's account (or add a charge to

a user's credit card account).

1089 The issuer server may issue a payment command (eg, 452) to a database, eg, user profile database 409, that stores the user account information.

1091 The issuer server may provide (eg, 453) the funds transfer message to the payment network server, which may forward (eg, 454) the funds transfer message to the acquirer server.

1093 An exemplary HTTP(S) POST funds transfer message is provided below:

[0119]

1097 POST/clearance.php HTTP/1.1

[0120]

1101 Host:www.acquirer.com

[0121]

1105 Content-Type: Application/XML

[0122]

1109 Content-Length:206

[0123]

1113 <?

1114 XML version="1.0" encoding="UTF-8"?

1115 >

[0124]

1119 <deposit_ack>

[0125]

1123 <request_ID>CNI4ICNW2</request_ID>

[0126]

1127 <clear_flag>true</clear_flag>

[0127]

<timestamp>2011-02-22 17:00:02</timestamp>

[0128]

<deposit_amount>$34.78</deposit_amount>

[0129]

</deposit_ack>

[0130]

In some implementations, the acquirer server can parse the funds transfer message and associate the transaction (eg, using the request_ID field in the example above) to the merchant.

The acquirer server may then transfer the funds specified in the funds transfer message to the merchant's account, eg, 455.

[0131]

Figures 5A-E show logic flow diagrams illustrating exemplary aspects of implementing Snap Mobile Payments, such as Snap Mobile Payment Execution ("SMPE") component 500, in some embodiments of SNAP.

Referring to Figure 5A, in some implementations, a user may wish to purchase a product, service, offer, etc. ("Product") from a merchant through the merchant's online site or in the merchant's store.

The user can communicate with the merchant server through the client.

For example, a user may provide user input (eg, 501) into the client indicating that the user wishes to checkout shopping items in a (virtual) shopping cart.

The client can generate a checkout request, such as 502, and provide the checkout request to the merchant server.

The merchant server may obtain a checkout request from the client, and extract checkout details (eg, XML data) from the checkout request, eg 503 .

For example, the merchant server may use a parser such as the example parser described below with reference to the discussion of FIG. 14 .

The merchant server extracts this product data along with the client data from the checkout request.

In some implementations, the merchant server may query (eg, 504) a merchant database to obtain product data, eg, 505, such as product prices, sales tax, offers, discounts, rewards, and/or other information to process the purchase transaction.

[0132]

In response to obtaining the product data, the merchant server may generate (eg, 506) a QR payment code

and/or secure display element (see, eg, 358) according to the user's security settings.

For example, the merchant server may generate a QR code containing product information and merchant information required by the payment network to process the purchase transaction.

For example, the merchant server may first generate a custom, user-specific merchant-product XML data structure with a time-limited validity period in real time, such as the exemplary "QR_data" XML data structure provided below:

[0135]

In some implementations, merchants can utilize XML data to generate QR codes.

For example, the merchant server can use the PHP QR Code Open Source (LGPL) library available at http://phpqrcode.sourceforge.net/ for generating QR codes, 2D barcodes.

For example, the merchant server may issue PHP commands similar to the exemplary commands provided below:

[0136]

<?

PHP

[0137]

header('Content-Type: text/plain');

[0138]

//Create QR code image using data stored in $data variable

[0139]

QRcode::png($data, 'qrcodeimg.png');

[0140]

?

>

[0141]

The merchant server can provide the QR payment code to the client, eg 506.

The client can obtain the QR payment code and display the QR code, eg 507, on a display screen associated with the client device.

1214 In some implementations, a user can use a user device, such as 509, to capture a QR code presented by the client device for payment processing.

1216 The client device can decode the QR code to extract the information embedded in the QR code.

1217 For example, a client device may use an application, such as the ZXing multi-format 1D/2D barcode image processing library available at http://code.google.com/p/zxing/, to extract information from the QR code.

1219 In some implementations, the user can provide payment input into the user device, eg, 508 .

1220 Upon obtaining user purchase input, the user device may generate a card authorization request, eg, 509, and provide the card authorization request to the payment network server.

[0142]

1225 Referring to Figure 5B, in some implementations, the payment network server can parse the card authorization request, eg, 510, and generate a query, eg, 511, for the issuer server corresponding to the payment option selected by the user.

1228 In some implementations, the payment network database may store details of issuer servers associated with issuers.

1230 In response to obtaining the issuer server query, the pay network database may provide, eg, 512, the requested issuer server data to the pay network server.

1232 In some implementations, the payment network server can use the issuer server data to generate authorization requests for each issuer server, eg, 425134, and provide the card authorization requests to the issuer servers.

[0143]

1238 In some implementations, the issuer server can parse the authorization request and, based on the details of the request, query the user profile database for data associated with the account linked to the user.

1240 In some implementations, upon obtaining the user data, the issuer server can determine whether the user can pay for the transaction with available funds in the account, eg, 517 .

1242 For example, the issuer server may determine whether the user has sufficient balance remaining in the account, has sufficient credit associated with the account, and the like.

1244 Based on this determination, the issuer server may provide an authorization response to the payment network server, eg, 518.

1246 In some implementations, if at least one issuer server determines (e.g., 519) that the user cannot pay for the transaction with available funds in the account, see e.g., 520, option "No," then the payment network server may again request payment options from the user (See eg 521, option "No", by providing an authorization failure message to the user equipment and requesting the user equipment to provide a new payment option), and retry the authorization of the purchase transaction. In some implementations, if the number of failed authorization attempts exceeds a threshold, see e.g. 521, option "Yes", then the payment network server may exit the authorization process and provide an "Authorization Failed" message to the merchant server, user device and /or client, eg 522.

[0144]

1257 In some implementations, the payment network server may obtain an authorization message including notification of successful authorization, see eg 520, option "Yes", and parse the message to extract authorization details.

1260 After determining that the user has sufficient transaction funds, the payment network server can generate transaction data records according to the authorization request and/or authorization response, such as 523, and store details of the transaction and authorization related to the transaction in the transaction database, such as 524 .

[0145]

1267 Referring to FIG. 5C , in some implementations, the payment network server may forward an authorization success message (eg, 525) to the user device and/or the merchant server, and sometimes through the acquirer server, eg, 526 .

1270 The merchant can parse the authorization message, eg 528, and from it determine that the user has sufficient funds in the card account to carry out the transaction, see eg 529. The merchant server may add a transaction record for the user to a batch of transaction data related to authorized transactions, see eg 530-531. In some implementations, the merchant server may also generate a purchase receipt, eg, 532, and provide the purchase receipt to the client. The client may render and display the purchase receipt, eg, 534, for the user. In some implementations, user device 405 may also provide a notification of successful authorization to the user.

[0146]

1280 Referring to Figures 5D-E, in some implementations, a merchant server can initiate clearing of a batch of authorized transactions.

1282 For example, the merchant server may generate a batch data request, such as 535, and provide the request (eg, 536) to a database, such as a merchant database. In response to the batch data request, the database can provide, eg, 536, the requested batch data. The server can use the batch data obtained from the database to generate a batch settlement request, eg 537, and provide the batch settlement request to the acquirer server. The acquirer server may generate (eg, 539) a batch payment request using the obtained batch clearing request and provide the batch payment request to the payment network server. The payment network server can parse the batch of payment requests and extract transaction data, eg, 540-542, for each transaction stored in the batch of payment requests. The pay network server may store the transaction data, eg 543-544, for each transaction in a database such as a pay network database. For each extracted transaction, the Pay Network Server may query (eg, 545-546) a database, such as a Pay Network Database, for the address of the Issuer Server. The payment network server may generate, eg, 547, a single payment request for each transaction for which transaction data was extracted, and provide the single payment request to the associated issuer server.

[0147]

1298 In some implementations, the issuer server can generate payment commands, eg, 548-549.

1299 For example, the issuer server may issue a command to debit funds from the user's account (or add a charge to the user's credit card account). The issuer server may issue the payment command to a database storing the user's account information (eg, a user profile database), eg, 549 . The issuer server may provide the funds transfer message to a payment network server, such as 551, that may forward the funds transfer message to the acquirer server. In some implementations, the acquirer server can parse the funds transfer message and associate the transaction (eg, using the request_ID field in the example above) to the merchant. The acquirer server may then transfer the funds specified in the funds transfer message to the merchant's account, eg, 553-555.

[0148]

1310 6A-B show logic flow diagrams illustrating example aspects of processing quick response codes, such as quick response code processing ("QRCP") component 600, in some embodiments of the SNAP.

1312 Referring to FIG. 6A , in some implementations, a virtual wallet application executing on a user device can determine whether a QR code has been captured in an image frame obtained by a camera operatively connected to the user device, and can also determine the QR code. The type and content of the code. Using this information, the virtual wallet application can redirect the user's user experience and/or initiate purchases, update aspects of the virtual wallet application, and the like. For example, the virtual wallet application may trigger the capture of image frames via a camera operatively connected to the user device, 601. The virtual wallet application can use an image segmentation algorithm to identify the foreground in the image, 602, and can crop the rest of the image to reduce background noise in the image, 603. The virtual wallet application can determine whether the foreground image includes a QR code from which data can be reliably read (e.g., if the image does not include a QR code, or if the QR code is partially cropped, blurred, etc. may not be reliably read fetch data), 604. For example, the virtual wallet application can use a code library, such as the ZXing multi-format 1D/2D barcode image processing library available at http://code.google.com/p/zxing/, to try and extract information. If the virtual wallet application can detect the QR code (605, option "yes"), the virtual wallet application can decode the QR code and extract data from the QR code. If the virtual wallet application cannot detect the QR code (605, option "No"), the virtual wallet application may attempt to perform optical character recognition on the image. For example, the virtual wallet application may perform optical character recognition, 606, using the Tesseract C++ open source OCR engine available at www.pixeltechnology.com/freewarw/tessnet2. The virtual wallet application can thus obtain the data encoded in the image and proceed if the data can be processed by the virtual wallet application. The virtual wallet application may query a database for the QR code type using the fields identified in the extracted data, 608. For example, the QR code may include invoices/bills, coupons, money orders (e.g., in P2P transfers), new account information packages, product information, purchase commands, URL navigation instructions, browser automated scripts, their combinations etc.

[0149]

1338 In some embodiments, the QR code may include data about the new account to be added to the virtual wallet application (see 609).

1340 The virtual wallet application may query the issuer of the new account (eg, obtained from the extracted data) for data associated with the new account, 610. The virtual wallet application may compare the data provided by the issuer with the data extracted from the QR code, 611. If the new account is confirmed (611, option "Yes"), the virtual wallet app can update the wallet credentials with the new account details, 613, and update the virtual wallet app's snapshot with data from the QR code History, 614.

[0150]

1348 Referring to FIG. 6B, in some embodiments, the QR code can include data (see 615) about bills, invoices, or coupons for purchases using the virtual wallet application, which can be queried with the virtual wallet application. The merchant associated with the purchase (as obtained from the extracted data) to query data associated with the bill, invoice, or coupon used for the purchase (e.g. offer details, offer ID, expiration time, etc. etc.), 616.

1353 The virtual wallet application can compare the data provided by the merchant with the data extracted from the QR code, 617. If the bill, invoice, or coupon for purchase is validated (618, option "Yes"), the virtual wallet application can generate a data structure that includes the QR code data (see, e.g., above referenced FIGS. 4-5 XML QR_data structure in the description of) to generate and provide a card authorization request, 619, and use the data from the QR code to update the snapshot history of the virtual wallet application 620.

[0151]

1362 In some embodiments, the QR code may include product information, commands, user navigation instructions, etc. for the virtual wallet application (see 621).

1364 The virtual wallet application can query a database of products using the information encoded in the QR. The virtual wallet application may provide various features including, but not limited to: displaying product information, redirecting the user to: a product page, a commerce website, a product page on a commerce website, adding items to a user's shopping cart on a commerce website, and the like. In some implementations, the virtual wallet application can perform a process such as that described above for any image frames that are pending and/or that the user selects for processing (eg, based on a snapshot history).

[0152]

1373 Figure 7 shows a user interface diagram illustrating an overview of example features of the virtual wallet application in some embodiments of the SNAP.

1375 FIG. 7 shows an illustration of various exemplary features of a virtual wallet mobile application 700 . Some of the features displayed include Wallet 701, Social Integration via TWITTER, FACEBOOK, etc., Quotes and Taxes 703, Snap Mobile Purchases 704, Alerts 705, and Security, Settings and Analytics 796. These features are explored in more detail below.

[0153]

1382 8A-G show user interface diagrams illustrating example features of the virtual wallet application in shopping mode, in some embodiments of the SNAP.

1384 Referring to Figure 8A, some embodiments of the virtual wallet mobile application help and greatly enhance the consumer's shopping experience. As shown in Figure 8A, the consumer has various shopping patterns available to peruse. In one implementation, for example, a user may initiate this shopping mode by selecting the store icon 810 at the bottom of the user interface. A user may search for and/or add items to the shopping cart 811 by typing items in the search field 812 . The user can also use the voice-activated shopping mode by speaking into the microphone 813 the name or description of the item to be retrieved and/or added to the shopping cart. In further implementations, the user may also select other shopping options 814 , such as current items 815 , billing 816 , address book 817 , merchants 818 and local proximity 819 .

[0154]

1395 In one embodiment, for example, a user may select option current item 815, as shown on the far left of the user interface of FIG. 8A.

1397 When the current item 815 option is selected, an intermediate user interface may be displayed. As shown, the middle user interface may provide a current list of items 815a-h in the user's shopping cart 811. A user may select an item, such as item 815a, to view product descriptions 815j for the selected item and/or other items from the same merchant. Price and total due information may also be displayed along with a QR code 815k that captures the information necessary to conduct a snap mobile purchase transaction.

[0155]

1405 Referring to FIG. 8B, in another embodiment, the user may select a billing 816 option.

1406 When the bill 816 option is selected, the user interface may display a list of bills and/or receipts 816a-h from one or more merchants. Additional information can be displayed next to each bill, such as date of visit, whether items from multiple stores are present, last bill payment date, automatic payment, number of items, etc. In one example, a wallet purchase statement 816a dated January 20, 2011 may be selected. The wallet shopping bill selection may display a user interface that provides various information about the selected bill. For example, the user interface may display a list of purchased items 816k, <<816i>>, the total number of items and corresponding values. For example, 7 items worth $102.54 are on the selected wallet shopping statement. Users can now select any item and select Buy Again to add purchases to that item. The user may also refresh offers 816j from the last time to clear any invalid offers and/or search for new offers that may be suitable for the current purchase. As shown in Figure 8B, the user may select two items for repeat purchases. Once added, a message 816i may be displayed to confirm the addition of both items, which yields the total number of items in the shopping cart 14.

[0156]

1421 Referring to Figure 8C, in yet another embodiment, the user may select the address book option 817 to browse the address book 817a, which includes a list of contacts 817b and make any transfers or payments.

1423 In one embodiment, the address book may identify each contact using the contact's name and available

and/or preferred payment modes. For example, contact Amanda G. Payment may be via social payment (eg, via FACEBOOK) as represented by icon 817c. In another example, money may be transferred to Brian S. via a QR code as represented by QR code icon 817d. In another example, Charles B. Payments may be accepted via near field communication 817e, Bluetooth 817f and email 817g. Payment can also be made via USB 817h (eg, through a physical connection of the two mobile devices) and other social channels such as TWITTER.

[0157]

1433 In one implementation, the user may select JoeP.

1434 to pay. As shown in the UI, next to the Joe P. next to his name, JoeP. Features an email icon 8i7g, representing Joe P. Payment via email is accepted. When his name is selected, the user interface may display his contact information, such as email, phone, and so on. If the user wishes to contact Joe P. payment, the user can add another transfer mode 817j to his contact information and make a payment transfer. Referring to Figure 8D, the user may be provided with a screen 817k where the user may enter an amount to send to Joe, and add other text to provide Joe with context for the payment transaction 817l. The user may select the mode by which Joe may be contacted (eg, SMS, email, social networking) through graphical user interface element 817m. As a user type, text input may also be provided for browsing within the GUI element 817n. When the user has finished entering the necessary information, the user can press the send button 817o to send the social message to Joe. If Joe also has a virtual wallet application, Joe will be able to browse 817p social payment messages within the application or directly on the website of the social network (such as Twitter , , etc.). Messages may be aggregated from various social networks as well as other sources (eg, SMS, email). The redemption method appropriate for each messaging method may be indicated along with the social pay message. In the illustration of FIG. 8D , the SMS 817q received by Joe indicates that Joe can redeem the $5 obtained via SMS by replying to the SMS and entering the hash tag value "#1234". In the same illustration, Joe has received a message 817r via that includes a URL link that Joe can activate to initiate a redemption of the $25 payment.

[0158]

1457 Referring to FIG. 8E, in some other embodiments, a user may select a merchant 818 from a list of options in a shopping mode to browse a selection list of merchants 818a-e.

1459 In one implementation manner, the merchants in the list may be in contact with the wallet, or have a relationship with the wallet. In another implementation, merchants may include a listing of merchants that meet user-defined or other criteria. For example, the list may be the one curated by the user, the merchant that the user shopped most frequently or spent more than x total amount of money, or shopped for three consecutive months, and the like. In one implementation, the user may further select a merchant, such as Amazon 818a. The user can then navigate through the merchant's listings to discover items of interest, such as 818f-j. Directly through the wallet and without accessing the merchant's site from a separate page, the user

can select items 818j from Amazon's 818a catalog. As shown at the far right of the user interface of Figure 8D, the selected item can then be added to the shopping cart. Message 818k indicates that the selected item has been added to the shopping cart, and the updated quantity of the item in the shopping cart is now 13.

[0159]

1472 Referring to Figure 8F, in one embodiment, there may be a local proximity option that may be selected by the user to browse a listing of businesses that are geographically in close proximity to the user.

1474 For example, the list of merchants 819a-e may be merchants located close to the user. In one implementation, the mobile application can further identify when the user is in the store based on the user's location. For example, location icon 819d may be displayed next to a store (eg, Walggreens) when the user is in close proximity to the store. In one implementation, the mobile application may periodically refresh its location if the user leaves the store (eg, Walgreens). In a further implementation, a user may navigate through the mobile application to offers of selected Walgreens stores. For example, a user may use the mobile application to navigate to items 819f-j available on aisle 5 at Walgreens. In one implementation, the user can select corn 819i to add to cart 819k from his or her mobile application.

[0160]

1485 Referring to FIG. 8G, in another embodiment, the local proximity option 819 may include a map of the store, particularly a real-time map feature.

1487 For example, when a Walgreens store is selected, the user may activate the aisle map 8191 that displays a map 819m showing the store organization and user location (indicated by yellow circles). In one implementation, a user can easily configure the map to add one or more other users (eg, the user's children) to share each other's locations within the store. In another implementation, the user may have the option to initiate a "store browsing" like street browsing in the map. Store Browsing 819n may display images/videos around the user. For example, if the user is about to enter hallway 5, the store browsing map may display a view of hallway 5. Additionally, the user can manipulate the orientation of the map using the navigation tool 8190 to move the store view forward, backward, right, left, and rotate clockwise and counterclockwise.

[0161]

1498 9A-F show user interface diagrams illustrating example features of the virtual wallet application in payment mode in some embodiments of SNAP.

1500 Referring to FIG. 9A , in one embodiment, the wallet mobile application can provide the user via wallet mode 910 with multiple options for payment transactions. In one implementation, an exemplary user interface 911 for making a payment is shown. The user interface can clearly identify the amount 912 and currency 913 used for the transaction. The amount may be an amount payable and the currency may include real currencies such as dollars and euros, and also virtual currencies such as reward points. The amount of the transaction 914 may also be prominently displayed on the user interface. The user may select the funds tab 916 to select one or more forms of payment 917, which may include various credit, debit, gift, reward, and/or prepaid cards. The user may also have the option to pay in whole or in part with reward points. For

example, a graphical indicator 918 on the user interface shows the number of points available, and the graphical indicator 919 shows the number of points that will be used against the amount due 234.56 and the value of the points in the selected currency (USD, for example). Equivalent to 920.

[0162]

1514 In one implementation, the user can combine funds from multiple sources to pay for the transaction.

1515 The amount 915 displayed on the user interface may provide an indication of the amount of total funds covered thus far by the selected form of payment (eg, Discover Card and reward points). The user may select another payment form or adjust the amount to be debited from one or more payment forms until the amount 915 matches the amount due 914 . Once the user has settled on the amount to be debited from one or more payment forms, payment authorization can begin.

[0163]

1523 In one implementation, the user may select security authorization for the transaction by selecting the hide button 922 to effectively hide or anonymize some (e.g., pre-configured) or all identifying information so that when the user selects the pay button 921, the transaction Authorization is done securely and anonymously.

1527 In another implementation, the user may select a payment button 921, which may use standard authorization techniques for transaction processing. In another implementation, when the user selects the social button 923, a message about the transaction can be passed to one or more social networks (established by the user), which can post or announce the purchase transaction in a social forum , such as a poster or tweet. In one implementation, a user may select a social payment processing option 923. This indicator 924 may show authorization and sending of social sharing data in progress.

[0164]

1536 In another implementation, a restricted payment mode 925 may be activated for certain purchasing activities, such as prescribed purchases.

1538 This mode can be activated according to rules defined by issuers, insurance companies, merchants, payment processors, and/or other entities to facilitate the processing of particular goods and services. In this mode, the user can scroll down the list of payment forms 926 by following the Funds tab to select a particular account, such as a Flexible Payment Account (FSA) 927, Health Savings Account (HAS), etc., and the account that will be credited to the selected account amount. In one implementation, this restricted payment mode 1925 process may prohibit social sharing of purchase information.

[0165]

1547 In one embodiment, through the input funds user interface 928, the wallet mobile application may facilitate the entry of funds.

1549 For example, a user who is unemployed can access unemployment benefits funds 929 through the wallet

mobile application. In one implementation, the entity providing these funds may also configure rules for using these funds, as indicated by process indicator message 930 . The wallet can read and apply the rule in advance, and can reject any purchases with the unemployment fund that fail to meet the criteria set by the rule. Exemplary criteria include, for example, Merchant Category Code (MCC), transaction time, transaction location, and the like. For example, a transaction with a grocery merchant with MCC 5411 is approved, while a transaction with a bar merchant with MCC 5813 is declined.

[0166]

1559 Referring to Figure 9B, in one embodiment, the wallet mobile application can facilitate dynamic payment optimization based on factors such as user location, preference, and currency value of preference.

1561 For example, when the user is in the United States, the country indicator 931 may display a flag for the United States and may set the currency 933 to be the United States. In further implementations, the wallet mobile application may automatically rearrange the order in which payment forms 935 are listed to reflect the popularity or acceptability of various forms of payment. In one implementation, the ranking may reflect user preferences, which cannot be changed by the wallet mobile application.

[0167]

1569 Similarly, when a German user operates a wallet in Germany, the mobile wallet application user interface can be dynamically updated to reflect the operations 932 and currency 934 of that country.

1571 In further implementations, the wallet application may be rearranged in order where different payment forms 936 are listed based on acceptance levels in that country. Of course, the order of these forms of payment can be changed by the user to suit his or her own preferences.

[0168]

1577 Referring to Figure 9C, in one embodiment, a Payee tab 937 in the Wallet mobile application user interface may assist the user in selecting one or more payees to receive the funds selected in the Funds tab.

1579 In one implementation, the user interface can display a list of all payees 938 with whom the user has previously transacted or is available for transacting. The user can then select one or more payees. Payees 938 may include larger merchants such as Amazon.com Corporation, and individuals such as Jane P. Doe. Next to each payee name may be displayed a list of payment modes accepted by that payee. In one implementation, the user may select Payee Jane P. Doe 939 to receive payment. Once selected, the user interface can display additional identifying information related to the payee.

[0169]

1588 Referring to FIG. 9D, in one embodiment, a mode tab 1940 may assist in selecting the payment modes accepted by the payee.

1590 Multiple payment modes are available for selection. Exemplary modes include, Bluetooth 941, Wireless 942, SnapMobile via user-obtained QR code 943, Security Chip 944, TWITTER 945, Near Field

Communication (NFC) 946, Cellular 947, SnapMobile via user-provided QR code 948, USB949 and FACEBOOK 950, etc. In one implementation, only payment modes accepted by the payee may be selected by the user. Other non-accepted payment modes may be prohibited.

[0170]

1598 Referring to FIG. 9E , in one embodiment, an offer tab 951 may provide real-time offers for user selection, which relate to items in the user's shopping cart.

1600 The user may select one or more offers from the list of applicable offers 952 for redemption. In one implementation, some offers can be combined while others cannot. When the user selects an offer that cannot be combined with other offers, unselected offers can be disabled. In another implementation, an offer recommended by the wallet application's recommendation engine may be identified by an indicator, such as that shown at 953 . In another implementation, the user can read the details of the quote by expanding the quote line, as shown at 954 in the user interface.

[0171]

1609 Referring to FIG. 9F , in one embodiment, social tags 955 can help integrate wallet applications with social channels 956 .

1611 In one implementation, a user may select one or more social channels 956 and may log in to select a social channel from the wallet application by providing a social channel username and password 957 to the wallet application and logging in 958 . The user can then use social buttons 959 to send or receive money through the integrated social channels. In another implementation, users can send socially shared data, such as purchase information or links, through integrated social channels. In another embodiment, user-supplied login credentials may allow SNAP to participate in intercept resolution.

[0172]

1620 Figure 10 shows a user interface diagram illustrating example features of the virtual wallet application in history mode, in some embodiments of the SNAP.

1622 In one embodiment, the user may select the history mode 1010 to browse the history of previous purchases and perform various actions on those previous purchases. For example, a user may enter merchant identifying information, such as name, product, MCC, etc., into the search bar 1011. In another implementation, the user can use the voice-activated retrieval feature by clicking on the microphone icon 1014 . The wallet application may query a storage area on the mobile device or elsewhere (eg, one or more databases and/or tables remote from the mobile device) for transactions matching the search keyword. The user interface can then display the results of the query, such as transaction 1015. The user interface may also identify the date 1012 of the transaction, the merchant and item 1013 involved in the transaction, the barcode of the receipt confirming that the transaction was made, the amount of the transaction, and any other relevant information.

[0173]

1635 In one implementation, a user may select a transaction, such as transaction 1015, to view details of that transaction.

1637 For example, the user can view details of items associated with the transaction and the amount 1016 of each item. In another implementation, the user can select the display option 1017 to view actions 1018 that the user can take with respect to the transaction or items in the transaction. For example, a user may add a photo to the transaction (eg, a picture of the user and the iPad the user purchased). In another implementation, if the user previously shared the purchase via a social channel, a post including the photo can be generated and sent to the social channel for publication. In one implementation, any sharing may be optional, and a user who does not share the purchase through social channels may still share the photo through one or more social channels he or she selects directly from the wallet application's history mode. In another implementation, the user can add the transaction to a group, such as user-created business expenses, household expenses, travel expenses, or other categories. Such a group can assist with year-end closing of expenses, submission of work expense reports, submission of value-added tax (VAT) refunds, personnel expenses, etc. In another implementation, the user may purchase one or more items purchased in the transaction. The user can then perform a transaction without going to the merchant's directory or site to discover the item. In another implementation, the user may also place one or more items in the shopping cart during the transaction for later purchase.

[0174]

1655 In another embodiment, the history mode may provide facilities for obtaining and displaying ratings 1019 for items in the transaction.

1657 The source of the rating can be the user, the user's friends (eg, from social channels, contacts, etc.), browsing aggregated from the webpage, and the like. In some implementations, the user interface may also allow users to post messages to other users of social channels (eg, TWITTER or FACEBOOK). For example, display area 1020 shows a FACEBOOK message exchange between two users. In one implementation, the user may share the link via message 1021 . The selection of such a message with a link embedded into the product may allow the user to browse the product's description and/or purchase the product directly from the history mode.

[0175]

1667 In one embodiment, the history mode may also include tools for outputting receipts.

1668 The output receipt popup 1022 may provide a number of options for outputting receipts for transactions in the history. For example, the user may use one or more options 1025 including save (to local removable storage, to server, to cloud account, etc.), print to printer, fax, email, etc. A user can use his or her address book 1023 to look up email or fax numbers for output. The user may also specify format options 1024 for outputting receipts. Exemplary format options include, but are not limited to: text files (.doc, .txt, .rtf, .iif, etc.), spreadsheets (.csv, .xls, etc.), image files (.jpg, .tff, . png, etc.), Portable Document Format (.pdf), Appendices (.ps), etc. The user can then click or tap output button 1027 to initiate receipt output.

[0176]

1678 11A-F show user interface diagrams illustrating example features of the virtual wallet application in snap mode, in some embodiments of the SNAP.

1680 Referring to FIG. 11A , in some embodiments, a user may select the snap mode 1101 to access the snap feature. In various embodiments, the virtual wallet application is able to snapshot and identify various items. For example, the virtual wallet application can snap and identify purchase invoices 1103, coupons 104, money (e.g., sent in person-to-person transfers) 1105, bills (e.g., utilities, etc.) 1106, receipts (e.g., for storage , expense report, etc.) 1107, payment account (eg, to add new credit/debit/prepaid card to the virtual wallet application) 1108. The user can return to the shopping screen at any time by activating the graphical user interface element 1102 . In some embodiments, the user can set the name of the shopping cart or wish list stored within the user's virtual wallet application to which the snapped items should be sent (see 1109). In some embodiments, the virtual wallet application may allow the user to create a new shopping cart or wish list to which the snapped items should be added.

[0177]

1693 In one embodiment, a user may select the snap mode 1110 to access its snap feature.

1694 The snap mode can handle any machine-readable data representation. Examples of such data may include linear and 2D barcodes, such as UPC codes and QR codes. These codes can be found on receipts, product packaging, etc. The snapshot mode can also process and manipulate pictures of receipts, products, offers, credit cards or other payment devices, and the like. FIG. 11A shows an exemplary user interface in snapshot mode. The user can use his or her mobile phone to take a picture of the QR code 1115 and/or barcode 1114. In one implementation, the bar 1113 and snapshot box 1115 can help the user to properly snap a snapshot of these codes. For example, as shown, snap frame 1115 does not capture all of code 1116 . Thus, the code captured in this browse is not parseable because the information in the code may be incomplete. This is indicated by a message on bar 1113 indicating that the snap mode is still looking for a code. The user can change the camera's zoom level 1117 to facilitate taking a snapshot of the QR code. When the code 1116 is fully framed by the snap box 1115, the message may be updated to read, for example, "Snapshot found." In one implementation, when the code is found, the user can use the mobile device camera to initiate code capture (see 1120). In another implementation, snapshot mode can automatically take a snapshot of the code using the mobile device camera (see 1119). In some implementations, the virtual wallet application can optionally apply a GPS tag (see 1118) to the QR code before storing it or using it in a transaction.

[0178]

1712 Referring to FIG. 11B , in one embodiment, the snap mode can facilitate payment redistribution posting transactions.

1714 For example, a user may purchase groceries and prescribed items from retailer Acme Supermarket. A user may inadvertently or for checkout convenience, for example, use his or her Visa card to pay for groceries and prescribed items. However, the user may have an FSA account that can be used to pay for prescribed items, and it will provide the user tax benefits. In this case, the user can use snapshot mode to initiate

transaction reallocation.

[0179]

1722 As shown, the user enters a search term (eg, billing) in the search bar 2121 .

1723 The user may then identify in tab 1122 the receipt 1123 that the user wishes to redistribute. Alternatively, the user can directly snap a picture of the barcode on the receipt, and the snapshot mode can generate and display the receipt 1123 using information from the barcode. Now the user can reassign 1125. In some implementations, the user may also challenge 1124 the transaction or file the receipt 1126.

[0180]

1730 In one implementation, when the reassign button 1125 is selected, the wallet application can perform optical character recognition (OCR) of the receipt.

1732 Each item in the receipt can then be reviewed to identify which payment device or account the item or items can be credited for taxes or other benefits such as cash back, reward points, and the like. In this example, there is a tax benefit if the prescription drug charged to the user's Visa card is charged to the user's FSA. The wallet application can then perform this reallocation as a finale. The reallocation process may include the wallet contacting the payment processor to credit the Visa card for the amount of the prescription drug and debit the same amount to the user's FSA account. In an alternative embodiment, a payment processor (eg, Visa or MasterCard) may obtain and OCR the receipt, identify the item and payment account for redistribution and perform the redistribution. In one implementation, the wallet application may request confirmation from the user to reallocate billing for the selected item to another payment account. Receipt 1127 may be generated after the reallocation process is complete. As discussed, the receipt shows that some charges have been moved from the Visa account to the FSA.

[0181]

1746 Referring to FIG. 11C , in one embodiment, snap mode can facilitate payment through payment codes such as barcodes or QR codes.

1748 For example, users can take a snapshot of the QR code of a transaction that has not yet been completed. The QR code can be displayed at a merchant POS terminal, website, or web application, and can be encoded with information identifying the item for purchase, merchant details, and other relevant information. When a user snaps such as a QR code, the snap mode can decode the information in the QR code and can use the decoded information to generate a receipt 1132 . Once the QR code is recognized, the navigation bar 1131 may indicate that the payment code is recognized. The user may now have the option to add to shopping cart 1133, pay with default payment account 1134 or pay with wallet 1135.

[0182]

1758 In one implementation, the user may decide to utilize a default 1134 payment.

1759 In this wallet example, the wallet application can then use the user's default payment method to complete the

purchase transaction. When the transaction is complete, a receipt can be automatically generated to prove the purchase. The user interface can also be updated to provide other options for processing completed transactions. Example options include social 1137 to share purchase information with others, redistribute 1138 as discussed with respect to FIG. 11B , and archive 1139 to store the receipt.

[0183]

1767 Referring to Figure 11D, in one embodiment, the snap mode can also help with quote identification, application and storage for future use.

1769 For example, in one implementation, a user can snap an offer code 1141 (eg, barcode, QR code, etc.). The wallet application can then generate offer text 1142 based on the information encoded in the offer code. Users can perform several actions on quote codes. For example, the user uses the lookup button 1143 to look up all merchants that accept the offer code, nearby merchants that accept the offer code, products from merchants that qualify for the offer code, and the like. The user can also use the add to cart button 1144 to apply the offer code to items currently in the shopping cart. Additionally, the user may also save the offer for future use by selecting the save button 1145 .

[0184]

1779 In one implementation, after an offer or coupon is applied 1146, the user may have the option to use a lookup to find eligible merchants and/or products, the user may enter the wallet using 1148, and the user may also save the offer Or Coupon 1146 for later use.

[0185]

1785 Referring to FIG. 11E , in one embodiment, the snapshot mode may also provide convenience for adding a funding source to the wallet application.

1787 In one implementation, payment cards such as credit cards, debit cards, prepaid cards, smart cards, and other payment accounts may have an associated code, such as a barcode or QR code.

1789 Such a code may have payment card information encoded therein including, but not limited to, name, address, payment card type, payment card account details, balance, spending limits, return balance, and the like. In one implementation, the code can be found on the face of the physical payment card. In another implementation, the code can be obtained by accessing an associated online account or another secure location. However, in another implementation, the code may be printed on the envelope accompanying the payment card. In one implementation, the user can snap a picture of the code. The wallet application can recognize the payment card 1151 and display textual information 1152 encoded in the payment card. The user can then perform verification of the information 1152 by selecting a verification button 1153 . In one implementation, the verification may include contacting the issuer of the payment card with information 1152 for confirmation of decoding, as well as any other relevant information. In one implementation, the user can add the payment card to the wallet by selecting the "Add to Wallet" button 1154 . Instructions to add a payment card to the wallet may cause the payment card to appear as one of the forms of payment for the funds tag 916 discussed with respect to FIG. 9A . The user may also cancel entering the payment card as

a funding source by selecting the cancel button 1155. When the payment card has been added to the wallet, the user interface may be updated to indicate completion of the entry via notification display 1156. The user can then access wallet 1157 to begin using the added payment card as a funding source.

[0186]

1808 Referring to FIG. 11F , in some implementations, the virtual wallet application can identify a product by processing the QR code, and can provide information related to the product, as well as information related to purchasing the product, ancillary services, and the like.

1811 For example, the virtual wallet application may provide a window 1161 in which the virtual wallet application may display images, product descriptions, prices, merchant information, etc. (see 1162). In some implementations, the virtual wallet application can provide a QR code that includes the displayed information so that another user can quickly snap the information to enter it into another virtual wallet application. In some implementations, the virtual wallet application can provide features so that the user can request doorman services (e.g., help when shopping), shipping services (e.g., so the user can leave the store without carrying the item out)), 1164. In some implementations, the virtual wallet application can provide competitive prices from local merchants (eg, using the GPS location of the user device) or merchants on the Internet (see 1165). In some implementations, the virtual wallet application can provide users with features including but not limited to: browse previous stories, snap new codes, add GPS tags to codes, retrieve codes from earlier stories to use, manually Enter information about the QR code, attribute the QR code to an object (eg so that for organizational purposes QR codes for furniture products for the home can be grouped into a "bedroom furniture" object), etc. (see 1166). In some embodiments, the user can set the name of the shopping cart or wishlist stored within the user's virtual wallet application to which the snapped items should be sent (see 1167). In some embodiments, the virtual wallet application may allow the user to create a new shopping cart or wish list to which the snapped items should be added.

[0187]

1830 Figure 12 shows a user interface diagram illustrating example features of the virtual wallet application in offer mode in some embodiments of the SNAP.

1832 In some implementations, SNAP may allow users to retrieve offers for products and/or services from within the virtual wallet mobile application. For example, a user may enter text into graphical user interface ("GUI") element 1211, or issue a voice command by activating GUI element 1212 and speaking the command into the device. In some implementations, SNAP may provide an offer based on the user's previous behavior, demographics, current location, current shopping cart selections or purchased items, and the like. For example, if a user is in a physical store, or an online shopping site, and leaves the (virtual) store, the merchant associated with the store may wish to provide an enticement process to entice the customer to return to the (virtual) store. A merchant may provide 1213 such an offer. For example, the offer can offer a discount and can include an expiration time. In some implementations, other users can offer a gift (eg, 1214) to the user that the user can redeem. In some implementations, the offer section may include warnings about payment of outstanding funds to other users (e.g., 1215). In some implementations, the offer section can include a warning (eg, 1216) about requesting receipts of funds from other users. For example,

such features may identify funds that are receivable from other applications (eg, mailings, calendars, tasks, notes, reminders, alerts, etc.), or by manual input by the user into the virtual wallet application. In some implementations, the offers section may provide offers from participating merchants in SNAP, eg, 1217-1219, 1220. These offers can sometimes be aggregated using a combination of participating merchants, eg 1217. In some implementations, SNAP itself can provide offers, eg, 1220, for users to use with a particular form of payment from within the virtual wallet application.

[0188]

1853 13A-B show user interface diagrams illustrating exemplary features of the virtual wallet application in security and privacy mode, in some embodiments of SNAP.

1855 Referring to FIG. 13A , in some implementations, the user can view and/or change the user profile and/or the user's settings, such as by activating a user interface element. For example, a user can view/modify username (eg, 1311a-b), account number (eg, 1312a-b), user security access code (eg, 1313-b), user pin (eg, 1314-b), user address (eg, 1315 -b), social security number associated with the user (e.g. 1316-b), current device GPS location (e.g. 1317-b), user account at the merchant where the user is currently located (e.g. 1318-b), user's return Account (eg 1319-b), etc. In some implementations, the user can select which data fields and their associated values should be transmitted to facilitate the purchase transaction, thus providing the user with enhanced data security. For example, in the exemplary illustration in FIG. 13A, the user has selected Name 1311a, Account Number 1312a, Security Code 1313a, Merchant Account ID 1318a, and Rewards Account ID 1319a as fields to be sent as part of the notification to process the purchase transaction . In some implementations, the user can socket the fields and/or data values sent as part of the notification to process the purchase transaction. In some implementations, the application may provide the user with multiple screens of data fields and/or stored associated values to select as part of the purchase order transmission. In some implementations, the application can provide SNAP with the user's GPS location. Based on the user's GPS location, SNAP can determine the user's environment (eg, whether the user is in a store, doctor's office, hospital, post office, etc.). Based on the circumstances, the user application may present the appropriate fields to the user from which the user may select fields and/or field values to send as part of the purchase order transmission.

[0189]

1876 For example, a user may walk into a doctor's office and wish to pay for co-pays for a doctor's appointment.

1877 In addition to basic transaction information, such as account number and name, the application can provide users with the ability to choose to transfer medical records, health information, which can be provided to medical providers, insurance companies, and transaction processors to reconcile between the parties pay. In some implementations, the records can be sent and encrypted in a data format compliant with the Health Insurance Act for Portability and Obligation (HIPAA), and only recipients authorized to view such records can have the appropriate decryption key to decrypt and view the records. Private User Information.

[0190]

1886 Referring to Figure 13B, in some implementations, an application executing on the user's device may provide a "VerifyChat" feature for fraud prevention.

1888 For example, SNAP can detect unusual and/or suspicious transactions. The SNAP can use the Verifychat feature to communicate with the user and verify the authenticity of the originator of the purchase transaction. In various implementations, SNAP can send email messages, text (SMS) messages, messages, Twitter tweets, text chats, voice chats, video chats (eg, Apple FaceTime), etc. to communicate with the user. For example, SNAP may initiate a video inquiry, e.g., 1321, for the user. For example, a user may need to present himself/herself via video chat, eg 1322. In some implementations, a customer service representative, such as agent 1324, can use the user's video to manually determine the user's authenticity. In some implementations, SNAP may use facial, biometric, etc. recognition methods (eg, using pattern classification techniques) to determine the user's identity. In some implementations, the application can provide fiducial markers (eg, crosshairs, target boxes, etc.) such as 1323 so that the user can provide video to aid in the automatic identification of the user's SNAP. In some implementations, the user may not have initiated the transaction, eg, the transaction was fraudulent. In this implementation, the user can cancel the query. SNAP may then cancel the transaction, and/or initiate a fraud investigation process on behalf of the user.

[0191]

1906 In some implementations, SNAP may use a text challenge process to determine the user's authenticity, e.g., 1325.

1908 For example, SNAP may communicate with users via text chat, SMS messages, emails, messages, Twitter tweets, and the like. SNAP can ask the user to ask questions, such as 1326. The application may provide user input interface elements (eg, virtual keyboard 1328) to answer query questions posed by SNAP. In some implementations, the inquiry question can be automatically and randomly selected by SNAP; in some implementations, a customer service representative can communicate with the user manually. In some implementations, the user may not have initiated the transaction, eg, the transaction was fraudulent. In this implementation, the user can cancel the text query. SNAP can then cancel the transaction, and/or initiate the fraud investigation process on behalf of the user.

[0192]

1920 SNAP controller

[0193]

1924 FIG. 14 shows a block diagram illustrating an embodiment of a SNAP controller 1401 .

1925 In this embodiment, the SNAP controller 1401 can be used to aggregate, process, store, retrieve, serve, identify, command, generate, match, and/or facilitate interaction with computers through various techniques, and/or other related data.

[0194]

1931 Typically, users such as 1433a, which may be people and/or other systems, may engage information technology systems (eg, computers) to aid in information processing.

1933 In contrast, a computer employs a processor to process information; such a processor 1403 may be referred to as a central processing unit (CPU).

1935 One form of processor is known as a microprocessor. The CPU uses communication circuits to communicate binary-coded signals, which act as instructions to allow various operations. These instructions may be operations and/or data containing and/or referencing other instructions and data in various accessible processor and operable storage areas 1429 (e.g., registers, cache memory, random access memory, etc.) instruction. Such communicated instructions may be stored and/or transmitted in batches (eg, batches) of program and/or data components to facilitate desired operations. These stored instruction codes, such as programs, may engage CPU circuit elements and other motherboard and/or system components to perform desired operations. One type of program is a computer operating system, which may be executed by the CPU on a computer; the operating system allows and assists users in accessing and operating computer information technology and resources. Some of the resources that can be employed in an information technology system include: the input and output mechanisms through which data can be moved into and out of a computer; memory in which data can be saved; and processors through which information can be processed. These information technology systems can be used to collect data for later retrieval, analysis, and manipulation, which can be assisted by database programs. These information technology systems provide interfaces that allow users to access and operate various system elements.

[0195]

1953 In one embodiment, SNAP controller 1401 may be connected to and/or communicate with entities such as, but not limited to: one or more users from user input device 1411; peripheral device 1412; optional encryption process device 1428; and/or communication network 1413.

1956 For example, SNAP controller 1401 may connect to and/or communicate with users, such as 1433a, running client devices, such as 1433b, including but not limited to personal computers, servers, and/or various mobile devices, including but not Limited to cellular phones, smart phones (such as phones based on the Android operating system, etc.), tablet computers (such as Apple iPadTM, HP SlateTM, Motorola XoomTM, etc.), eBook readers (such as Amazon KindleTM, Barnes and Noble's NookTMeReader etc.), laptops, notebooks, netbooks, game consoles (such as XBOX LiveTM, DS, Sony Portable, etc.), portable scanners, etc.

[0196]

1970 Networks are generally considered to include the interconnection and interoperation of clients, servers, and intermediate nodes in a graph topology.

1972 It should be noted that the term "server" is used throughout this application to generally refer to a computer, other device, program, or combination thereof, that processes and responds to requests from remote users across a communications network. Servers use their information to make requests to "clients". As used herein, the term "client" generally refers to a computer, program, other device, user, and/or combination thereof that is capable of processing and generating requests and obtaining and processing any responses from servers across a communication network. Computers, other devices, programs, or combinations thereof that facilitate information processing and requests, and/or send pieces of information from a source user to a target user, are commonly referred to as "nodes." Networks are generally thought of as facilitating the transfer of information from source to destination. Specifically, nodes that perform the task of pushing pieces of information from sources to destinations are often referred to as "routers." There are many forms of networks such as local area networks (LANs), piconets, wide area networks (WANs), wireless networks (WLANs), and so on. For example, the Internet is generally accepted as an interconnection of networks whereby remote clients and servers can access and interoperate with each other.

[0197]

1988 SNAP controller 1401 may be computer system based, which may include, but is not limited to, components such as computer system 1402 connected to memory 1429 .

[0198]

1993 computer system

[0199]

1997 Computer system 1402 may include clock 1430, central processing unit ("CPU" and/or "processor" (these terms are used interchangeably throughout this disclosure unless noted to the contrary)) 1403, memory 1429 (e.g., read-only memory (ROM) 1406, random access memory (RAM) 1405, etc.), and/or interface bus 1407, and almost often, though not necessarily, all interconnected and/or via one or more The transmission circuit path (the system bus 1404 on the (mother) board 1402 through which instructions (eg, binary coded signals) can be transmitted to achieve communication, operation, storage, etc.).

2003 The computer system may be connected to a power supply 1486; for example, the power supply may optionally be internal.

2005 Optionally, cryptographic processor 1426 and/or transceiver (eg, IC) 1474 may be connected to the system bus.

2007 In another embodiment, cryptographic processors and/or transceivers may be connected as internal and/or external peripherals 1412 via interface bus I/O. The transceiver, in turn, can be connected to the antenna 1475, thereby enabling wireless transmission and reception of various communications and/or sensor protocols; for example, the antenna can be connected to: Texas Instruments WiLink WL1283 transceiver chip (e.g., provides 802.11n, Bluetooth 3.0 , FM, Global Positioning System (GPS) (thus allowing the SNAP

controller to determine its location)); BroadcomBCM4329FKUBG transceiver chip (for example, providing 802.11n, Bluetooth 2.1+EDR, FM, etc.); BroadcomBCM4750IUB8 receiver chip (For example, GPS); Infineon Technologies X-Gold 618-PMB9800 (for example, providing 2G/3G HSDPA/HSUPA0 communication), etc. A system clock typically has a crystal oscillator and generates a reference signal through the circuit paths of the computer system. Clocks are typically connected to the system bus and various clock multipliers that increase or decrease the base operating frequency for other components interconnected in the computer system. The clock and various components in a computer system drive the signals that carry out information throughout the system. This sending and receiving of instructions to effectuate information throughout a computer system may generally be referred to as a communication. These communication instructions may also be transmitted, received, and caused to return and/or respond to communications beyond the example computer system to: communication networks, input devices, other computer systems, peripheral devices, and the like. It should be understood that in alternative embodiments, any of the above-described components may be connected directly to each other, to the CPU, and/or organized in numerous variations as exemplified by various computer systems.

[0200]

2029 The CPU includes at least one high-speed data processor sufficient to execute program components for executing user- and/or system-generated requests.

2031 The processor itself will often include various specialized processing units such as, but not limited to: integrated system (bus) controllers, memory management control units, floating point units, and even specialized processing subunits like graphics processing units, digital signal processing unit, etc. In addition, the processor may include internal fast-access addressable memory, and be able to map and address memory 1429 outside of the processor itself; memory may include, but is not limited to: fast registers, various levels of cache memory (e.g., 1, 2 , Level 3, etc.), RAM, etc. A processor can access these memories by using a storage address space accessible through an instruction address, which the processor can construct and decode, allowing it to access a circuit path to a specific storage address space with a stored state. The CPU can be a microprocessor such as: AMD's Athlon, Duron and/or Opteron; ARM's application, embedded security processor; IBM and/or Motorola's DragonBall and PowerPC; IBM and Sony's Cell processor; Intel's Celeron , Core(2)Duo, Itanium, Pentium, Xeon, and/or Xscale processors. The CPU interacts with the memory by passing instructions according to conventional data processing techniques across conductive and/or transmission channels (eg (printed) electronic and/or optical circuits) to execute stored instructions (in other words, program code). This command passing facilitates communication within the SNAP controller and out across various interfaces. If processing requirements dictate greater speed and/or capacity, distributed processor (eg, distributed SNAP), mainframe, multi-core, parallel, and/or supercomputer architectures may similarly be employed. Alternatively, a small personal digital assistant (PDA) can be used if the configuration needs dictate greater portability.

[0201]

2052 Depending on the particular implementation, the features of SNAP may be implemented by implementing a microcontroller such as CAST's R8051XC2 microcontroller, Intel's MCS 51 (ie, 8051 microcontroller), or

the like.

2055 Also, to implement certain features of SNAP, some feature implementations may rely on embedded components such as: Application Specific Integrated Circuits (“ASICs”), Digital Signal Processing (“DSPs”), Field Programmable Gate Arrays (“FPGAs”) , and/or similar embedded technologies. For example, any SNAP component set (distributed, etc.) and/or features may be implemented by a microprocessor and/or implemented by embedded components; for example, by an ASIC, coprocessor, DSP, FPGA, etc. Alternatively, some implementations of SNAP may be implemented with embedded components configured and used to implement various features or signal processing.

[0202]

2065 Depending on the particular implementation, embedded components may include software solutions, hardware solutions, and/or a combination hardware/software solutions.

2067 For example, the SNAP features discussed herein can be implemented by implementing an FPGA, which is a semiconductor device containing programmable logic elements called "logic blocks," and programmable interconnects, such as high-performance FPGAs from the Virtex family and/or low-level FPGAs produced by Xilinx. Cost Spartan series. After the FPGA is fabricated, the logic blocks and interconnects can be programmed by the customer or designer to implement any SNAP features. A hierarchy of programmable interconnects allows logic blocks to be interconnected as desired by the SNAP system designer/administrator, somewhat like a single programmable breadboard. The logic blocks of the FPGA can be programmed to perform operations on basic logic gates, such as AND and XOR, or more complex combinational operators such as decoders or simple math operations. In most FPGAs, logic blocks also include storage elements, which may be circuit flip-flops or more complete blocks of memory. In some cases, SNAPs can be developed on regular FPGAs and then ported to fixed versions that more closely resemble ASIC implementations. Alternative or cooperative implementations may migrate the SNAP controller features to the final ASIC instead of the FPGA, or migrate the SNAP controller features to the final ASIC in addition to the FPGA. According to all implementations of the aforementioned embedded components, a microprocessor may be envisaged as the "CPU" and/or "processor" for the SNAP.

[0203]

2085 power supply

[0204]

2089 The power supply 1486 may be any standard form used to power small electronic circuit board devices, such as the following batteries: alkaline, lithium hydride, lithium ion, lithium polymer, nickel cadmium, solar cells, and the like.

2092 Other types of AC or DC power sources may also be used.

2093 In the case of a solar cell, in one embodiment, the case provides an aperture through which the solar cell can capture photon energy. The battery 1486 is connected to at least one subsequent component of the interconnected SNAP, thereby providing electrical current to all subsequent components. In one example,

power supply 1486 is coupled to system bus unit 1404 . In an alternative embodiment, external power 1486 is provided through a connection through the I/O 1408 interface. For example, USB and/or IEEE 1394 connections carry data and power across the connection and are thus suitable power sources.

[0205]

2102 interface adapter

[0206]

2106 Interface bus 1407 accepts, connects, and/or communicates to a number of interface adapters, although generally not necessarily in the form of adapter cards, such as, but not limited to: input output interface (I/O) 1408, storage interface 1409, network interface 1410 etc.

2109 Optionally, cryptographic processor interface 1427 may similarly be connected to the interface bus.

2110 The interface bus provides communication of the interface adapters with each other and with other components of the computer system. Interface adapters are available for compatible interface buses. Interface adapters are usually connected to the interface bus through a slot structure. Conventional socket architectures can be used such as, but not limited to: Accelerated Graphics Port (AGP), Card Bus, (Extended) Industry Standard Architecture ((E)ISA), Micro Channel Architecture (MCA), NuBus, Peripheral Component Interconnect (Extended) (PCI(X)), PCI passthrough, Personal Computer Memory Card International Association (PCMCIA), etc.

[0207]

2120 The storage interface 1409 can accept, transfer, and/or connect to a plurality of storage devices, such as but not limited to: the storage device 1414, removable disk devices, and the like.

2122 The storage interface may employ connectivity protocols such as, but not limited to: (Ultra) (Serial) Advanced Technology Attachment (Packet Interface) ((Ultra) (Serial) ATA (PI)), (Enhanced) Integrated Drive Electronics ((E)IDE), Institute of Electrical and Electronics Engineers (IEEE) 1394, Fiber Channel, Small Computer System Interface (SCSI), Universal Serial Bus (USB), etc.

[0208]

2129 The network interface 1410 can accept, communicate and/or connect to a communication network 1413 .

2130 Through the communication network 1413, the SNAP controller is accessible by a user 1433a through a remote client 1433b (eg, a computer with a web browser). The network interface may employ connection protocols such as, but not limited to: direct connect, Ethernet (thick, thin, twisted pair 10/100/1000 10/100/1000Base T, etc.), token ring, such as IEEE8o2.11a- x wireless connection, etc. If processing requirements dictate greater overall speed and/or capacity, a distributed network controller (eg, distributed SNAP), fabric may similarly be employed to aggregate, load balance, and/or increase the communication bandwidth required by the SNAP controller. The communication network can be any one and/or combination of the following: direct interconnection; Internet; local area network (LAN); metropolitan area

network (MAN); operational mission as a node on the Internet (OMNI);); wireless network (eg, employing protocols such as but not limited to: Wireless Application Protocol (WAP), I-mode, etc.), etc. A network interface can be viewed as a specialized form of an input-output interface. Additionally, multiple network interfaces 1410 may be used to interface with various communication network types 1413 . For example, multiple network interfaces may be employed to allow communication via broadcast, multicast, and/or unicast networks.

[0209]

2147 Input output interface (I/O) 1408 accepts, communicates and/or connects to user input device 1411, peripheral device 1412, cryptographic processor device 1428, and the like.

2149 I/O can employ connection protocols such as but not limited to: Audio: Analog, Digital, Monaural, RCA, Stereo, etc.; Data: Apple Desktop Bus (ADB), IEEE 1394a-b, Serial, Universal Serial Bus (USB); infrared; joystick; keyboard; midi; optical; PC AT; PS/2; parallel; radio; video interface: Apple Desktop Connector (ADC), BNC, coaxial, component, composite, digital, DVI (DVI), High Definition Multimedia Interface (HDMI), RCA, RF Antenna, S-Video, VGA, etc.; Wireless Transceivers: 802.11a/b/g/n/x; Bluetooth; Cellular (e.g., Code Division Multi Address (CDMA), High Speed Packet Access (HSPA(+)), High Speed Downlink Packet Access (HSDPA), Global System for Mobile Communications (GSM), Long Term Evolution (LTE), WiMax, etc.); etc. A typical output device may include a video display, typically comprising a cathode ray tube (CRT) or liquid crystal display (LCD) based monitor, with an interface (such as DVI circuitry and cable) to accept a signal from a video interface. The video interface synthesizes information generated by the computer system and generates a video signal in a video storage frame based on the synthesized information. Another output device is a television, which accepts the signal from the video interface. Typically, the video interface provides composite video information through a video connection interface that accepts a video display interface (eg, an RCA composite video connector that accepts an RCA composite video cable; a DVI connector that accepts a DVI display cable, etc.).

[0210]

2167 User input device 1411 is often a type of peripheral device 1412 (see below) and may include: card reader, dongle, fingerprint reader, gloves, graphics tablet, joystick, keyboard, microphone, mouse, remote control , retina reader, touch screen (eg, capacitive, resistive, etc.), trackball, trackpad, sensor (eg, accelerometer, ambient light, GPS, gyroscope, proximity, etc.), stylus wait.

[0211]

2174 Peripherals 1412 may be connected to and/or communicated to I/O and/or other similar equipment, such as a network interface, storage interface, direct-to-interface bus, system bus, CPU, and the like.

2176 Peripherals can be external, internal and/or part of the SNAP controller.

2177 Peripherals can include: antennas, audio devices (e.g., line-in, line-out, microphone-in, speakers, etc.), cameras (e.g., still, video, webcam, etc.), dongles (e.g., for copying protection, use of digital signatures to ensure secure transactions, etc.), external processors (for additional capacity; e.g., encryption device 1428),

force feedback devices (e.g., vibrating motors), network interfaces, printers, scanners, storage devices, transceivers sensors (eg, cellular, GPS, etc.), video equipment (eg, goggles, monitors, etc.), video sources, helmets, etc. Peripherals often include various types of input devices (eg, video cameras).

[0212]

2186 It should be noted that while user input devices and peripherals may be employed, the SNAP controller may be embodied as an embedded, dedicated and/or monitor-less (ie headless) device where access will be provided via a network interface connection.

[0213]

2192 Cryptographic units, such as, but not limited to, microcontrollers, processors 1426, interfaces 1427, and/or devices 1428, can be attached to and/or communicate with the SNAP controller.

2194 An MC68HC16 microcontroller manufactured by Motorola may be used in and/or within the encryption unit.

2196 The MC68HC16 microcontroller uses 16-bit multiply and add instructions in a 16 MHz configuration and takes less than 1 second to execute 512-bit RSA private key operations. The cryptographic unit supports authentication of communications from interactive agents as well as allowing bearer transactions. The encryption unit can also be configured as part of the CPU. Equivalent microcontrollers and/or processors could also be used. Other commercially available dedicated encryption processors include: Broadcom's CryptoNetx and other security processors; Ncipher's nShield, SafeNet's Luna PCI (e.g., 7100) series; Semaphore Communication's 40MHz Roadrunner 184; Sun's encryption accelerator (e.g., Accelerator 6000PCIe Board, Accelerator 500Daughtercard); Via nanoprocessor (eg, L2100, L2200, U2400) line capable of executing 500+MB/s encrypted instructions; VLSI Technology's 33MHz 6868, etc.

[0214]

2208 memory

[0215]

2212 In general, any mechanism and/or embodiment that allows a processor to store and/or retrieve information can be considered memory 1429 .

2214 However, memory is an alternative technology and resource, and thus multiple memory embodiments may be employed in place of each other or in combination.

2216 It should be understood that various forms of memory 1429 may be employed by the SNAP controller and/or computer system. For example, a computer system may be configured in which the operation of the on-chip CPU memory (e.g., registers), RAM, ROM, and any other storage devices is provided by a paper punched tape or paper punched card mechanism; however, such an embodiment would result in Very slow operating speed. In a typical configuration, memory 1429 will include ROM 1406 , RAM 1405 , and storage device 1414 . Storage device 1414 may be any conventional computer system memory. Storage devices may

include drums; magnetic disk drives (fixed and/or removable); magneto-optical drives; optical drives (i.e., Blu-ray, CD/ROM/RAM/Recordable (R)/Writable (RW), DVD R/ RW, HD DVD R/RW, etc.); device arrays (e.g., redundant array of independent disks (RAID)); solid-state memory devices (USB memory, solid-state drive (SSD), etc.); other processor-readable storage media ; and/or other similar devices. Therefore, computer systems generally require and use memory.

[0216]

2230 parts set

[0217]

2234 Memory 1429 may contain a collection of program and/or database components and/or data such as, but not limited to: operating system component 1415 (operating system); information server component 1416 (information server); user interface component 1417 (user interface); Web browser component 1418 (web browser); database 1419; mail server component 1421; mail client component 1422; encryption server component 1420 (encryption server);

2239 These components may be stored and accessed from a storage device and/or from a storage device accessible through an interface bus.

2241 Although non-traditional program components, such as those of a collection of components, are typically stored in local storage device 1414, they may also be loaded and/or stored in storage devices such as peripheral devices, RAM, memory in remote storage facilities.

[0218]

2247 operating system

[0219]

2251 Operating system components 1415 are executable program components that facilitate operation of the SNAP controller.

2253 Typically, an operating system facilitates access to I/O, network interfaces, peripherals, storage devices, and so on.

2255 Operating systems can be highly fault-tolerant, scalable, and secure systems such as Apple Macintosh computer OS X (Server); AT&T Plan 9; Be OS; Unix and Unix-like system distributions (such as AT&T's UNIX; Berkley Software Distribution Program (BSD) variants, such as FreeBSD, NetBSD, OpenBSD, etc.; Linux distributions, such as Red Hat, Ubuntu, etc.); and/or similar operating systems. However, more restricted and/or less secure operating systems such as Apple Macintosh computer OS, IBM OS/2, Microsoft DOS, Microsoft Windows2000/2003/3.1/95/98/CE/Millenium/NT/ Vista/XP (server), Palm OS, etc. The operating system can communicate unidirectionally and/or bidirectionally with other components in the component set, including itself, and the like. The operating system most often communicates with other program components, user interfaces, and/or the like. For example, an operating system may contain,

communicate, generate, obtain, and/or provide program component, system, user, and/or data communications, requests, and/or responses. Once executed by the CPU, the operating system may allow interaction with communication networks, data, I/O, peripherals, program components, memory, user input devices, and the like. The operating system may provide a communication protocol that allows the SNAP controller to communicate with other entities over the communication network 1413 . The SNAP controller can use various communication protocols as the subcarrier transport mechanism for interaction, such as but not limited to: multicast, TCP/IP, UDP, unicast, etc.

[0220]

2274 information server

[0221]

2278 Information server component 1416 is a stored program component that is executed by the CPU.

2279 The information server may be a traditional Internet information server, such as but not limited to Apache based on Apache software, Internet information server of Microsoft Corporation, and the like.

2281 The Information Server may allow the execution of program components through facilities such as: Active Server Pages (ASP), ActiveX, (ANSI) (Objective-)C(++), C# and/or . NET, Common Gateway Interface (CGI) Scripting, Dynamic (D) Hypertext Markup Language (HTML), FLASH, Java, JavaScript, Practical Extractable Reporting Language (PERL), Hypertext Preprocessor (PHP), Pipeline, Python, Wireless Application Protocol (WAP), WebObjects, etc. The information server may support secure communication protocols such as, but not limited to: File Transfer Protocol (FTP); Hypertext Transfer Protocol (HTTP); Hypertext Transfer Protocol Secure (HTTPS), Secure Sockets Layer (SSL), messaging protocols (e.g. America Online Services (AOL) Instant Messenger (AIM), Application Exchange (APEX), ICQ, Internet Multithreaded Chat (IRC), Microsoft Networks (MSN) Messenger Service, Protocol for Presence and Instant Messaging (PRIM), Internet Engineering Task Force's (IETF's) Session Initiation Protocol (SIP), SIP for Instant Messaging and Presence Impact Extensions (SIMPLE), the open XML-based Extensible Messaging and Presence Protocol (XMPP) (i.e. Jabber or Open Mobile Alliance's (OMA's) Instant Messaging and Presence Service (IMPS), Yahoo! Instant Messenger Service, etc. The information server provides results in the form of web pages to the web browser and allows controlled generation of web pages through interaction with other program components. After the Domain Name System (DNS) resolved portion of the HTTP request is resolved to a particular Information Server, the Information Server resolves the request for information at the specified location on the SNAP Controller based on the remainder of the HTTP request. For example, a request such as http://123.124.125.126/myInformation.html may have the IP portion of the request "123.124.125.126", which resolves to an information server at that IP address through a DNS server; that information server may in turn resolve http request for the "/mylnformation.html" portion of the request and resolve it to a location in memory containing the information "mylnformation.html". In addition, other information used as a protocol can be employed across various ports, eg, FTP communication across ports, etc. The information server can communicate unidirectionally and/or bidirectionally with other components in the component set, including itself, and/or the like. Most information servers communicate constantly with the SNAP database 1419, operating system,

other program components, user interfaces, web browsers, and the like.

[0222]

2310 Access to the SNAP database can be achieved through a number of database bridging mechanisms, such as through scripting languages (eg, CGI) as listed below and through inter-application communication channels as listed below (eg, CORBA, WebObjects, etc.).

2313 Any data request by the web browser is parsed by the bridging mechanism into the appropriate syntax as required by SNAP. In one embodiment, the information server will provide a web form accessible by a web browser. An entry in a web form that is filled into a provided field is marked as having been entered into a particular field and is parsed accordingly. The entered terms are then passed along with the field labels, which instruct the parser to generate queries directed to the appropriate tables and/or fields. In one embodiment, based on the marked text entries, the parser can generate queries in standard SQL fashion by instantiating search strings with appropriate join/select commands, where the resulting commands are provided to SNAP as queries via a bridging mechanism. When query results are generated according to the query, the results are passed via the bridging mechanism and can be parsed by the bridging mechanism for formatting and generation of new result web pages. This new resulting web page is then provided to the information server, which can serve it to the requesting web browser.

[0223]

2327 Likewise, an information server may contain, communicate, generate, obtain, and/or provide program component, system, user, and/or data communications, requests, and/or responses.

[0224]

2332 user interface

[0225]

2336 Computer interfaces are similar in some respects to automotive operating interfaces.

2337 Automotive operating interface elements such as the steering wheel, transmission, and speedometer facilitate the access, operation, and display of vehicle resources and status.

2339 Computer interactive interface elements such as checkboxes, cursors, menus, scrollers, and windows (collectively and often referred to as widgets) similarly facilitate access, capacity, operation of data and computer hardware and operating system resources and state , and display.

2342 The operator interface is often called the user interface. Graphical User Interface (GUI) provides the baseline and means to graphically access and display information to the user, GUI such as Aqua of the Apple Macintosh computer operating system, OS/2 of International Business Machines Corporation, Windows 2000/2003/3.1/95 of Microsoft Corporation /98/CE/Millenium/NT/XP/Vista/7 (i.e. Aero), X-Windows for Unix (which may include, for example, additional Unix graphical interface libraries and layers such as the K Desktop Environment (KDE), mythTV, and GNU Network Object Model Environment (GNOME)), web

interface libraries (for example, ActiveX, AJAX, (D)HTML, FLASH, Java, JavaScript, etc., interface libraries such as but not limited to, Dojo, jQuery (UI), MooTools, Prototype, script.aculo.us, SWFObject, Yahoo UI, whatever can be used).

[0226]

2354 User interface component 1417 is a stored program component executed by the CPU.

2355 The user interface may be, for example, a conventional graphical user interface provided by and/or on top of the already discussed operating system and/or operating environment. A user interface may allow display, execution, interaction, processing, and/or operation of program components and/or system facilities through textual and/or graphical facilities. A user interface provides a facility by which a user can implement, interact with, and/or operate a computer system. A user interface can communicate unidirectionally and/or bidirectionally with other components within a component set, including itself, and/or the like. Most of the user interface often communicates with the operating system, other program components, and so on. The user interface may contain, communicate, generate, obtain and/or provide program component, system, user, and/or data communications, requests, and/or responses.

[0227]

2367 browser

[0228]

2371 Web browser component 1418 is a stored program component executed by the CPU.

2372 The web browser may be a conventional hypertext browsing application such as Microsoft Internet Explorer or Netscape Navigator.

2374 Secure web browsing can be provided over HTTPS, SSL, etc. utilizing 128-bit (or more) encryption. Web browsers allow the execution of program components through facilities such as ActiveX, AJAX, (D)HTML, FLASH, Java, JavaScript, web browser plug-in APIs (eg, FireFox, Safari Plug-in, etc. APIs), etc. Web browsers and similar information access tools can be integrated into PDAs, cell phones, and/or other mobile devices. A user's web browser can communicate unidirectionally and/or bidirectionally with other components within a component component set, including itself, and/or similar facilities. Most web browsers frequently communicate with information servers, operating systems, integrated program components (such as plug-ins), etc.; for example, it may contain, transmit, generate, obtain and/or provide program components, systems, users and/or data Communications, Requests and/or Responses. Also, instead of a web browser and an information server, a combined application can be developed to perform similar operations of both. Composite applications similarly implement retrieval of information from SNAP-enabled nodes and provision of information to users, user agents, etc. The composite application may be non-trivial on systems employing standard web browsers.

[0229]

2390 Mail Server

[0230]

2394 The mail server component 1421 is a stored program component executed by the CPU 1403 .

2395 The mail server may be a conventional Internet mail server, such as but not limited to sendmail, Microsoft Exchange, and the like.

2397 The mail server may allow the execution of program components through facilities such as ASP, ActiveX, (ANSI) (Objective-)C(++), C#_ and/or . NET, CGI scripts, Java, JavaScript, PERL, PHP, pipes, Python, WebObjects, etc. The mail server can support communication protocols, such as but not limited to: Internet Message Access Protocol (IMAP), Message Application Programming Interface (MAPI)/Microsoft Exchange, post office protocol (POP3), Simple Mail Transfer Protocol (SMTP) and the like. The mail server may route, forward and process incoming and outgoing mail messages that have been sent, relayed and/or traversed through and/or to the SNAP.

[0231]

2407 Access to SNAP mail can be accomplished through multiple APIs provided by individual web server components and/or operating systems.

[0232]

2412 Also, a mail server may contain, communicate, generate, obtain, and/or provide program component, system, user, and/or data communications, requests, information, and/or responses.

[0233]

2417 mail client

[0234]

2421 Mail client component 1422 is a stored program component executed by CPU 1403 .

2422 The mail client can be a traditional mail browsing application, such as: Apple Mail, Microsoft Entourage, Microsoft Outlook, Microsoft Outlook Express, Mozilla, Thunderbird, etc.

2424 The mail client can support multiple transfer protocols, such as: IMAP, Microsoft Exchange, POP3, SMTP, etc.

2426 The mail client can communicate unidirectionally and/or bidirectionally with other components in the component set, including itself, and/or the like.

2428 Most mail clients routinely communicate with mail servers, operating systems, other mail clients, etc.; for example, it may contain, deliver, generate, obtain and/or provide program components, system, user and/or data communications, requests, Information and/or Responses. Mail clients typically provide facilities to compose and transmit e-mail messages.

[0235]

2435 encrypted server

[0236]

2439 Crypto server component 1420 is a stored program component executed by CPU 1403, crypto processor 1426, crypto processor interface 1427, crypto processor device 1428, and the like.

2441 A cryptographic processor interface would allow acceleration of encryption and/or decryption requested by the cryptographic element; however, the cryptographic element could alternatively run on a conventional CPU.

2444 Cryptographic elements allow encryption and/or decryption of provided data. Cryptographic elements allow symmetric and asymmetric (eg, Pretty Good Protection (PGP)) encryption and/or decryption. The encryption technology that can be used by the encryption element is such as but not limited to: digital certificate (for example, X.509 authentication framework), digital signature, double signature, envelope, password access protection, public key management and so on. Cryptographic elements will facilitate many (encryption and/or decryption) security protocols such as but not limited to: checksum, Data Encryption Standard (DES), Elliptic Curve Cryptography (ECC), International Data Encryption Algorithm (IDEA), message Digest (MD5, which is a form of hashing), Cipher, Rivest Cipher (RC5), Rijndael, RSA (which is an Internet encryption and authentication system using an algorithm developed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977), Secure Hash Algorithm (SHA), Secure Sockets Layer (SSL), Secure Hypertext Transfer Protocol (HTTPS), etc. Using these encrypted security protocols, SNAP can encrypt all incoming and/or outgoing communications and can utilize wider communication networks as nodes within a Virtual Private Network (VPN). The cryptographic element facilitates the processing of "security authorization", whereby access to resources is prohibited by security protocols, wherein the cryptographic element implements authorized access to secure resources. Additionally, the cryptographic element may provide a unique identifier of the content, for example using and MD5 hashing to obtain a unique signature for a digital audio file. A cryptographic element may communicate unidirectionally and/or bidirectionally with other components within a component set, including itself, and/or the like. The cryptographic element supports cryptographic mechanisms that allow secure transmission of information across communication networks to allow SNAP components to engage in secure transactions, if desired. The cryptographic element facilitates secure access to resources on SNAP and facilitates access to secure resources on remote systems; ie it can act as a client and/or server to secure resources. Most cryptographic components often communicate with information servers, operating systems, other program components, etc. The cryptographic element may contain, communicate, generate, obtain, and/or provide program component, system, user, and/or data communications, requests, and/or responses.

[0237]

2472 SNAP database

[0238]

2476 The SNAP database component 1419 can be embedded in the database and the data it stores.

2477 The database is a stored program component, which is executed by the CPU; the stored program component configures the CPU in part to process the stored data.

2479 The database may be a traditional, fault-tolerant, relational, scalable, secure database, such as Oracle or Sybase. Relational databases are an extension of flat files. A relational database consists of a series of related tables. Tables are joined to each other by key fields. The use of key fields allows tables to be combined through indexes relative to the key fields; that is, the key fields serve as dimensional pivots for the combined information of the various tables. Relationships typically identify links between tables by means of matching primary keys. A primary key represents a field that uniquely identifies a table row in a relational database. More precisely, they uniquely identify table rows on the "one" side of a one-to-many relationship.

[0239]

2489 Alternatively, SNAP databases can be implemented using various standard data structures, such as arrays, hashes, (linked) lists, structures, structured text files (eg XML), tables, etc.

2491 These data structures can be stored in memory and/or in (structure) files. In another alternative, an object-oriented database such as Frontier, ObjectStore, Poet, Zope, etc. can be used. An object database may comprise a plurality of object collections grouped and/or linked by common attributes; they are related to other object collections by some common attributes. Object-oriented databases perform similarly to relational databases, except that their objects are not just pieces of data, but can have other types of functionality encapsulated within a given object. The use of SNAP database 1419 may be integrated into another component, such as SNAP component 1435, if the SNAP database is implemented as a data structure. Likewise, databases can be implemented as a mix of data structures, objects, and relational structures. Databases can be consolidated and/or distributed in myriad variations by standard data processing techniques. Parts of the database, such as tables, may be exported and/or imported and thus decentralized and/or integrated.

[0240]

2505 In one embodiment, the database component 1419 includes several tables 1419a-o.

2506 The user table 1419a may include fields such as, but not limited to: user_id, ssn, dob, first_name, last_name, age, state, address_firstline, address_secondline, zipcode, devices_list, contact_info, contact_type, alt_contact_info, alt_contact_type, and the like. A user form may support and/or track multiple entity accounts on SNAP. The device table 1419b may include fields such as, but not limited to: device_ID, device_name, device_IP, device_MAC, device_type, device_model, device_version, device_OS, device_apps_list, device_securekey, wallet_app_installed_flag, and the like. The Apps table 1419c may include fields such as, but not limited to: app_ID, app_name, app_type, app_dependencies, and the like. Account table 1419d may include fields such as, but not limited to: account_number, account_security_code, account_name, issuer_acquirer_flag, issuer_name, acquirer_name, account_address, routing_number, access_API_call, linked_wallets_list, and the like. Merchant table 1419e

may include fields such as, but not limited to: merchant_id, merchant_name, merchant_address, ip_address, mac_address, auth_key, port_num, security_settings_list, etc. Issuer table 1419f may include fields such as, but not limited to: issuer_id, issuer_name, issuer_address, ip_address, mac_address, auth_key, port_num, security_settings_list, and the like. The acquirer table 1419g may include fields such as, but not limited to: account_firstname, account_lastname, account_type, account_num, account_balance_list, billingaddress_linei, billingaddress_line2, billing_zipcode, billing_state, shipping_preferences, shippingaddress_linei, shippingaddress_line2, shipping_zipcode, etc.

2523 The payment gateway table 1419b may include fields such as, but not limited to: gateway_ID, gateway_IP, gateway_MAC, gateway_secure_key, gateway_access_list, gateway_API_call_list, gateway_services_list, and the like. Transaction table 1419i may include fields such as but not limited to: order_id, user_id, timestamp, transaction_cost, purchase_details_list, num_products, products_list, product_type, product_params_list, product_title, product_summary, quantity, user_id, client_system_id, client_ip, client_type, client_atversion_moding ,app_installed_flag,user_id,account_firstname,account_lastname,account_type,account_num,account_priority_account_ratio,billingaddress_linei,billingaddress_line2,billing_zipcode,billing_state,shipping_preferences,shippingaddress_linei,shippingaddress_line2,shipping_zipcode,shipping_state,merchant_id,merchant_name,merchant_auth_key等。 The batch table 1419j may include fields such as, but not limited to: batch_id, transaction_id_list, timestamp_list, cleared_flag_list, clearance_trigger_settings, and the like. Ledger table 1419k may include fields such as, but not limited to: request_id, timestamp, deposit_amount, batch_id, transaction_id, clear_flag, deposit_account, transaction_summary, payor_name, payor_account, and the like.

2537 Products table 14191 may include fields such as, but not limited to: product_ID, product_title, product_attributes_list, product_price, tax_info_list, related_products_list, offers_list, discounts_list, rewards_list, merchants_list, merchant_availability_list, and the like. The offer form 1419m may include fields such as, but not limited to: offer_ID, offer_title, offer_attributes_list, offer_price, offer_expiry, related_products_list, discounts_list, rewards_list, merchants_list, merchant_availability_list, and the like. The behavior data table 1419n may include fields such as but not limited to: user_id, timestamp, activity_type, activity_location, activity_attribute_list, activity_attribute_values_list, and the like. Analysis table 1419o may include fields such as, but not limited to: report_id, user_id, report_type, report_algorithm_id, report_destination_address, and the like.

[0241]

2549 In one embodiment, the SNAP database can interact with other database systems.

2550 For example, using a distributed database system, query and data access by retrieving SNAP components can handle the combination of SNAP database, integrated data security layer database as a single database entity.

[0242]

2555 In one embodiment, the user program may contain various user interface primitives that may be used to update SNAP.

2557 Likewise, various accounts may require custom database tables depending on the environment in which

SNAP may need to serve, as well as the type of client. It should be noted that any unique field can be specified as the key field throughout. In an alternative embodiment, these tables have been dispersed into their own databases and their respective database controllers (ie, a single database controller for each of the above tables). Using standard data processing techniques, one can further distribute the database via several computer systems and/or storage devices. Similarly, by consolidating and/or distributing the various database components 1419a-o, the configuration of decentralized database controllers may be changed. SNAP can be configured to track various settings, inputs and parameters through the database controller.

[0243]

2568 The SNAP database can communicate unidirectionally and/or bidirectionally with other components within the component set, including itself, and/or similar facilities.

2570 Most SNAP databases communicate frequently with SNAP components, other program components, and the like. A database may contain, maintain and provide information about other nodes and data.

[0244]

2575 SNAP

[0245]

2579 SNAP component 1435 is a stored program component executed by the CPU.

2580 In one embodiment, a SNAP component includes any and/or all combinations of aspects of SNAP discussed in the preceding figures.

2582 Thus, SNAP implements the access, acquisition and provision of information, services, transactions, etc. across various communication networks.

[0246]

2587 The SNAP component can convert real-time generated merchant-product quick response codes into virtual wallet card-based transaction purchase notifications, etc. and use of SNAP through the SNAP component.

2589 In one embodiment, the SNAP component 1435 takes input (e.g., checkout input 411; product data 414; payment input 419; issuer server data 423; user data 427a-n, etc.) and transforms the input through the SNAP component (e.g., SMPE 1441; QRCP 1442, etc.) are outputs (eg, QR payment code 417; card authorization request 421; authorization response 429a-n; authorization success message 433a-b; batch additional data 435; purchase receipt 436, etc.).

[0247]

2597 SNAP components that allow information access between nodes can be developed using standard development tools and languages such as, but not limited to: Apache components, Assembly, ActiveX, executable binary, (ANSI) (Objective-)C (++), C #_and / or.

2600 NET, database adapters, CGI scripts, Java, JavaScript, drawing tools, procedural and object-oriented development tools, PERL, PHP, Python, shell scripts, SQL commands, web application server extensions, web development environments and libraries (e.g., Microsoft Corporation ActiveX; Adobe AIR, FLEX&FLASH; AJAX; (D)HTML; Dojo, Java; JavaScript; jQuery (UI); MooTools; etc.), WebObjects, etc. In one embodiment, the SNAP server employs an encryption server to encrypt and decrypt communications. A SNAP element can communicate unidirectionally and/or bidirectionally with other components within a component set, including itself, and/or the like. Most SNAP components constantly communicate with SNAP databases, operating systems, other program components, and so on. A SNAP may contain, communicate, generate, obtain and/or provide program component, system, user and/or data communications, requests and/or responses.

[0248]

2613 Distributed SNAP

[0249]

2617 The structure and/or operation of any SNAP node controller component can be combined, merged and/or distributed in any number of ways to aid in development and/or configuration.

2619 Similarly, component sets can be combined in any number of ways to aid deployment and/or development.

2620 To achieve this, components can be integrated into a common code base or into a facility where components can be dynamically loaded in an integrated fashion on demand.

[0250]

2625 Component sets can be combined and/or distributed in myriad variations through standard data processing and/or development techniques.

2627 Multiple instances of any of the program components in a program component set may be instantiated on a single node, and/or across multiple nodes to improve performance through load balancing and/or data processing techniques. Additionally, a single instance may also be distributed across multiple controllers and/or storage devices; eg, a database. All program component instances and controllers working together may do so through standard data process communication techniques.

[0251]

2635 The configuration of the SNAP controller will depend on the environment in which the system is deployed.

2636 Factors such as, but not limited to, budget, capacity, location, and/or utilization of underlying hardware resources may enforce deployment requirements and configurations. Regardless of whether the configuration results in more consolidated and/or integrated program components, results in more distributed families of program components, and/or results in a combination between consolidated and distributed configurations, data may be communicated, obtained, and/or provided. Depending on the set of program components, component instances incorporated into the common code base can pass, obtain,

and/or provide data. These can be achieved through in-application data handling communication techniques such as but not limited to: data references (eg pointers), internal message passing, object instance variable communication, shared memory space, variable passing, and the like.

[0252]

2648 If the component set components are mutually discrete, independent and/or external, then passing, obtaining and/or providing data and/or to other components can be achieved through in-application data processing communication techniques, such as but not limited to: Application programming interface (API) information transfer; (distributed) component object model ((D)COM), (distributed) object linking and embedding ((D)OLE), etc.), common object request agent architecture (CORBA), Jini local and remote APIs, Javascript Object Notation (JSON), Remote Method Reference (RMI), SOAP, process pipes, shared files, etc.

2655 Messages sent between discrete components for inter-application communication, or within the storage space of a single component for intra-application communication, can facilitate the creation and parsing of the grammar. Grammars can be developed using development tools, such as lex, yacc, XML, etc., which allow grammar generation and parsing functions, which in turn can form the basis of communication messages within and between components.

[0253]

2663 For example, the syntax can be set to recognize a token for an HTTP post directive, such as:

[0254]

2667 w3c-post http://...

2668 Value1

[0255]

2672 Where Value1 is identified as a parameter because "http://" is part of the syntax and subsequent is considered part of the posted value.

2674 Similarly, using this syntax, the variable "value1" can be inserted into the "http://" post command and then sent.

2676 The grammar itself may be presented as structured data that is interpreted and/or used to generate parsing mechanisms (such as grammar description text files processed by lex, yacc, etc.). Likewise, once a parsing mechanism has been spawned and/or instantiated, it itself processes and/or parses structured data such as, but not limited to: characters delineating text (e.g. tags), HTML, structured text streams, XML, etc. data. In another embodiment, the inter-application data processing protocol itself may have integrated and/or readily available parsers (eg, JSON, SOAP, etc. parsers) that may be used to parse (eg, communicate) data. Furthermore, parse syntax can be used on top of message parsing, but also for parsing: databases, datasets, data stores, structured data, etc. Again, the desired configuration will depend on the context, environment,

and needs of system development.

[0256]

2688 For example, in some implementations, the SNAP controller may be a PHP script that implements a Secure Sockets Layer (“SSL” socket server) executed by the message server, which listens for data that the client may send (e.g., data encoded in JSON format) incoming traffic on the server port.

2691 Once the incoming communication is identified, the PHP script can read the incoming message from the client device, parse the received JSON-encoded data to extract information from the JSON-encoded text data into PHP script variables, and query it using the Structured Query Language (“SQL ") to store the data (eg, client identification information, etc.) and/or the extracted information in a relational database accessible by Basically written as PHP/SQL commands to accept JSON-encoded input data from a client device over an SSL connection, parse the data to extract variables, and store the data to a database An exemplary list is provided below:

[0258]

2701 Likewise, the following resources are available to provide exemplary embodiments showing SOAP parser implementations:

[0259]

2706 http://www.xav.com/perl/site/lib/SOAP/Parser.html

[0260]

2710 http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?
2711 topic=/com.ibm

[0261]

2715 .
2716 IBMDI.doc/referenceguide295.htm

[0262]

2720 and other parser implementations:

[0263]

2724 http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?
2725 topic-/com.ibm

[0264]

2729 .

2730 IBMDI.doc/referenceguide259.htm

[0265]

2734 All of these are therefore included here by reference.

[0266]

2738 In order to solve various problems and develop technologies, it is used for snapshot mobile payment devices, methods and systems (including cover, title, subtitle, technical field, background technology, summary of the invention, description of drawings, detailed description, claims, abstract , drawings, appendices and/or others) of this application throughout are shown by various schematic embodiments in which the claimed innovations can be practiced.

2743 The advantages and features of the present application are merely representative examples of embodiments, not exhaustive and/or exclusive.

2745 They exist only to aid in understanding and to teach the principles as claimed.

2746 It should be understood that they do not represent all innovations as claimed.

2747 Accordingly, certain aspects of the disclosure are not discussed here.

2748 Alternative embodiments have not necessarily been presented for specific parts of the invention or otherwise undescribed alternative embodiments may be available to contemplate disclaimed components of an alternative embodiment.

2751 It will be appreciated that many of those non-described embodiments employ the same principles of the invention and that others are equivalent. Accordingly, it is to be understood that other embodiments may be utilized and functional logical, operational, organizational, structural and/or topological modifications may be made without departing from the scope and/or spirit of this disclosure. Accordingly, all examples and/or embodiments are considered to be non-limiting throughout this disclosure. No inference should be drawn to consider those embodiments discussed here relative to those not discussed here, except for the sake of reducing space and repetition. For example, it should be understood that the logical and/or topological structure of any group of any program component (collection of components), other components and/or provided component arrangements as shown in the figures and/or fully described is not limited to a fixed operating order and/or permutation, but any order disclosed is exemplary and all equivalents, regardless of order are contemplated by this disclosure. Furthermore, it should be understood that such components are not limited to serial execution, but that multiple threads, processes, services, servers, and/or those that can execute asynchronously, synchronously, in parallel, concurrently, synchronously, etc. are contemplated by this disclosure. Thus, some components may be mutually exclusive in that they cannot both exist in a single embodiment. Similarly some components are applicable to one aspect of the invention and not applicable to other aspects. Additionally, the disclosure includes other novel methods that are not presently claimed. All rights reserved to the presently unclaimed applicant for a new method, including the right to claim such a

new method, file addition application, continuation, continuation in part, severance, and/or its equivalents. Thus, it should be understood that advantages, embodiments, examples, functions, components, logical operations, organization, structures, topologies and/or other aspects of the disclosure are not intended to be limited to or limited to the disclosure defined by the claims On the equivalent of claims. It should be understood that various implementations of SNAP depend on the specific needs and/or characteristics of SNAP individual and/or business users, database configurations and/or relational models, data types, data transfer and/or network frameworks, syntax structures, etc. Example can be implemented which allows a lot of flexibility and customization. For example, aspects of SNAP may be adapted for restaurant ordering, online shopping, shopping in brick and mortar stores, secure information processing, healthcare information systems, and the like. While the various embodiments and discussions of SNAP have been directed to electronic purchase transactions, however, it should be understood that the embodiments herein can be readily configured and/or customized for a wide variety of other applications and/or implementations Way.

Notice

CLAIMS CN106803175A

1.

13 A computer-implemented snapshot payment method comprising:
14 obtaining user input at the mobile computing device to initiate a purchase transaction;
15 acquiring image frames by an image acquisition device operatively connected to said mobile computing device;
16 identify the payment code depicted within the captured image frame;
17 generating a purchase transaction request via the mobile computing device using the identified payment code;
18 providing the purchase transaction request for payment processing; and
19 A purchase receipt is obtained for the purchase transaction.

2.

23 The method of claim 1, further comprising:
24 An image of the payment code is provided for purchase transaction processing.

3.

28 The method of claim 1, further comprising:
29 acquiring video including said image frames by said image acquisition device included in said user mobile device;
31 extracting said image frames from the acquired video; and
32 The image frame is analyzed to determine whether the image frame includes the described payment code.

4.

36 The method of claim 1, wherein the user input is a touch screen gesture on a touch screen operatively connected to the mobile computing device.

5.

41 The method of claim 1, wherein the payment code is a one-dimensional barcode.

6.

45 The method of claim 1, wherein the payment code is a two-dimensional barcode including a quick response code.

7.

50 The method of claim 1, further comprising:

51 extract purchase session data from said payment code; and

52 Wherein the purchase transaction request is generated through the user's mobile device using the extracted purchase session data.

8.

57 The method of claim 7, wherein the purchasing session data includes a merchant identifier and a session identifier for a user shopping session with a merchant associated with the merchant identifier.

9.

62 The method of claim 8, wherein the session identifier is configured as a token parameter in a Uniform Resource Locator for data about a user's shopping session with the merchant.

10.

67 The method of claim 1, further comprising:

68 Obtain payment information associated with a virtual wallet account for payment processing;

69 Wherein the generated purchase transaction request includes the payment information associated with the virtual wallet account.

11.

74 The method of claim 10, wherein the payment information includes a dynamically generated card verification value code.

12.

79 The method of claim 11, further comprising:

providing a request to the server for the dynamically generated card verification value code; and

The dynamically generated card verification value code is obtained from the server in response to providing the request.

13.

The method of claim 12, wherein the dynamically generated card verification value has an expiration time and corresponds to a user shopping session with the merchant.

14.

The method of claim 1, wherein the payment code depicted within the captured image frame is captured from a display of a media device and encodes data to purchase the requested media content.

15.

The method of claim 14, wherein the media device is a television.

16.

The method of claim 15, wherein the television is part of an in-flight entertainment system.

17.

The method of claim 16, wherein the media device is displaying a web page.

18.

A computer-implemented snapshot payment system comprising:

processor; and

a memory configured to communicate with the processor and store processor-executable instructions to:

obtaining user input at the mobile computing device to initiate a purchase transaction;

acquiring image frames by an image acquisition device operatively connected to said mobile computing device;

identify the payment code depicted within the captured image frame;

generating a purchase transaction request via the mobile computing device using the identified payment code;

providing the purchase transaction request for payment processing; and

A purchase receipt is obtained for the purchase transaction.

19.

A computer-readable tangible medium storing computer-executable snapshot payment instructions to:

obtaining user input at the mobile computing device to initiate a purchase transaction;
acquiring image frames by an image acquisition device operatively connected to said mobile computing device;
identify the payment code depicted within the captured image frame;
generating a purchase transaction request via the mobile computing device using the identified payment code;
providing the purchase transaction request for payment processing; and
A purchase receipt is obtained for the purchase transaction.

20.

A computer-implemented snapshot payment device, comprising means for:
obtaining user input at the mobile computing device to initiate a purchase transaction;
acquiring image frames by an image acquisition device operatively connected to said mobile computing device;
identify the payment code depicted within the captured image frame;
generating a purchase transaction request via the mobile computing device using the identified payment code;
providing the purchase transaction request for payment processing; and
A purchase receipt is obtained for the purchase transaction.

21.

A computer-implemented reverse snapshot payment method comprising:
obtaining user input at the user device to initiate a purchase transaction with a merchant;
obtain user payment information for processing said purchase transaction;
generating, by the user device, a payment code image using payment information for processing the purchase transaction;
displaying the payment code image for a point-of-sale terminal via a display operatively connected to the user device to capture an image of the payment code image; and
A purchase receipt is obtained for the purchase transaction.

22.

A computer-implemented group decomposition snapshot payment method, comprising:
obtaining user input at the user's user device to initiate a group purchase transaction;
obtaining purchase data for said group purchase transaction;
generating, by said user device, a disassembled payment code image using purchase data for said group purchase transaction;
wherein said disassembled payment code image includes information about another user's payment amount; and
The split payment code image is displayed for another user device of the other user by a display operatively connected to the user device to obtain an image of the split payment code image.

23.

A computer-implemented person-to-person snapshot payment method comprising:

obtaining user input at the user's user device to initiate a person-to-person transaction;

obtaining a transfer amount for said person-to-person transaction;

generating, by said user device, a payment code image using a transfer amount for said person-to-person transaction;

wherein said payment code image includes information about the amount transferred by another user; and

The payment code image is displayed for another user device of the other user by a display operatively connected to the user device to obtain an image of the payment code image.

24.

A computer-implemented method of mobile selling on snaps, comprising:

obtaining a user checkout request at the point-of-sale device;

obtaining user shopping cart information about a merchant for use in processing purchase transactions associated with said user's checkout request;

using the user shopping cart information to generate a payment code image through the user device;

via a display operatively connected to the point-of-sale device, displaying the payment code image for user equipment to capture an image of the payment code image; and

An authorization notification is obtained for the purchase transaction.

25.

A computer-implemented reverse snapshot mobile selling method comprising:

obtaining a user checkout request at the point-of-sale device;

acquiring an image frame by an image acquisition device operatively connected to said point-of-sale device;

identify the payment code depicted within the captured image frame;

generating a purchase transaction request through said point-of-sale device using the identified payment code;

providing the purchase transaction request for payment processing; and

An authorization notification is obtained for the purchase transaction.

(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106803175 A
(43)申请公布日 2017.06.06

(21)申请号 201710037081.6

(22)申请日 2012.02.16

(30)优先权数据
61/443,624 2011.02.16 US
61/512,248 2011.07.27 US
61/522,213 2011.08.10 US
61/527,576 2011.08.25 US

(62)分案原申请数据
201280018719.7 2012.02.16

(71)申请人 维萨国际服务协会
地址 美国加利福尼亚

(72)发明人 A·哈曼德 I·卡彭科
M·加夫利洛夫 A·施里瓦司塔瓦
M·卡尔森 P·哈里拉马尼

(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 张劲松

(51)Int.Cl.
G06Q 20/36(2012.01)

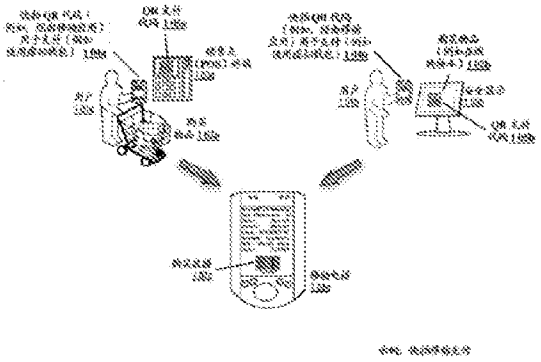
权利要求书3页 说明书46页 附图53页

(54)发明名称

快拍移动支付装置,方法和系统

(57)摘要

本发明公开了快拍移动支付装置,方法和系统。快拍移动支付装置、方法和系统("SNAP")经由SNAP部件传送实时产生的商家一产品快速响应代码到基于虚拟钱包卡的交易购买通知。在一个实施例中,该SNAP从移动设备获得出现在销售点设备的显示屏上的QR代码的快照。所述SNAP解码所述QR代码来获得包括在用户的结帐请求中的产品信息,以及商家信息以用于处理和提供该QR代码的商家的用户购买交易。所述SNAP访问用户虚拟钱包来获得用户账户信息以处理与商家的用户购买交易。所述SNAP利用该产品信息、商家信息和用户账户信息产生卡授权请求,SNAP提供其到支付网络用于交易处理。此外,所述SNAP获得确认用户购买交易的处理的购买收据。



CN 106803175 A

1.一种计算机实现的快拍支付方法,包括:

在移动计算设备处获得用户输入来启动购买交易;

通过操作地连接至所述移动计算设备的图像获取设备获取图像帧;

识别在所获取的图像帧内描述的支付代码;

使用所识别的支付代码,通过所述移动计算设备产生购买交易请求;

提供所述购买交易请求用于支付处理;以及

获得用于所述购买交易的购买收据。

2.如权利要求1所述的方法,还包括:

提供所述支付代码的图像用于购买交易处理。

3.如权利要求1所述的方法,还包括:

通过包括在所述用户移动设备中的所述图像获取设备获取包括所述图像帧的视频;

从所获取的视频提取所述图像帧;以及

分析所述图像帧来确定所述图像帧是否包括所描述的支付代码。

4.如权利要求1所述的方法,其中所述用户输入是在操作地连接至所述移动计算设备的触摸屏上的触摸屏手势。

5.如权利要求1所述的方法,其中所述支付代码是一维条型码。

6.如权利要求1所述的方法,其中所述支付代码是包括快速响应代码的二维条型码。

7.如权利要求1所述的方法,还包括:

从所述支付代码提取购买会话数据;以及

其中所述购买交易请求是使用所提取的购买会话数据,通过所述用户移动设备产生的。

8.如权利要求7所述的方法,其中所述购买会话数据包括商家标识符,以及用于和与所述商家标识符相关联的商家的用户购物会话的会话标识符。

9.如权利要求8所述的方法,其中所述会话标识符被配置为用作关于和所述商家的用户购物会话的数据的统一资源定位符中的令牌参数。

10.如权利要求1所述的方法,还包括:

获得与虚拟钱包帐户相关联的支付信息用于支付处理;

其中所产生的购买交易请求包括与所述虚拟钱包帐户相关联的所述支付信息。

11.如权利要求10所述的方法,其中所述支付信息包括动态产生的卡验证值代码。

12.如权利要求11所述的方法,还包括:

提供对动态产生的卡验证值代码的请求到服务器;以及

响应提供所述请求,从所述服务器获得所述动态产生的卡验证值代码。

13.如权利要求12所述的方法,其中动态产生的卡验证值具有期满时间并且对应于和商家的用户购物会话。

14.如权利要求1所述的方法,其中在所获取的图像帧内描述的所述支付代码是从媒体设备的显示器获取的,并且编码数据来购买所要求的媒体内容。

15.如权利要求14所述的方法,其中所述媒体设备是电视。

16.如权利要求15所述的方法,其中所述电视是飞机上娱乐系统的一部分。

17.如权利要求16所述的方法,其中所述媒体设备正显示网页。

18.一种计算机实现的快拍支付系统，包括：

处理器；以及

存储器，配置为与所述处理器通信并存储处理器可执行指令以：

在移动计算设备处获得用户输入来启动购买交易；

通过操作地连接至所述移动计算设备的图像获取设备获取图像帧；

识别在所获取的图像帧内描述的支付代码；

使用所识别的支付代码，通过所述移动计算设备产生购买交易请求；

提供所述购买交易请求用于支付处理；以及

获得用于所述购买交易的购买收据。

19.一种计算机可读的有形介质，存储计算机可执行的快拍支付指令以：

在移动计算设备处获得用户输入来启动购买交易；

通过操作地连接至所述移动计算设备的图像获取设备获取图像帧；

识别在所获取的图像帧内描述的支付代码；

使用所识别的支付代码，通过所述移动计算设备产生购买交易请求；

提供所述购买交易请求用于支付处理；以及

获得用于所述购买交易的购买收据。

20.一种计算机实现的快拍支付装置，包括装置以用于：

在移动计算设备处获得用户输入来启动购买交易；

通过操作地连接至所述移动计算设备的图像获取设备获取图像帧；

识别在所获取的图像帧内描述的支付代码；

使用所识别的支付代码，通过所述移动计算设备产生购买交易请求；

提供所述购买交易请求用于支付处理；以及

获得用于所述购买交易的购买收据。

21.一种计算机实现的反向快拍支付方法，包括：

在用户设备处获得用户输入来启动和商家的购买交易；

获得用于处理所述购买交易的用户支付信息；

通过所述用户设备使用用于处理所述购买交易的支付信息产生支付代码图像；

通过操作地连接至所述用户设备的显示器，为销售点终端显示所述支付代码图像以获取所述支付代码图像的图像；以及

获得用于所述购买交易的购买收据。

22.一种计算机实现的群组分解快拍支付方法，包括：

在用户的用户设备处获得用户输入来启动群组购买交易；

获得用于所述群组购买交易的购买数据；

通过所述用户设备，使用用于所述群组购买交易的购买数据产生分解支付代码图像；

其中所述分解支付代码图像包括有关另一个用户的支付金额的信息；以及

通过操作地连接至所述用户设备的显示器，为所述另一个用户的另一个用户设备显示所述分解支付代码图像以获取所述分解支付代码图像的图像。

23.一种计算机实现的个人对个人的快拍支付方法，包括：

在用户的用户设备处获得用户输入来启动个人对个人的交易；

获得用于所述个人对个人的交易的转帐金额；

通过所述用户设备，使用用于所述个人对个人的交易的转帐金额产生支付代码图像；

其中所述支付代码图像包括有关另一个用户的转帐金额的信息；以及

通过操作地连接至所述用户设备的显示器，为所述另一个用户的另一个用户设备显示所述支付代码图像以获取所述支付代码图像的图像。

24.一种计算机实现的快拍移动销售方法，包括：

在销售点设备处获得用户结帐请求；

获得关于商家的用户购物车信息用于处理与所述用户结帐请求相关的购买交易；

通过所述用户设备，使用所述用户购物车信息产生支付代码图像；

通过操作地连接至所述销售点设备的显示器，显示所述支付代码图像以便用户设备获取所述支付代码图像的图像；以及

获得所述购买交易的授权通知。

25.一种计算机实现的反向快拍移动销售方法，包括：

在销售点设备处获得用户结帐请求；

通过操作地连接至所述销售点设备的图像获取设备获取图像帧；

识别在所获取的图像帧内描述的支付代码；

使用所识别的支付代码，通过所述销售点设备产生购买交易请求；

提供所述购买交易请求用于支付处理；以及

获得所述购买交易的授权通知。

快拍移动支付装置,方法和系统

[0001] 本申请是基于申请号为201280018719.7、申请日为2012年2月16日、发明名称为“快拍移动支付装置,方法和系统”的专利申请的分案申请。

[0002] 本专利申请公开文档(在下文中称“说明书”)描述指导各个新的革新(在下文中是新发明新技术和/或新方法)的发明方面并包含附属于版权,掩模工作和/或其它知识产权保护的材料。当它出现在公开的专利局文件/记录中时,这种知识产权的各个所有人不反对任何人作出专利公开文档的传真再现,但在别的方面保留所有权利。

[0003] 优先权声明

[0004] 本申请按照35USC$119,要求了下列优先权:于2011年2月16日申请的序号为61/443,624、标题为“移动捕获结帐装置、方法和系统”,代理人编号为P-42032PRV|20270-127PV的美国临时专利申请;2011年7月27日申请的序号为61/512,248,标题为“快拍移动支付装置,方法和系统”,代理人编号为10US01|20270-175PV的美国临时专利申请;2011年8月10日申请的序号为61/522,213,标题为“通用移动支付平台、装置、方法和系统”,代理人编号为10US03|20270-175PV2的美国临时专利申请;以及2011年8月25日申请的序号为61/527,576,标题为“快拍移动支付装置、方法和系统”,代理人编号为10US02|20270-175PV1的美国临时专利申请。将前述的申请的整个教导在此引入,以供参考。

技术领域

[0005] 本发明一般地涉及用于电子购买交易的装置、方法和系统,具体而言,涉及快拍移动支付装置、方法和系统(“SNAP”)。

背景技术

[0006] 顾客交易通常需要顾客从商品陈列架或网站选择产品,然后在结帐柜台或 网页上结帐。产品信息通常是从网页目录或进入销售点终端设备中被选择出来的。在物理零售环境中,产品信息是通过利用集成的条形码扫描器在销售点记录器上扫描物品条型码而自动输入的,以及顾客通常被配有多个支付选项,诸如现金、支票、信用卡或借记卡。一旦支付被提出并同意,所述销售点记录器在商家的计算机系统中存储所述交易,以及产生表示所述交易圆满结束的收据。

附图说明

[0007] 根据本发明的发明方面,所述附录和/或附图非限制的举例说明了根据本发明的各个示例、发明的方面:

[0008] 图1A-F示出了说明了在SNAP的一些实施例中的基于快拍移动支付的购买交易的示例方面的框图;

[0009] 图2A-F示出了在所述SNAP的一些实施例中,说明帮助快拍移动支付的快拍移动支付应用的示例特征的应用程序用户界面图;

[0010] 图3A-E示出了在所述SNAP的一些实施例中,说明用于捕获产品条型码、保护用户

数据并防止欺诈的快拍移动支付应用的示例特征的应用程序用户界面图；

[0011] 图4A-D示出了在所述SNAP的一些实施例中，说明示例快拍移动支付过程的数据流程图；

[0012] 图5A-E示出了在所述SNAP的一些实施例中，说明实行快拍移动支付的示例方面的逻辑流程图，例如快拍移动支付执行(“SMPE”)部件500；

[0013] 图6A-B示出了在所述SNAP的一些实施例中，说明处理快速响应代码的示例方面的逻辑流程图，例如快速响应代码处理(“QRCP”)部件600；

[0014] 图7示出了在所述SNAP一些实施例中，说明虚拟钱包应用的示例特征的概述的用户界面图；

[0015] 图8A-G示出了在所述SNAP的一些实施例中，说明购物模式中的虚拟钱包应用的示例特征的用户界面图；

[0016] 图9A-F示出了在所述SNAP的一些实施例中，说明支付模式中的虚拟钱包应用的示例特征的用户界面图；

[0017] 图10示出了在所述SNAP一些实施例中，说明历史模式中的虚拟钱包应用的示例特征的用户界面图；

[0018] 图11A-F示出了在所述SNAP的一些实施例中，说明快拍模式中的虚拟钱包应用的示例特征的用户界面图；

[0019] 图12示出了在所述SNAP一些实施例中，说明报价模式中的虚拟钱包应用的示例特征的用户界面图；

[0020] 图13A-B示出了在所述SNAP的一些实施例中，说明安全和隐私模式中的虚拟钱包应用的示例特征的用户界面图；

[0021] 图14示出了说明SNAP控制器的实施例的框图。

[0022] 所述附图内的每个附图标记的前沿的数字表示其中附图标记被引入和/或详细说明的附图。因而，附图标记101的详细论述将在附图1中出现和/或被引用，附图标记201被引进附图2中等等。

具体实施方式

[0023] 快拍移动支付(SNAP)

[0024] 所述快拍移动支付装置、方法和系统(在下文中“SNAP”)通过SNAP部件将实时产生的商家产品的快速响应代码转换成为基于卡的虚拟钱包的交易购买通知。图1A-F示出了说明在SNAP的一些实施例中的基于快拍移动支付的购买交易的示例方面的框图。参见附图1A，在一些实现方式中，例如101a-b的用户可能希望在例如103a的商家商店或在例如103b的商家网站购买产品。例如，在商家商店，用户可在例如103a的商店中的销售点(“POS”)终端上扫描多个产品(例如102a)的条型码，然后指示用户希望结帐的扫描物品。在一些实现方式中，所述POS终端经由支付网络产生包括扫描的产品物品相关的信息，以及用于处理所述购买交易的商家信息的快速响应(“QR”)代码，例如105a。用户使用诸如智能电话的用户设备可捕获由所述POS终端产生的所述QR代码的图像。例如，所述用户设备可以具有用于迅速获取所述商家产品QR代码的应用。所述用户设备可使用从所述QR代码中提取的信息，连同有关绑定到用户设备的虚拟钱包的信息一起来启动购买交易。例如，所述用户设备可使

用从所述QR代码中提取的所述产品和商家信息以及来自所述虚拟钱包的金融支付信息来建立购买交易请求，并将所述请求提交到支付网络(例如，信用卡处理网络)。

[0025] 在一些实现方式中，所述用户设备可使用捕获QR代码的替换方法来从所 述POS终端获得信息。例如，所述POS终端可经由蓝牙™、Wi-Fi、SMS、文本信息、电子邮件、和/或其它通信方法来传递提交购买交易请求到支付网络所需的信息到用户设备。

[0026] 在一些实现方式中，用户101b可能希望对存储在例如102b的在线商店网站上的虚拟购物车中的物品结帐。例如，用户可以使用安全显示器(例如，所述用户的信任计算设备的一部分)浏览所述网站。当指示用户希望对所述虚拟购物车的物品结帐，所述网站可提供包括有关所述虚拟购物车中的产品和商家信息的信息的QR代码。例如，在其中所述用户使用安全显示器的情况中，为安全目的，QR代码可以被显示在所述安全显示器内的随机位置。所述用户可获取所显示的QR代码的快照，并使用来自与所述用户设备相关联的虚拟钱包的支付信息来创建购买交易请求以便由支付网络处理。当购买交易完成时，支付网络直接向用户设备106、商店中的所述POS终端和/或所述安全显示器(用于安全的在线购物情况)提供例如107的购买收据，作为交易处理完成的确认。因此，在一些实现方式中商家可以在处理所述购买交易时被屏蔽以免获得用户的个人和/或私人信息，同时使用用于呈现商家产品QR代码的安全显示器来确保所述用户的虚拟钱包的完整性。

[0027] 在各个实现方式中，这种支付处理可以被用于各式各样的交易。例如，在餐厅用餐的用户可获得包括QR支付代码的帐单，QR支付代码包括关于包括在该账单中的餐费的细节，以及该餐厅的的商家ID。在没有向该餐厅披露关于该用户的任何金融或个人信息的情况下，用户可使用用户的智能电话给该餐厅账单拍快照，以及使用用户的虚拟钱包为支付该餐厅账单。

[0028] 参见附图1B，在一些实现方式中，例如110，用户111可能希望使用反向快拍移动支付过程来结帐存储在(在线)商店例如112中的(虚拟)购物车中的物品。例如，用户看使用作为用户的信任计算设备的一部分的安全显示器，例如113，或经由实体商店中的POS终端浏览网站。当指示用户希望结帐所述虚拟购物车中的物品时，用户可经由连接至该用户的虚拟钱包的用户移动设备上的移动应用生成(例如114)包括有关该用户的支付方式、报价、回报、和/或其它方面的信息的QR代码115b。该用户可提供显示在用户移动设备上的该QR代码给安装在信任计算设备(或POS终端)上的网络摄像机(或其它QR代码捕捉设备和/或机制)。用户的信任计算设备或POS终端可获得由该用户的 移动设备产生的该QR代码的快照，例如116，并且利用来自该用户产生的QR代码的支付信息来创建购买交易请求，以用于支付网络进行处理。当完成该购买交易时，该支付网络可直接向用户移动设备、商店中的POS终端和/或安全显示器(用于安全的在线购物情况)提供购买收据，作为交易处理完成的确认。因此，在一些实现方式中，该用户将能使用由该用户的移动设备产生的QR代码作为塑料支付卡(例如信用、借记、预付卡)的替代，或作为其它诸如近场通信、蓝牙®等等的金融信息传输机制的代替。在一些实现方式中，该QR代码可以是一次性匿名的信用卡号码的代表(例如，参见与附图3B相关联的说明)。

[0029] 在一些实现方式中，第一用户121b可能希望支付给第二用户121a某金额(或等价物，例如虚拟货币、替代货币、回报、里程、点数等等)，例如P2P快拍移动支付120。第二用户121a可产生限制时间有效性的QR代码，例如122，包括关于将被转帐的该金额以及链接到第

二用户的金融账户的隐私记号/别名的信息。第二用户可向第一用户显示产生的该QR代码(例如,通过维持第二用户的移动电话向第一用户显示该QR代码;通过电子邮件、社交网络消息、推特等等发送该QR代码)。第一用户使用第一用户的移动电话给该QR代码拍快照,例如123,并且使用该金额、第二用户的链接到金融账户的隐私记号/别名、以及链接到该第一用户的移动电话的第一用户的虚拟钱包,来产生用于由该支付网络处理的购买交易请求。当该交易完成时,该支付网络可向作为交易当事方的用户提供交易通知收据。在作为替代的实现方式中,该两个用户可经由该QR代码的备用方法共享在该QR代码中编码的数据,包括但不限于:近场通信(NFC)、Wi-Fi™、蓝牙™、蜂窝网络、SMS、电子邮件、文本消息和/或其它通信协议。

[0030] 通常,应该理解的是,在快拍移动支付的各个实现方式中,这种记号、别名和/或处理可以被有利地使用。例如,希望参与反向快拍移动支付过程(参见,例如附图1B,元件110)的用户可产生包含关于指向存储在支付网络系统的服务器上的金融支付信息的句柄(handle)的信息的QR代码。例如,快拍移动支付的一些实现方式可使用支付象征过程来产生和/或处理句柄,支付象征过程与编号为13/153,301、标题为"支付象征装置方法以及系统"的美国申请所描述的内容相似,此处该整个内容通过引用被明确地包括在此。此外,在一些实现方式中,该句柄可根据简洁消息传递协议编码信息,诸如在编号为6,837,425,标题为"简洁协议以及解决便携式消费者设备和基础设备之间基本上离线消息传递的方法"的美国专利中描述的,此处通过引用其整个内容被明确地包括在此。在一些反向快拍移动实现方式中,用户可提供包含有该句柄并显示在用户的移动设备上的该QR代码给安装在信任计算设备(或POS终端)上的网络摄像机(或其它QR代码捕捉设备和/或机制)。该用户信任的计算设备或POS终端可获得由该用户的移动设备产生的QR代码的快照,例如116,并为由该支付网络处理的购买交易请求提供从该QR代码中提取的句柄给商家服务器。为了使用该句柄处理该购买交易,该商家服务器可产生卡授权请求(诸如参考附图4A在以下的讨论中进一步描述的),并提供该卡授权请求给支付网络。当完成该购买交易时,该支付网络可直接向用户移动设备、该商店中的该POS终端和/或该安全显示器(例如用于安全的在线购物情况)提供购买收据,作为使用该句柄的交易处理完成的确认。

[0031] 在一些实现方式中,用户警告机制可以被建立到快拍移动支付购买交易处理流程中。例如,在一些实现方式中,商家服务器可嵌入专用于该交易的URL到卡授权请求中。例如,在一些实现方式中,POS终端、远程设备和/或台式计算机可在卡授权请求中将该URL嵌入到可选的层3数据中。该URL可指向存储在作为卡授权请求的主体的专用于该交易的商家服务器上的网页。例如,由该URL指向的网页可包括关于该购买交易的细节,例如被购买的产品、进货成本、时间期满、订单处理的状态等。因此,通过传递该网页的URL给该支付网络,商家服务器可向该支付网络提供该交易的细节。在一些实现方式中,该支付网络可提供通知给用户,诸如支付收据、交易授权确认消息、运输通知等。在这种消息中,该支付网络可提供该URL给用户设备。该用户可在用户的设备上导航到该URL来获得关于该用户的购买的警告,以及其他的信息,诸如报价、优惠券、相关产品、回报通知等。

[0032] 在一些实现方式中,多个用户可经由快拍移动支付可参与群组支付来分解偿付(tender),例如130。在一些实现方式中,用户之一131a可获得在例如133的POS终端处生成的(或例如在诸如用餐账单的纸上呈现的)QR支付代码(例如134)的快照(例如132)。该用户

可又生成QR分解支付代码，包含有关于该偿付已经被分解为的金额的信息。该用户131a可呈现该分解的偿付QR代码135给其他用户131b-c，用户131b-c可获得该分解的偿付QR代码的快照，例 如136。在一些实现方式中，为了该原始QR代码的支付，该用户131b-c可以经由该支付网络偿还用户131a，或用户131b-c可以经由该分解的偿付QR代码进行直接支付给该商家(例如，当该用户131a给该商家的QR代码拍快照的时候，没有立即发生支付处理)。在一些实现方式中，该商家可为用户131a-c直接提供分解偿付QR代码。

[0033] 在一些实现方式中，通过使用作为替代的通信机制可以实现群组移动支付，而不是使用QR代码。例如，在一些实现方式中，该POS终端133可使用诸如蓝牙™的通信协议来与用户131a-c通信。该POS终端可串行或并行地与每一个用户建立独立的通信会话。通过这些独立的通信会话，POS终端可传输该用户的设备所需要的产品和/或商家数据来产生各个购买交易处理请求。因此，通过这些独立的通信会话，POS终端可将与用户131a-c相关联的群组偿付分解成单个支付金额。

[0034] 参见附图1C，在一些实现方式中，为了认证/验证目的，以及为了提供用于公开个人和/或私人信息的数字准许，可以使用快拍移动付帐方式。例如，拜访他/她的医生143的用户142可能被要求提供正式准许来向该医生公开个人信息(例如病历)。该医生的终端(例如144)可产生包含有这个医生数字凭证以及有关被请求的用户的病历的类型/内容的信息的QR代码。用户可通过该用户的移动设备对该QR代码拍快照。用户的移动设备可根据该QR代码产生记录释放的请求，以及用作该请求是从个人信任设备(例如该用户的移动设备)获得的验证。在作为替代的实现方式中，用户能够选择该用户意欲向医疗供应商披露的个人信息，以及该用户的移动设备可产生一QR代码以用于该医生的终端来获得快照以便检索该用户的医疗信息。在一些实现方式中，该QR代码也可以包括支付信息(例如用户的支付帐户信息，或该医生的收单机构信息)以及有关个人信息的受控释放的信息。

[0035] 在一些实现方式中，SNAP可通过预先填充可变更的QR支付代码来辅助P2P交易，例如150。例如，具有公开的简档页面(例如151)的第一用户可放置QR代码的图像在公开的简档中，例如152。例如，该QR代码可包括预先确定的支付金额用于通过获取该QR代码的快照发起的购买交易。在一些实现方式中，该预定的金额可以是$0(例如，$0QR支付代码)。第二用户可使用移动设备来捕捉该QR支付代码的快照，并可通过第二用户的移动设备来设置第二用户意欲支付第一用户的金额。第二用户的移动设备可给用于交易处理的支付网络提供在该QR代码内编码的信息以及第二用户选择的支付金额。

[0036] 应该理解的是，可以使用此处描述的快拍移动支付的各个方面以用于信息的任何受控交换和/或支付。例如，参考附图1D，在一些实现方式中，用户可通过快拍移动支付获得按次计费的节目，例如160。例如，电视显示器可提供包括节目信息(例如162)的广告以及QR支付代码用于获得该节目内容，例如161。该QR代码包括标识该节目信息的信息，以及标识该电视预订者帐户信息、电视机地址等的信息。该用户可获得该QR代码的快照，并提供嵌入在该QR代码中的信息以及该用户的移动设备的信息(例如，链接到该用户的虚拟钱包的预订者帐号、付款帐户信息等)。当通过支付网络处理支付信息时，该支付网络可将支付完成的指示提供给电视节目供应商，并且该电视节目供应商可放出节目内容到用户的电视。作为另一例子，相似流程可以被用于飞机上的娱乐活动，例如170，其中飞机上的屏幕可提供节目信息172以及QR支付代码171以供用户快拍来用于飞机上娱乐活动的启动。作为另一例

子，广告牌、壁挂、海报、商店内广告、临时围墙等等，例如180，可包括用于产品/服务的报价，以及包括商家信息和标识购买量的产品信息的QR代码等。用户可利用链接到该用户的虚拟钱包的用户的移动设备来对该QR代码拍快照，以购买该产品和/或服务，以及，如果合适，该产品可以被直接按照与该支付网络交换的作为用户的移动设备发送的购买请求的一部分的购买信息说明的地址运往用户地址处。作为另一例子，报纸，例如185，可包括报价、广告、工作邮寄等，其包含有QR代码，例如186，其中包含有用户利用支付网络发起购买交易所必须的信息。应该理解的是，在此处论述的任何其它实现方式和/或他们的等价物中，可以使用实现此处实现方式中论述的快拍移动支付的任何方面，和/或他们的等价物。

[0037] 参见附图1E-F，在一些实现方式中，处理购买交易所需的数据可以通过替换QR代码的方法来提供，包括但不限于：近场通信(NFC)、Wi-Fi™、蓝牙™、蜂窝网络、SMS、电子邮件、文本消息和/或其它通信协议。例如，在一些实现方式中，通过在客户端设备上执行的网络浏览器进行在线购物的用户，例如190，可能希望从在线商店网站(例如191)对物品的购买进行支付。该网站可包括用户界面元件，用户可激活其来发起购物结帐和支付。当该用户激活该用户元件时，显示在线购物网站的客户端可提供消息给商家的服务器来发起 安全购买交易处理。运行该在线购物网站的商家服务器可建立安全连接(例如安全套接字层连接)到支付网络(例如192)的支付网络服务器。并且，该支付网络服务器可建立安全连接到该客户端。例如，该客户端可包括安全I/O芯片，其仅仅允许通过该客户端和该支付网络的支付网络服务器建立安全连接。通过安全连接，该支付网络服务器可提供指令到该客户端来请求用户启动该用户的用户设备上的虚拟钱包移动应用，参见例如附图1F，196。该客户端可因此提供请求给用户来启动该用户的用户设备(例如193)上的虚拟钱包移动应用。当用户启动该用户设备上的虚拟钱包移动应用时，该用户设备和该客户端可互相建立安全连接(例如通过蓝牙™、Wi-Fi、蜂窝等等)。在一些实现方式中，该客户端和用户设备可以被预先配置来互相快速地建立该安全通信通道。通过该安全通信通道，该客户端可提供数据给用户的移动设备，或反之亦然，来帮助该购买交易的启动。该用户的移动设备(或客户端)上的虚拟钱包应用然后可以产生购买交易启动消息并提供这消息到支付网络服务器以用于处理该购买交易。当交易处理完成时，支付网络服务器可提供支付完成的通知到该客户端，例如附图1F的197，或到该用户设备。

[0038] 图2A-F示出了在该SNAP的一些实施例中，示出帮助快拍移动支付的快拍移动支付应用的示例特征的应用程序用户界面图。参见附图2A，在一些实现方式中，用户可能希望对存储在在线商家网站的虚拟购物车中一个或多个物品结帐。例如，用户可以使用浏览器应用，例如201，来视觉化该商家网站的结帐页面，例如202。该结帐网页可描述该结帐定单的细节，例如203，并可为用户提供一个或多个选项来为存储物品的购买提供支付。在一些实现方式中，该结帐网页可包括选项来使用快拍移动支付过程支付该购买，例如204。

[0039] 参见附图2B，在一些实现方式中，当选择使用该快拍移动支付过程的选项时，商家结帐网页，例如206，可通过该浏览器应用205提供QR代码，例如209，其包括有关虚拟购物车中物品的信息和商家信息以便支付网络处理该购买交易(例如链接到商家的收单机构金融账户的私人记号/别名)。在一些实现方式中，该网页可以通过用户的信任计算设备的安全显示器来显示。例如，作为安全措施，该显示器内的QR代码框架的位置，例如207，可以被随机地改变来防止该QR代码的快照被通过欺诈手段(例如对该信任计算设备的篡改)获得。在

一些实现方式中，由用户预先选择的安全图像，例如208，可以被显示在屏幕 上以便用户可验证为是准确的。在一些实现方式中，在提供图像到信任计算设备以前，该图像可以由SNAP加密。在一些实现方式中，信任计算设备可以是保存解密并且成功地在安全显示器上向用户显示该图像的所需要的解密密钥的唯一设备。

[0040] 参见附图2C，在一些实现方式中，这种包含QR代码的商家产品信息可以被销售点(“POS”)终端使用，例如210a-b。例如，在实体店中，当该用户指示其希望对用户的物理购物车中的物品结账时，POS终端可显示QR代码，例如211a-b，其包括购买支付金额，例如212a-b。例如，该QR代码可包括根据可扩展标记语言(“XML”)格式化的数据，诸如以下示例的数据结构：

[0041]

```
<QR_data>
    <order_ID>4NFU4RG94</order_ID>
    <timestamp>2011-02-22 15:22:43</timestamp>
    <expiry_lapse>00:00:30</expiry_lapse>
    <transaction_cost>$34.78</transaction_cost>
    <user_ID>john.q.public@gmail.com</user_ID>
    <client_details>
        <client_IP>192.168.23.126</client_IP>
        <client_type>smartphone</client_type>
        <client_model>HTC Hero</client_model>
        <OS>Android 2.2</OS>
        <app_installed_flag>true</app_installed_flag>
    </client_details>
    <secure_element>www.merchant.com/securedyn/0394733/123.png</secure_element>
    <purchase_details>
        <num_products>1</num_products>
        <product>
            <product_type>book</product_type>
            <product_params>
                <product_title>XML for Dummies</product_title>
                <ISBN>978-2-14-168710-0</ISBN>
                <edition>2nd ed.</edition>
                <cover>hardbound</cover>
                <seller>bestbuybooks</seller>
            </product_params>
            <quantity>1</quantity>
        </product>
    </purchase_details>
    <merchant_params>
        <merchant_id>3FHCR41HC</merchant_id>
        <merchant_name>Books & Things, Inc.</merchant_name>
        <merchant_auth_key>1MHF484MCP5SCH827365</merchant_auth_key>
    </merchant_params>
</QR_data>
```

[0042] 参见附图2D，在一些实现方式中，用户可使用智能电话(例如213)获得被显示在安全显示器或该POS终端的屏幕上的该QR代码的快照。例如，该用 户的智能电话可以在其上运行以检测和捕捉QR代码(例如216a)的应用，例如214。例如，该用户可使用注册特征，例如215，来在该智能电话的显示器内对其该QR代码。在一些实现方式中，该应用可为用户提供放大(例如217)或缩小(例如218)该QR代码的能力，来确保该QR代码的图像符合该智能电话的屏幕的尺寸。当在该智能电话的显示器内对其QR代码时，用户将能使用用户界面元件例如219来获得该QR代码的快照。该用户可使用该智能电话的显示器上的用户界面元件220取

消该快拍移动支付过程。

[0043] 参见附图2E，在一些实现方式中，当获得该商家产品QR代码的快照时，用户的智能电话可提取存储在该QR代码内的产品以及商家数据，并使用链接到该用户的智能电话的用户虚拟钱包的账号来产生购买交易请求，以用于由支付网络处理。当完成由该支付网络使用由该用户的智能电话提供的信息处理该支付交易时，商家网站222(通过该浏览器应用221)可为该用户提供购买收据225。参见附图2F，在其中用户在实体店使用该快拍移动支付过程的实现方式中，该POS终端可为用户显示购买收据。在一些实现方式中，该支付网络可直接给该用户的智能电话提供买方收据。

[0044] 图3A-E示出了在该SNAP的一些实施例中，举例说明用于捕获产品条型码、保证用户数据安全并防止欺诈的快拍移动支付应用的示例部件的应用程序用户界面图。参见附图3A，在一些实现方式中，在用户的设备上执行的应用可包括为该用户提供各个特征的应用接口。在一些实现方式中，该应用可以被配置为识别产品标识符(例如条型码、QR代码等等)，例如301。例如，该应用可以被配置为捕捉商家产品QR代码以用于快拍移动支付处理，如上参考附图2A-F所讨论的。在一些实现方式中，可能需要用户登陆到该应用来启动它的特征。一旦被启动，摄像机可为该用户提供亲身般一次轻敲购买特征。例如，该客户端设备可具有摄像机，应用通过其可获取图像，视频数据、流现场视频等，例如303。该应用可以被配置为分析输入数据并检索(例如301)产品标识符，例如304，诸如QR代码209、211a-b、216a和227。在一些实现方式中，该应用可覆盖十字线、目标框，和/或类似对准参考标记，例如305，以便用户可使用该参考标记对准该产品标识符，从而帮助产品标识符的识别和解释。在一些实现方式中，该应用可包括接口元件来允许用户在产品识别模式和产品报价接口显示屏幕之间来回切换(参见例如306)，以便用户在捕捉产品标识符以前 可准确地研究对用户可用的交易。在一些实现方式中，该应用可为用户提供浏览先前的产品标识符捕捉(参见例如307)的能力，以便该用户将能更好地决定哪个产品标识符是用户希望捕捉的。在一些实现方式中，用户可能希望取消产品购买；该应用可为用户提供用户界面元件(例如308)来取消产品标识符识别过程并返回到用户原来使用的先前界面屏幕。在一些实现方式中，可以例如以列表形式(参见例如309)为该用户提供关于产品、用户设置、商家、报价等的信息，以便用户可以更好理解用户的购买选项。在应用中可提供各种其他特征(参见例如310)。

[0045] 参见附图3B，在一些实现方式中，该应用可包括用户的位置的指示(例如商家商店的名称、地理位置，与商家商店内的走廊有关的信息，等等)，例如311。该应用可提供用于产品购买的应付金额的指示，例如312。在一些实现方式中，该应用可为用户提供各种选项来支付用于购买产品的金额。例如，该应用可使用GPS坐标来确定该用户所在的商家商店，并指引用户到该商家的网站。在一些实现方式中，SNAP可提供API来直接参与商家以帮助交易处理。在一些实现方式中，标记商家的SNAP应用可以被开发具有SNAP功能，其可直接连接用户到商家的交易处理系统。例如，用户可从各个卡供应商(例如313)的多个卡(例如信用卡、借记卡、预付卡等等)中选择。在一些实现方式中，该应用可给用户提供选项来使用包括在用户的银行帐户例如支票、存款、金融市场、当前帐户等等(例如314)中的资金支付购买金额。在一些实现方式中，用户可以通过该应用设置默认选项来设置哪个卡、银行帐户等要用于该购买交易。在一些实现方式中，这种缺省选项的设置可允许用户通过单个点击、轻敲、扫和/或其它校正的用户输入动作发起该购买交易，例如315a。在一些实现方式中，当用户

使用这种选项的时候，该应用可使用该用户的默认设置来发起该购买交易。在一些实现方式中，该应用允许用户使用其它帐号(例如Google™结帐，Paypal™帐号等等)来支付该购买交易，例如316。在一些实现方式中，该应用允许用户使用回报点、航线里程、旅馆积分、电子优惠券、打印的优惠券(例如通过与产品标识符相似的方式捕捉打印的优惠券)等等来支付该购买交易，例如317-318。在一些实现方式中，该应用在发起购买交易以前提供选项来提供快速授权，例如319。在一些实现方式中，该应用可在用户已经选择某选项来发起该购买交易以后提供进度指示符来提供关于该交易的进度的指示，例如320。在一些实现方式中，该应用可给用户提供关于该用户先前通过该应用进行的购买的历史信息，例如321。在一些实现方式中，该应用可给用户提供选项来与其它用户共享关于该购买的信息(例如，通过电子邮件、SMS、Facebook®上的墙贴、Twitter™上的推特，等等)和/或控制与商家、收单机构、支付网络等等共享的信息，以处理该购买交易，例如322。在一些实现方式中，该应用可给用户提供选项来显示由客户端设备捕捉的产品识别信息(例如以便在离开商店时显示该产品信息的客户服务代表)，例如324。在一些实现方式中，该用户、应用、设备和/或SNAP在处理中可能遇到错误。在这种情况中，用户将能和客户服务代表聊天(例如VerifyChat 323)来解决该购买交易过程中的困难。

[0046] 在一些实现方式中，用户可选择使用一次性的匿名信用卡号码来进行交易，例如参见315b。例如SNAP可使用一组预先指定的匿名卡细节(参见，例如“AnonCard1”，“AnonCard2”)。作为另一例子，SNAP可能例如实时产生一组一次性的不记名卡细节来安全地完成购买交易(例如Anon It 1X)。在这种实现方式中，该应用可自动设置用户简档设置，以便用户的任何个人识别信息将不能被提供给商家和/或其它实体。在一些实现方式中，用户需要输入用户名和密码来启动不记名特征。

[0047] 参见附图3C，在一些实现方式中，该快拍移动支付应用的用户界面元件可以有利地被配置成以应用于该用户的移动设备的最小数量的用户手势来为用户提供利用自定义支付参数处理购买的能力。例如，可以为用户提供超负荷用户界面元件，例如325-326。例如，如果用户在包括在用户的移动设备中的摄像机的视角内具有QR支付代码，那么该用户可激活元件325来给QR代码拍快照并使用预先确定的默认设置来基于该QR代码处理该购买。然而，如果用户希望自定义支付参数，那么该用户可启动用户界面元件326(例如按压并连续保持)。这样做时，该应用可提供弹出菜单，例如327，其提供各种支付定制选择，诸如先前提供的那些。例如，用户可拖动用户手指到用户喜欢的适当设置，并从用户的移动设备的触摸屏释放用户手指来选择该设置用于支付处理。在可选实现方式中，该支付设置选项，例如330，以及QR捕捉激活按钮，例如328a-b(例如328b可提供比显示在初始屏幕中的那些甚至更多的设置)可以和窗口(例如329)一起被包括在用户界面中，以用于通过移动设备的摄像机捕捉该QR代码。在作为替代的实现方式中，该用户的移动设备可产生混合QR代码 支付设置图形，并且POS终端(或用户的信任计算设备)可捕捉该整个图形用于支付处理。

[0048] 参见附图3D，在一些实现方式中，用户可以有利地能够在产生用于购买交易的QR代码的设备中提供用户设置，然后使用该用户的移动设备捕捉该QR代码。例如，销售点终端的显示设备可以显示结帐屏幕，诸如在客户端上运行的网络浏览器，例如331，显示在线购物网站的结帐网页，例如332。在一些实现方式中，结帐屏幕可提供用户界面元件，例如333a-b，借此用户可以指示使用快拍移动支付的希望。例如，如果用户激活元件331a，该网

站可使用用户的默认设置产生QR代码，并在客户端的屏幕上显示该QR代码(例如335)来便于用户使用用户的移动设备捕捉。在一些实现方式中，用户能激活用户界面元件，例如333b，借此客户端可显示具有用户可从中选择的附加选项的弹出菜单，例如334。例如，网站可给用户提供与上述参见附图3B-C的说明中所讨论的相似的选项。在一些实现方式中，当用户修改通过激活该用户界面元件333b而提供的设置时，该网站可实时修改该QR代码335。一旦用户已经使用弹出菜单修改了设置，用户就可捕捉该QR代码的快照来发起购买交易处理。

[0049] 参见附图3E，在一些实现方式中，SNAP可向用户提供用户界面来修改用户的快拍移动支付设置。例如，该SNAP可提供网络界面，例如341。例如，用户能使用该网络界面修改该用户的虚拟钱包的安全设置，例如342。例如，该用户可浏览信任设备的列表，例如344，用户通过该列表可访问该用户的虚拟钱包。在一些实现方式中，该网络界面可提供用户界面元件来添加信任设备，例如343。该网络界面也可以为用户提供附加安全选项。例如，该用户能够设置安全密码(例如345)，更改关于在授权购买交易以前用户何时应被询问的设置(例如346)，安全特征的表示的类型/风格(例如347)，以及将被显示在快拍移动支付中使用的终端上的安全图像(例如348)。在各个实现方式中，用户能访问包括修改用户简档、帐号、帐号偏好、添加卡、获得报价以及优惠券、定位ATM机等等的其它服务。

[0050] 图4A-D示出了在该SNAP的一些实施例中，说明示例快拍移动支付过程的数据流程图。参见附图4A，在一些实现方式中，例如401的用户可能希望通过商家在线站点或商家的商店，从例如403的商家购买产品、服务、报价等(“产品”)。用户可通过客户端，诸如但不局限于个人计算机、移动设备、电视、销 售点终端、商亭、ATM等(例如402)，与例如403的商家服务器通信。例如，用户可提供指示用户希望购买产品的用户输入(例如结帐输入411)到客户端中。例如，商家商店中的用户可通过在销售点终端的条形码扫描器扫描产品的产品条型码。作为另一例子，用户可从商家网站的网页目录选择产品，并添加产品到该商家网站上的虚拟购物车。用户然后可以指示用户希望结帐该(虚拟)购物车中的物品。客户端可产生例如412的结帐请求，并提供该结帐请求(例如413)到商家服务器。例如，客户端可以以根据可扩展标记语言(XML)格式化的数据的形式为商家服务器提供包括产品细节的(安全)超文本传输协议(“HTTP(S)”)GET消息。以下是用于商家服务器的包括XML格式的结帐请求的示例HTTP(S)GET消息：

```
GET /checkout.php HTTP/1.1
Host: www.merchant.com
Content-Type: Application/XML
Content-Length: 718
<?XML version = "1.0" encoding = "UTF-8"?>
<checkout_request>
    <session_ID>4nru48Q94</session_ID>
    <timestamp>2011-02-22 15:22:43</timestamp>
    <user_ID>john.q.public@gmail.com</user_ID>
    <client_details>
          <client_IP>192.168.23.126</client_IP>
          <client_type>smartphone</client_type>
          <client_model>HTC Hero</client_model>
          <OS>Android 2.2</OS>
          <app_installed_flag>true</app_installed_flag>
[0051]    </client_details>
    <purchase_details>
          <num_products>1</num_products>
          <product>
                <product_type>book</product_type>
                 <product_params>
                       <product_title>XML for dummies</product_title>
                       <ISBN>978-3-14-168710-0</ISBN>
                       <edition>2nd ed.</edition>
                       <cover>hardbound</cover>
                       <seller>bestbuybooks</seller>
                 </product_params>
                 <quantity>1</quantity>
          </product>
    </purchase_details>
</checkout_request>
```

[0052] 在一些实现方式中，该商家服务器可从客户端获得该结帐请求，并从该结帐请求提取该结帐细节(例如，XML数据)。例如，商家服务器可使用解析器，诸如如下参见附图14所论述的示例解析器。该商家服务器可从该结帐请求提取 该产品数据以及客户端数据。在一些实现方式中，该商家服务器可查询(例如414)商家数据库(例如404)来获得产品数据(例如415)，诸如产品定价、营业税、报价、折扣、回报和/或其它信息来处理该购买交易。例如，数据库可以是响应于结构化查询语言(“SQL”)命令的关系型数据库。商家服务器可执行包括SQL命令的超文本预处理器(“PHP”)脚本来查询产品数据的数据库。以下提供了说明查询数据库的实质方面的示例性PHP/SQL命令列表：

[0053]

```
<?PHP
header('Content-Type: text/plain');
mysql_connect("254.93.179.112",$DBserver,$password); // access database server
mysql_select_db("PRODUCTS.SQL"); // select database table to search
//create query
$query = "SELECT product_info product_price tax_linfo_list offers_list
    discounts_list rewards_list FROM ProdTable WHERE product LIKE '%' $prod";
$result = mysql_query($query); // perform the search query
mysql_close("PRODUCTS.SQL"); // close database access
?>
```

[0054] 在一些实现方式中，响应于获得产品数据，商家服务器可根据用户的安全设置(参见例如358)产生(例如416a)QR支付代码和/或安全显示元件。该商家服务器可提供该QR代码到客户端，以便客户端可显示该QR代码，然后用户就可使用用户的设备捕捉该QR代码来获得商家和/或产品数据，以用于产生购买交易处理请求。在作为替代的实现方式中，商家服务器可指引客户端通过作为替代的通信协议(诸如但不局限于：Wi-Fi™、蓝牙™、蜂窝网

络、SMS、电子邮件和/或类似通信协议)来传递处理该交易所需的产品和/或商家数据到用户的设备。例如,商家服务器可指引客户端来在它的系统上发起插件,以提供作为替代的通信业务,并通过该通信业务传输该产品和/或商家数据到用户的设备。

[0055] 在使用QR代码的实现方式中,商家服务器可产生包含支付网络处理购买交易所需的产品信息以及商家信息的QR代码。在一些实现方式中,该QR代码可至少包括捕捉该QR代码的用户设备所需的信息来产生购买交易处理请求,诸如商家标识符(例如,商家ID号、商家名称、商店ID等等)以及用于与商店网站/实体店相关联的用户购物会话的会话标识符。

[0056] 在一些实现方式中,该商家服务器可实时产生自定义的、用户指定的商家产品XML数据结构,该数据结构具有限制时间的有效期,诸如以下提供的示例性"QR_data"XML数据结构:

[0057]

```
<QR_data>
    <order_ID>4MRV4RG94</order_ID>
    <timestamp>2011-02-22 15:22:43</timestamp>
    <expiry_lapse>00:00:30</expiry_lapse>
    <transaction_cost>934.78</transaction_cost>
    <alerts_URL>www.merchant.com/shopcarts.php?sessionID=AEEB4356</alerts_URL>
    <user_ID>john.q.public@gmail.com</user_ID>
    <client_details>
        <client_IP>192.168.23.126</client_IP>
        <client_type>smartphone</client_type>
        <client_model>HTC Hero</client_model>
        <OS>Android 2.2</OS>
        <app_installed_flag>true</app_installed_flag>
    </client_details>
    <secure_element>www.merchant.com/securedyn/0394733/123.png</secure_element>
    <purchase_details>
        <num_products>1</num_products>
        <product>
            <product_type>book</product_type>
            <product_params>
                <product_title>XML for dummies</product_title>
                <ISBN>978-2-14-160710-0</ISBN>
                <edition>2nd ed.</edition>
                <cover>hardbound</cover>
                <seller>bestbuybooks</seller>
            </product_params>
            <quantity>1</quantity>
        </product>
    </purchase_details>
    <merchant_params>
        <merchant_id>3FBCP4INC</merchant_id>
        <merchant_name>Books & Things, Inc.</merchant_name>
        <merchant_auth_key>1mrf884MCP59CRm27365</merchant_auth_key>
    </merchant_params>
<QR_data>
```

[0058] 在一些实现方式中,该XML数据可包括句柄、别名、记号或指向存储在支付网络服务器上的信息的指针,而不是编码发起该交易所需的所有实际数据,以便编码到该QR代码中的信息可以有利地被最小化。在一些实现方式中,该商家可使用该XML数据产生QR代码。例如,商家服务器可使用在http://phpqrcode.sourceforge.net/可用的PHP QR代码开源(LGPL)库用于产生QR代码、2维条型码。例如,该商家服务器可发布与以下提供的示例性命令相似的PHP命令:

[0059] <?PHP

[0060] header('Content-Type:text/plain');

[0061] //Create QR code image using data stored in Sdata variable

[0062] QRoode::png(Sdata,'qxcodeimg.png');

[0063] ?>

[0064] 在作为替代的实现方式中，该商家服务器可随着请求一起提供(例如416b)XML数据到支付网络服务器(例如406)来产生QR代码。例如，商家服务器 使用API调用到该支付网络服务器来请求QR代码的生成。支付网络服务器可产生用于该商家服务器的QR代码，例如416c，并提供(例如416d)该QR代码到该商家服务器。例如，支付网络服务器可将由商家提供的信息编码到QR代码中，并且也可有利地将安全信息、时间有效性信息、数字证书信息、不记名发货消息、QR代码产生/处理付费信息等等编码到该QR代码中。

[0065] 在一些实现方式中，支付网络服务器为商家服务器提供加密密钥(例如Rivest-Shamir-Adleman(RSA)私有/公共密钥，数字证书)。商家可使用该加密密钥来加密该自定义的、用户特定的商家产品XML数据结构，以产生加密的购买数据(例如使用RSA算法)。该商家服务器然后可以将该加密的数据编码到QR代码中。在各种实施例中，对于与用户-商家购物会话相关的任何交易处理请求，该支付网络服务器可有利地采用这种方案来验证商家。

[0066] 在一些实现方式中，可以向用户设备提供预先设计的与验证、预先验证的商家相关联的QR代码。例如，用户可以在用户的设备上浏览在线网站。该用户设备可从网页服务器产生用于网页的HTTP(S)GET请求。在一些实现方式中，该网页服务器可响应于该用户设备的对网页的请求，产生用于广告的查询来显示在该网页上。例如，网页服务器可检索数据库或提供请求到广告网络服务器(例如，Akamai)来提供用于嵌入到该网页中的广告。在一些实现方式中，该广告网络服务器可使用从网页服务器中获得的关键字、元数据等(例如，与该网页相关联的关键字或元数据、用户简档信息、用户ID、来自存储在该用户设备上的cookie的用户浏览历史，等等)。该广告网络可使用关键字来产生与该关键字相关联的广告的数据库的查询，并且可获得广告来提供。在一些实现方式中，该广告网络服务器可提供(例如通过API调用)关于这种广告的信息(例如，商家名称，商家ID，产品名称，产品价格信息，相关报价，等等)到支付网络服务器。该支付网络服务器可基于由该广告网络服务器提供的信息产生QR代码，以便用户设备可对该QR代码拍快照来发起与该QR代码(例如，由该广告网络服务器提供到该支付网络服务器的)相关联的货物和/或服务的购买交易。广告网络服务器可提供该QR作为广告的一部分到该网页服务器，网页服务器又可在向用户设备提供网页以前，嵌入包括该QR代码的广告到该网页中。在作为替代的实现方式中，广告网络服务器/网页服务器可传输该QR代码(最终的)的URL或其它标识符到用户设备，并且该用户设备可使用该QR代码的URL(例如，托管在该支付网络服务器上)产生调用(例如HTTP(S)GET请求)来获得该QR代码并为用户显示它。

[0067] 在一些实现方式中，商家服务器可提供该QR代码到该客户端，例如417。例如，商家服务器可提供包括引用该QR代码图像和/或安全元件图像的超文本标记语言(“HTML”)页面，诸如以下示例性的HTML页面：

[0068]
```
<html>
    <img src="www.merchant.com/securedyn/0394733/qrcodeimg.png" alt="Merchant-
    Product QR code"/>
    <img src=" www.merchant.com/securedyn/0394733/123.png" alt="Secure
    Element"/>
</html>
```

[0069] 在一些实现方式中，客户端可获得该QR支付代码(例如417)并在与客户端设备相关联的显示屏幕上显示该QR代码(例如418)。在一些实现方式中，用户可使用用户设备，例如405，来捕捉由该客户端设备呈现的QR代码以用于支付处理。例如，用户可提供支付输入到用户设备例如419中。在各个实现方式中，用户输入可包括但不局限于：触摸屏接口的单次轻敲(例如，一次轻敲移动应用购买实施例)、键盘输入、扫卡、在该用户设备内激活支持RFID/NFC的硬件设备(例如，具有多个帐号的电子卡、智能电话、书写板等等)、鼠标点击、在操纵杆/游戏控制台上压下按钮、语音命令、触敏接口上的单次/多次触摸手势、触动触敏显示器上的用户界面元件，等等。例如，用户设备可从用户卡(例如信用卡、借记卡、预付卡、赊帐卡等等)获得追踪数据，诸如以下提供的示例性追踪数据：

[0070] %B1234567890123445^PUBLIC/J.Q.^99011200000000000000**901*****?*
(wherein '1234567890123445' is the card number of 'J.Q. Public' and has a CVV number of 901, '990112' is a service code, and '***' represents decimal digits which change randomly each time the card is used.)

[0071] 在一些实现方式中，用户设备可确定图像是否已经捕捉了描述QR代码。根据是否已经捕捉了QR代码，以及(可选地)也根据该QR代码的内容，该用户设备可重定向用户(例如通过在该用户设备上执行的网页浏览器应用)到：产品、商家网站、商家网站上的产品、网站以及包括命令来添加物品到与该网站相关联的用户购物车等。例如，用户设备可执行一部件，诸如如下参见附图6A-B的讨论所描述的示例性快速响应代码处理(“QRCP”)部件600。

[0072] 在一些实现方式中，当获得用户支付输入并捕捉了QR代码时，该用户设备可以产生用于提供到支付网络服务器的卡授权请求420(例如，如果该QR代码包括购买优惠券、报价、发货单、来自另一个虚拟钱包用户的个人支付等 等)。例如，用户设备可以以XML格式的数据的形式提供代表该用户的卡授权请求(例如421)、包括用于支付网络服务器的产品订购细节的HTTP(S)GET消息(例如406)。以下是用于该支付网络服务器的包括XML格式的卡授权请求的示例性HTTP(S)GET消息：

```
POST /purchase.php HTTP/1.1
Host: www.merchant.com
Content-Type: Application/XML
Content-Length: 1306
<?XML version = "1.0" encoding = "UTF-8"?>
<purchase_order>
    <order_ID>4RFU4RG94</order_ID>
    <alerts_URL>www.merchant.com/shopcarts.php?sessionID=AER34356</alerts_URL>
    <timestamp>2011-02-22 15:22:43</timestamp>
    <user_ID>john.q.public@gmail.com</user_ID>
    <client_details>
        <client_IP>192.168.23.126</client_IP>
        <client_type>smartphone</client_type>
        <client_model>HTC Hero</client_model>
        <OS>Android 2.2</OS>
        <app_installed_flag>true</app_installed_flag>
    </client_details>
    <purchase_details>
        <num_products>1</num_products>
        <product>
            <product_type>book</product_type>
            <product_params>
                <product_title>XML for dummies</product_title>
                <ISBN>978-2-14-168710-0</ISBN>
                <edition>2nd ed.</edition>
                <cover>hardbound</cover>
                <seller>bestbuybooks</seller>
            </product_params>
            <quantity>1</quantity>
        </product>
    </purchase_details>
    <merchant_params>
        <merchant_id>3FDCR41HC</merchant_id>
        <merchant_name>Books & Things, Inc.</merchant_name>
        <merchant_auth_key>1UH7484NCP59CH87365</merchant_auth_key>
    </merchant_params>
    <account_params>
        <account_name>John Q. Public</account_name>
        <account_type>credit</account_type>
        <account_num>1234567890123456</account_num>
        <billing_address>123 Green St., Norman, OK 98765</billing_address>
        <phone>123-456-7809</phone>
        <sign>/jqp/</sign>
        <confirm_type>email</confirm_type>
        <contact_info>john.q.public@gmail.com</contact_info>
    </account_params>
    <shipping_info>
        <shipping_adress>same as billing</shipping_address>
        <ship_type>expedited</ship_type>
        <ship_carrier>FedEx</ship_carrier>
        <ship_account>123-45-678</ship_account>
        <tracking_flag>true</tracking_flag>
        <sign_flag>false</sign_flag>
    </shipping_info>
</purchase_order>
```

[0073]

[0074] 在一些实现方式中，由用户设备产生的卡授权请求可包括处理该购买交易所需的最少信息。例如，这可提高传递该购买交易请求的效率，并且也可以有 利地提高提供到该用户和/或商家的隐私保护。例如，在一些实现方式中，该卡授权请求可至少包括商家ID、用于用户和商家的购物会话的会话ID，以及链接到该用户的虚拟钱包的用户设备(例如智能电话)的设备ID。在一些实现方式中，发送到/来自于该QR代码捕捉设备的QR代码和消息可包括源ID(例如产生该QR代码的设备的标识符)、会话ID、商家ID、物品ID(例如型号)、结帐金额，和/或交易设备ID(例如，用户的智能电话设备)。

[0075] 在一些实现方式中，卡授权请求可以由该商家服务器或销售点终端提供，而不是用户设备。在一些实现方式中，期望安全的用户可通过该用户设备请求支付网络服务器以

便动态地产生将在该购买交易中与该用户的主要帐户号

[0076] ("PAN",例如,信用卡号码)一起使用的卡验证值代码(dCVV™)。作为响应,该支付网络服务器可产生dCVV™代码(例如,使用随机数生成、输入键的MD5散列,其可以利用用户ID、商家ID、会话ID、时间戳、它们的组合等产生),并为该用户提供会话特定的dCVV™代码来与用户的PAN号码一起使用。例如,会话特定的dCVV™代码可以具有期满时间(例如,从发布开始的一分钟内失效)。该用户设备可(例如,通过蓝牙™、NFC、Wi-Fi、蜂窝、QR代码等等)将该PAN和dCVV传递到销售点终端,销售点终端可创建卡授权请求。例如,该用户设备可产生嵌有该PAN和dCVV号码的QR支付代码,并且销售点终端可对该用户设备产生的QR支付代码的图像拍快照。该销售点终端然后可以产生和提供该卡授权请求到支付网络服务器。该支付网络服务器然后可以比较从商家获得的dCVV和在该购买交易被发起以前提供到该用户设备的dCVV来确认该交易。如果来自该两个源(支付网络服务器和商家)的dCVV代码互相正确地对应,那么该支付网络服务器可继续处理该购买交易。

[0077] 在一些实现方式中,该来自用户设备的卡授权请求可包括从该QR代码提取的加密数据,其可以已经由该商家服务器作为商家验证方案的一部分而加密。在一些实现方式中,该支付网络服务器可从由用户设备提供的卡授权请求获得加密数据,并试图解密该加密数据,例如,利用RSA私有/公共密钥,其对于支付网络服务器开始提供给商家服务器用于在嵌入到该QR代码中以前加密购买数据的密钥是互补的。如果支付网络服务器能够解密该购买数据,那么商家被认证为有效商家。在一些实现方式中,支付网络服务器可以比较从该卡授权解密的购买数据和由用户/用户设备提供的数据,以确定来自这些不同源(用户/ 用户设备,和商家)的数据是否互相正确地对应。因此,在一些实现方式中,该支付网络服务器能验证该商家,并在处理交易以前关联该商家到特定的用户会话或用户设备。

[0078] 在一些实现方式中,支付网络服务器可提供通知给用户设备,通知该交易被验证并批准交易。在作为替代的实现方式中,支付网络服务器可继续进行交易处理。在一些实现方式中,当标识用户处于与商家会话中时,支付网络服务器可以与用户设备通信来为用户提供额外的特征。例如,在一些实现方式中,支付网络服务器可提供与用户设备的通信(例如,通过HTTP(S)POST消息),以提供:商家的虚拟店面;与包括在卡授权请求中的产品相关联的商家的走廊的描述、相关物品的列表等(参见,例如附图8E-G以及附加实施例的以下描述)。

[0079] 参见附图4B,在一些实现方式中,支付网络服务器可处理交易以便转帐购买资金到存储在商家的收单机构上的帐户中。例如,收单机构可以是维护商家的帐户的金融机构。例如,由商家处理的交易结果可以被存放到由收单机构的服务器维护的帐户中。

[0080] 在一些实现方式中,该支付网络服务器可以为对应于用户所选的支付选项的发布方服务器产生查询,例如422。例如,用户的帐户可以被链接到一个或多个发布用户的帐户的发布方金融机构("发布方"),诸如银行机构。例如,这种帐户包括但不局限于:信用卡、借记卡、预付卡、支票、存款、金融市场、存款凭证、积蓄(现金)值帐户等。发布方的发布方服务器,例如4o8a-n,可保持用户帐号的细节。在一些实现方式中,例如支付网络数据库407的数据库可存储与发布方相关联的发布方服务器的细节。例如,该数据库可以是响应于结构化查询语言("SQL")命令的关系型数据库。该支付网络服务器可为了发布方服务器细节而查询支付网络数据库。例如,该支付网络服务器可执行包括SQL命令的超文本预处理器

("PHP")脚本来查询数据库以查询发布方服务器的细节。以下提供了说明查询数据库的实质方面的示例性PHP/SQL命令列表：

[0081]
```
<?PHP
header('Content-Type: text/plain');
mysql_connect("254.93.179.112",$DBserver,$password); // access database server
mysql_select_db("ISSUERS.SQL"); // select database table to search
//create query for issuer server data
$query = "SELECT issuer_name issuer_address issuer_id ip_address mac_address
    auth_key port_num security_settings_list FROM issuerTable WHERE account_num
    LIKE '%' $accountnum";
$result = mysql_query($query); // perform the search query
mysql_close("ISSUERS.SQL"); // close database access
?>
```

[0082] 响应于获得该发布方服务器查询，例如422，该支付网络数据库可提供所请求的发布方服务器数据到支付网络服务器，例如423。在一些实现方式中，支付网络服务器可使用发布方服务器数据来为基于与该用户的虚拟钱包相关联的预定义的支付设置和/或用户的支付选项输入而选择的每个发布方服务器产生授权请求，例如424，并提供卡授权请求，例如425a-n到该发布方服务器，例如408a-n。在一些实现方式中，授权请求可包括细节，诸如但不局限于：包含在交易中的对用户的成本、用户的卡帐户细节、用户帐单和/或发货信息，等。例如，支付网络服务器可提供包括与以下提供的示例性列表相似的XML格式的授权请求的HTTP(S)POST消息：

[0083]
```
POST /authorization.php HTTP/1.1
Host: www.issuer.com
Content-Type: Application/XML
Content-Length: 624
<?XML version = "1.0" encoding = "UTF-8"?>
<card_query_request>
    <query_ID>VN813SFK</query_ID>
    <timestamp>2011-02-22 15:22:44</timestamp>
    <purchase_summary>
        <num_products>1</num_products>
        <product>
            <product_summary>Book - XML for dummies</product_summary>
            <product_quantity>1</product_quantity?
        </product>
    </purchase_summary>
    <transaction_cost>822.61</transaction_cost>
    <account_params>
        <account_type>checking</account_type>
        <account_num>123456789012345</account_num>
    </account_params>
    <merchant_params>
        <merchant_id>3FBC841MC</merchant_id>
        <merchant_name>Books & Things, Inc.</merchant_name>
        <merchant_auth_key>1MF48dMCP59CAM27365</merchant_auth_key>
    </merchant_params>
</card_query_request>
```

[0084] 在一些实现方式中，发布方服务器可解析该授权请求，并基于该请求细节可查询数据库，例如用户简档数据库409a-n，以查询与链接到该用户的账户相关联的数据。例如，发布方服务器可发布与以下提供的示例相似的PHP/SQL命令：

[0085]

```
<?PHP
header (' Content-Type : text/plain');
mysql_connect ("254.93.179.112", $DBserver, $password) ; // access
database server mysql_select_db ( "USERS . SQL" ) ; // select database table to
search
//create query for user data
$query = "SELECT user_id user_name user_balance account_type FROM
UserTable
    WHERE account_num LIKE '%' $accountnum" ;
$result = mysql_query ( $query) ; // perform the search query
mysql_close ( "USERS . SQL" ) ; // close database access
?>
```

[0086] 在一些实现方式中，在获得该用户数据后，例如427a-n，该发布方服务器可确定用户是否可以利用帐户上可用的资金支付该交易，例如428a-n。例如，发布方服务器可确定用户在帐户中是否具有足够的余额剩余、与该帐户相关联的足够信用等。基于该确定，发布方服务器可提供授权响应到支付网络服务器，例如，429a-n。例如，发布方服务器可提供与上面示例相似的HTTP(S)POST消息。在一些实现方式中，如果至少一个发布方服务器确定用户不能利用帐户中的可用资金支付该交易，参见例如430-431，那么该支付网络服务器可再次从用户请求支付选项(例如，通过提供授权失败消息431到用户设备并请求用户设备提供新支付选项)，并再尝试该购买交易的授权。在一些实现方式中，如果授权尝试的失败次数超出阈值，该支付网络服务器可退出授权处理，并提供“授权失败”消息到商家服务器、用户设备和/或客户端。

[0087] 参见附图4C，在一些实现方式中，支付网络服务器可获得包括成功授权的通知的授权消息，参见例如430、433，并解析该消息以提取授权细节。当确定用户拥有足够的交易资金时，支付网络服务器可根据该授权请求和/或授权响应产生交易数据记录，例如432，并在交易数据库中存储该交易的细节和关于该交易的授权。例如，支付网络服务器可发布与以下示例列表相似的PHP/SQL命令来在数据库中存储交易数据：

[0088]
```
<?PHP
header('Content-Type: text/plain');
mysql_connect("254.92.185.103",$DBserver,$password); // access database server
mysql_select("TRANSACTIONS.SQL"); // select database to append
mysql_query("INSERT INTO PurchasesTable (timestamp, purchase_summary_list,
    num_products, product_summary, product_quantity, transaction_cost,
    account_params_list, account_name, account_type, account_num,
    billing_addres, zipcode, phone, sign, merchant_params_list, merchant_id,
    merchant_name, merchant_auth_key)
VALUES (time(), $purchase_summary_list, $num_products, $product_summary,
    $product_quantity, $transaction_cost, $account_params_list, $account_name,
    $account_type, $account_num, $billing_addres, $zipcode, $phone, $sign,
    $merchant_params_list, $merchant_id, $merchant_name, $merchant_auth_key)");
    // add data to table in database
mysql_close("TRANSACTIONS.SQL"); // close connection to database
?>
```

[0089] 在一些实现方式中，支付网络服务器可转发授权成功消息，例如433a-b，到用户设备和/或商家服务器。商家可获得该授权消息并根据它确定用户在卡帐户中拥有足够的资金来进行该交易。该商家服务器可为用户添加交易记录到关于授权的交易的一批交易数据。例如，该商家可附加关于该用户交易的XML数据到包括用于已经为各个用户授权的交易的XML数据的XML数据文件，例如434，并在数据库(例如商家数据库404)中存储该XML数据文件，例如435。例如，批XML数据文件可以是与以下提供的示例XML数据结构模板相似的结构：

[0090] <?XML version＝"1.0"encoding＝"UTF-8"?>

[0091] <merchant_data>

[0092] <merchant_id>3FBCR4INC</merchant_id>

[0093] <merchant_name>Books&Things,Inc.</merchant_name>

[0094] <merchant_auth_key>1NNF484MCP59CHB27365</merchant_auth_key>

[0095] <account_number>123456789</account_number>

[0096] </merchant_data>

[0097] <transaction_data>

[0098] <transaction 1>

[0099] …

[0100] </transaction 1>

[0101] <transaction 2>

[0102] …

[0103] </transaction 2>

[0104] .

[0105] .

[0106] .

[0107] <transaction n>

[0108] …

[0109] </transaction n>

[0110] </transaction data>

[0111] 在一些实现方式中，服务器也可以产生购买收据，例如434，并提供该购买收据到客户端，例如436。该客户端可为用户呈递并显示该购买收据，例如437a。在一些实现方式中，用户设备405也可以提供成功授权的通知到用户，例如437b。例如，客户端/用户设备可

呈递网页、电子消息、文本/SMS消息、缓冲语音邮件、发出铃声、和/或播放音频消息等等，并提供包括但不限于以下各项的输出：声音、音乐、音频、视频、图像、触觉反馈、振动警告(例如，诸如智能电话等的支持振动的客户端设备)，等等。

[0112] 参见附图4D，在一些实现方式中，商家服务器可发起一批授权交易的清算。例如，商家服务器可产生批数据请求，例如438，并提供该请求，例如439，到例如商家数据库404的数据库。例如，商家服务器可使用与上面提供的示例相似的PHP/SQL命令来查询关系数据库。响应于该批数据请求，该数据库可提供所请求的批数据，例如440。服务器可利用从数据库中获得的批数据产生批清算请求，例如441，并提供(例如442)该批清算请求到收单机构服务器，例如410。例如，商家服务器可为收单机构服务器提供在消息主体中包括XML格式的批数据的HTTP(S)POST消息。该收单机构服务器可利用所获得的批清算请求产生批支付请求，例如443，并提供该批支付请求到支付网络服务器，例如444。支付网络服务器可解析该批支付请求并为存储在该批支付请求中的每个交易提取交易数据，例如445。支付网络服务器可在例如支付网络数据库407的数据库中为每个交易存储交易数据，例如446。对于每个提取的交易，支付网络服务器可查询例如支付网络数据库407的数据库，例如447-448，以查询发布方服务器的地址。例如，支付网络服务器可使用与上面提供的示例相似的PHP/SQL命令。支付网络服务器可为每个被提取了交易数据的交易产生单个支付请求，例如449，并提供该单个支付请求(例如450)到发布方服务器(例如408)。例如，支付网络服务器可提供与以下示例相似的HTTP(S)POST请求：

[0113]
```
POST /requestpay.php HTTP/1.1
Host: www.issuer.com
Content-Type: Application/XML
Content-Length: 788
<?XML version = "1.0" encoding = "UTF-8"?>
<pay_request>
    <request_ID>CN14IC8N2</request_ID>
    <timestamp>2011-02-22 17:00:01</timestamp>
    <pay_amount>$34.78</pay_amount>
    <account_params>
        <account_name>John Q. Public</account_name>
        <account_type>credit</account_type>
        <account_num>1234567890123456</account_num>
        <billing_address>123 Green St., Norman, OK 98765</billing_address>
        <phone>123-456-7809</phone>
        <sign>/jqp/</sign>
    </account_params>
    <merchant_params>
        <merchant_id>39BCR4IHC</merchant_id>
        <merchant_name>Books & Things, Inc.</merchant_name>
        <merchant_auth_key>1MNr884nCr5SCMn27365</merchant_auth_key>
    </merchant_params>
    <purchase_summary>
        <num_products>1</num_products>
        <product>
            <product_summary>Book - XML for dummies</product_summary>
            <product_quantity>1</product_quantity>
        </product>
    </purchase_summary>
</pay_request>
```

[0114] 在一些实现方式中，发布方服务器产生可产生支付命令，例如451。例如，发布方服务器可发布命令来从用户帐户扣除资金(或添加费用到用户信用卡帐户)。该发布方服务器可发布支付命令(例如452)到存储该用户帐户信息的数据库，例如，用户简档数据库409。发布方服务器可提供资金转帐消息(例如453)到支付网络服务器，支付网络服务器其可转发(例如454)该资金转帐消息到收单机构服务器。下面提供示例性HTTP(S)POST资金转帐消

息：

[0115] POST/clearance.php HTTP/1.1

[0116] Host:www.acquirer.com

[0117] Content-Type:Application/XML

[0118] Content-Length:206

[0119] <?XML version="1.0"encoding="UTF-8"?>

[0120] <deposit_ack>

[0121] <request_ID>CNI4ICNW2</request_ID>

[0122] <clear_flag>true</clear_flag>

[0123] <timestamp>2011-02-22 17:00:02</timestamp>

[0124] <deposit_amount>$34.78</deposit_amount>

[0125] </deposit_ack>

[0126] 在一些实现方式中，收单机构服务器可解析该资金转帐消息，并关联该交易(例如，利用在上述例子中的request_ID字段)到商家。该收单机构服务器然后可以移转资金转帐消息中指定的资金到商家的账户，例如455。

[0127] 附图5A-E示出了说明在SNAP的一些实施例中，执行快拍移动支付的示例性方面的逻辑流程图，例如快拍移动支付执行(“SMPE”)部件500。参见附图5A，在一些实现方式中，用户可能希望通过商家在线站点或在商家商店中从商家购买产品、服务、报价等(“产品”)。该用户可通过客户端与商家服务器通信。例如，用户可提供用户输入(例如501)到客户端中，指示用户希望结帐(虚拟)购物车中的购物物品。客户端可产生结帐请求，例如502，并提供该结帐请求到商家服务器。商家服务器可从该客户端获得结帐请求，并从该结帐请求提取结帐细节(例如XML数据)，例如503。例如，商家服务器可使用诸如如下参见附图14的讨论所描述的示例解析器的解析器。商家服务器从结帐请求中提取该产品数据以及客户端数据。在一些实现方式中，商家服务器可查询(例如504)商家数据库来获得产品数据，例如505，诸如产品价格、营业税、报价、折扣、回报，和/或其它信息来处理该购买交易。

[0128] 响应于获得该产品数据，该商家服务器可根据用户的安全设置产生(例如506)QR支付代码和/或安全显示元件(参见例如358)。例如，商家服务器可产生包含有支付网络处理该购买交易所要求的产品信息以及商家信息的QR代码。例如，该商家服务器可首先实时产生自定义的、用户特定的具有时间受限的有效期的商家-产品XML数据结构，诸如下面提供的示例性“QR_data”XML数据结构：

[0129]
```
<QR_data>
    <session_ID>4OFD8RG54</session_ID>
    <timestamp>2011-02-22 15:22:43</timestamp>
    <expiry_lapse>00:00:30</expiry_lapse>
    <transaction_cost>$34.78</transaction_cost>
    <user_ID>john.q.public@gmail.com</user_ID>
    <client_details>
            <client_IP>192.168.23.126</client_IP>
            <client_type>smartphone</client_type>
            <client_model>HTC Hero</client_model>
            <OS>Android 2.2</OS>
```

[0130]
```
                <app_installed_flag>true</app_installed_flag>
            </client_details>
            <secure_element>www.merchant.com/securedyn/6394733/123.png</secure_element>
            <purchase_details>
                <num_products>1</num_products>
                <product>
                    <product_type>book</product_type>
                    <product_params>
                        <product_title>XML for dummies</product_title>
                        <ISBN>978-3-16-148710-0</ISBN>
                        <edition>2nd ed.</edition>
                        <cover>hardbound</cover>
                        <seller>bestbuybooks</seller>
                    </product_params>
                    <quantity>1</quantity>
                </product>
            </purchase_details>
            <merchant_params>
                <merchant_id>3FWCR41MC</merchant_id>
                <merchant_name>Books & Things, Inc.</merchant_name>
                <merchant_auth_key>1MNF1S4MCPS9CHM27365</merchant_auth_key>
            </merchant_params>
        <QR_data>
```

[0131] 在一些实现方式中，商家可利用XML数据产生QR代码。例如，商家服务器可使用在http://phpqrcode.sourceforge.net/可用的PHP QR代码开源(LGPL)库以用于产生QR代码、2维条型码。例如，商家服务器可发布与以下提供的示例性命令相似的PHP命令：

[0132] <?PHP

[0133] header('Content-Type:text/plain');

[0134] //Create QR code image using data stored in $data variable

[0135] QRcode::png($data,'qrcodeimg.png');

[0136] ?>

[0137] 商家服务器可提供该QR支付代码到客户端，例如506。客户端可获得该QR支付代码，并在与客户端设备相关联的显示屏幕上显示该QR代码，例如507。在一些实现方式中，用户可使用用户设备，例如509，来捕捉由该客户端设备呈现的QR代码以用于支付处理。该客户端设备可解码该QR代码以提取嵌入在该QR代码中的信息。例如，客户端设备可使用在http://code.google.com/p/zxing/可用的应用程序，诸如ZXing多格式1D/2D条型码图像处理库，以从该QR代码提取信息。在一些实现方式中，用户可提供支付输入到用户设备中，例如508。当获得用户购买输入时，该用户设备可产生卡授权请求，例如509，并提供该卡授权请求到支付网络服务器。

[0138] 参见附图5B，在一些实现方式中，支付网络服务器可解析该卡授权请求，例如510，并为对应于用户所选的支付选项的发布方服务器产生查询，例如511。在一些实现方式中，支付网络数据库可存储与发布方相关联的发布方服务器的细节。响应于获得该发布方服务器查询，支付网络数据库可提供，例如，512，所请求的发布方服务器数据到该支付网络服务器。在一些实现方式中，该支付网络服务器可使用发布方服务器数据来为每个发布方服务器产生授权请求，例如，425134，并提供卡授权请求到发布方服务器。

[0139] 在一些实现方式中，发布方服务器可解析该授权请求，并基于该请求的细节，可为与链接到该用户的帐户相关联的数据查询用户简档数据库。在一些实现方式中，当获得该用户数据后，发布方服务器可确定该用户是否可以利用帐户中的可用资金支付交易，例如517。例如，发布方服务器可确定用户是否具有足够余额剩余在账户中、是否具有与该帐户相关联的足够信用等。基于该确定，发布方服务器可提供授权响应到支付网络服务器，例如

518。在一些实现方式中，如果至少一个发布方服务器确定(例如519)用户不能利用帐户中的可用资金支付该交易，参见例如520，选项“否”，那么该支付网络服务器可再次从用户请求支付选项(参见例如521，选项“否”，通过提供授权失败消息到用户设备并请求用户设备提供新支付选项)，并再尝试该购买交易的授权。在一些实现方式中，如果授权尝试的失败次数超出阈值，参见例如521，选项“是”，那么该支付网络服务器可退出该授权处理，并提供“授权失败”消息到该商家服务器、用户设备和/或客户端，例如522。

[0140] 在一些实现方式中，该支付网络服务器可获得包括成功授权的通知的授权消息，参见例如520，选项“是”，并解析该消息以提取授权细节。当确定用户拥有足够的交易资金后，支付网络服务器可根据该授权请求和/或授权响应产生交易数据记录，例如523，并在交易数据库中存储该交易的细节和涉及该交易的授权，例如524。

[0141] 参见附图5C，在一些实现方式中，该支付网络服务器可转发授权成功消息(例如525)到用户设备和/或商家服务器，有时通过收单机构服务器转发，例如526。该商家可解析该授权消息，例如528，并根据它确定用户在卡帐户中拥有足够资金来进行该交易，参见例如529。该商家服务器可为用户添加一条交易记录到涉及授权交易的一批交易数据中，参见例如530-531。在一些实现方式中，该商家服务器也可以产生购买收据，例如532，并提供该购买收据到客户端。该客户端可为用户呈递并显示该购买收据，例如534。在一些实现方式中，用户设备405也可以提供成功授权的通知给用户。

[0142] 参见附图5D-E，在一些实现方式中，商家服务器可发起一批授权交易的清算。例如，该商家服务器可产生批数据请求，例如535，并提供该请求(例如536)到数据库，例如商家数据库。响应于该批数据请求，该数据库可提供所请求的批数据，例如536。服务器可利用从数据库获得的批数据产生批清算请求，例如537，并提供该批清算请求到收单机构服务器。收单机构服务器可利用该获得的批清算请求产生(例如539)批支付请求，并提供该批支付请求到该支付网络服务器。该支付网络服务器可解析该批支付请求，并为存储在该批支付请求中的每个交易提取交易数据，例如540-542。该支付网络服务器可为例如支付网络数据库的数据库中的每个交易存储该交易数据，例如543-544。对于每个提取的交易，支付网络服务器可查询(例如545-546)例如支付网络数据库的数据库以查询发布方服务器的地址。该支付网络服务器可为每个被提取交易数据的交易产生单个支付请求，例如547，并提供该单个支付请求到关联的发布方服务器。

[0143] 在一些实现方式中，发布方服务器可产生支付命令，例如548-549。例如，发布方服务器可发布命令来从用户帐户扣除资金(或添加费用到用户的信用卡帐户)。发布方服务器可发布支付命令到存储用户的帐户信息的数据库(例如用户简档数据库)，例如549。该发布方服务器可提供资金转帐消息到可转发该资金转帐消息到收单机构服务器的支付网络服务器，例如551。在一些实现方式中，收单机构服务器可解析该资金转帐消息，并关联该交易(例如，利用在上述例子中的request_ID字段)到商家。该收单机构服务器然后可以移转资金转帐消息中指定的资金到商家的账户，例如553-555。

[0144] 图6A-B示出了在该SNAP的一些实施例中，说明处理快速响应代码的示例方面的逻辑流程图，例如快速响应代码处理(“QRCP”)部件600。参见附图6A，在一些实现方式中，在用户设备上执行的虚拟钱包应用可确定在操作地连接至该用户设备的照相机获得的图像帧中是否已经捕捉到QR代码，并也可以确定该QR代码的类型、内容。利用这种信息，该虚拟钱

包应用可重定向用户的用户体验和/或发起购买、更新该虚拟钱包应用的方面等等。例如，该虚拟钱包应用可通过操作地连接至用户设备的照相机触发图像帧的捕捉，601。该虚拟钱包应用可使用图像分割算法来标识图像中的前景，602，并可裁剪图像的其余部分以减少图像中的背景噪声，603。该虚拟钱包应用可确定前景图像是否包括QR代码，根据该QR代码可以可靠地读取数据(例如，如果图像不包括QR代码，或该QR代码被部分地裁剪、模糊等等可能无法可靠地读取数据)，604。例如，该虚拟钱包应用可使用代码库，诸如在http://code.google.com/p/zxing/可获得的比如ZXing多格式1D/2D条形码图像处理库，以尝试并从该QR代码提取信息。如果该虚拟钱包应用能够检测出QR代码(605，选项“是”)，那么该虚拟钱包应用可解码该QR代码，并从该QR代码提取数据。如果该虚拟钱包应用不能检测出QR代码(605，选项“否”)，那么该虚拟钱包应用可在图像上试图执行光学字符识别。例如，，该虚拟钱包应用可使用在www.pixeltechnology.com/freewarw/tessnet2可获得的Tesseract C++开源OCR引擎，来执行光学字符识别，606。因此该虚拟钱包应用可获得编码在该图像中的数据，并如果该数据可以被虚拟钱包应用处理则可继续进行。该虚拟钱包应用可利用在提取的数据中标识的字段查询数据库，以查询该QR代码类型，608。例如，该QR代码可包括发货单/帐单、优惠券、汇单(例如，P2P移账中的)、新帐户信息包、产品信息、购买命令、URL导航指令、浏览器自动脚本、它们的组合等。

[0145] 在一些实施例中，该QR代码可包括关于将被添加到该虚拟钱包应用的新帐户的数据(参见609)。该虚拟钱包应用可查询该新帐户(如从提取的数据中获得)的发布方，以查询与该新帐户相关联的数据，610。该虚拟钱包应用可比较发布方提供的数据和从该QR代码提取的数据，611。如果该新帐户被确认(611，选项“是”)，则该虚拟钱包应用可利用该新帐户的细节更新该钱包凭证，613，并利用来自该QR代码的数据更新该虚拟钱包应用的快拍历史，614。

[0146] 参见附图6B，在一些实施例中，该QR代码可包括关于使用该虚拟钱包应用的帐单、发货单或用于购买的优惠券的数据(参见615)，该虚拟钱包应用可查询与该购买(如从提取的数据中获得的)相关联的商家，以查询与该帐单、发货单或用于购买的优惠券相关联的数据(例如报价细节、报价ID、期满时间等等)，616。该虚拟钱包应用可比较商家提供的数据和从该QR代码提取的数据，617。如果该帐单、发货单或用于购买的优惠券被确认(618，选项“是”)，那么该虚拟钱包应用可产生包括该QR编码数据的数据结构(参见例如上述参 考图4-5的说明中的XML QR_data结构)以用于产生并提供卡授权请求，619，并且使用来自该QR代码的数据更新该虚拟钱包应用的快拍历史620。

[0147] 在一些实施例中，该QR代码可包括用于该虚拟钱包应用的产品信息、命令、用户导航指令等等(参见621)。该虚拟钱包应用可使用编码在QR中的信息查询产品数据库。该虚拟钱包应用可提供各种特征，包括但不限于：显示产品信息、重定向用户到：产品页面、商业网站、商业网站上的产品页面、在商业网站添加物品到用户购物车等等。在一些实现方式中，该虚拟钱包应用可执行诸如上面描述的过程以用于待处理的和/或用户选择用于处理(例如根据快拍历史)的任何图像帧。

[0148] 图7示出了在该SNAP一些实施例中，说明虚拟钱包应用的示例特征的概述的用户界面图。图7示出了虚拟钱包移动应用700的各种示例性特征的说明。显示的一些特征包括钱包701、经由TWITTER、FACEBOOK等等的社交融合、报价和税703、快拍移动购买704、警告

705以及安全、设置和分析796。以下更加详细地探索这些特征。

[0149] 图8A-G示出了在该SNAP的一些实施例中，说明购物模式中的虚拟钱包应用的示例特征的用户界面图。参见附图8A，该虚拟钱包移动应用的一些实施例帮助并极大地增强了消费者的购物体验。如图8A所示，消费者可获得各种购物模式来细读。在一种实现方式中，例如，用户可通过在用户界面底部选择商店图标810来启动该购物模式。用户可在检索字段812中键入物品来搜索和/或添加物品到购物车811。用户也可以通过说出将被检索和/或添加到购物车的物品的名称或描述到麦克风813中来使用语音激活的购物模式。在进一步的实现方式中，用户也可以选择其它购物选项814，比如当前物品815，帐单816，地址薄817，商家818和本地邻近819。

[0150] 在一个实施例中，例如，用户可选择选项当前物品815，如图8A的用户界面的最左边所示。当选择了当前物品815选项时，可以显示中间的用户界面。如图所示，中间的用户界面可提供用户的购物车811中的物品815a-h的当前列表。用户可选择一个物品，例如物品815a，来浏览所选物品和/或来自相同商家的其他物品的产品说明815j。也可以随着捕捉实施快拍移动购买交易必需的信息的QR代码815k一起显示价格和总的应付信息。

[0151] 参见图8B，在另一个实施例中，用户可选择帐单816选项。当选择帐单816 选项后，用户界面可显示来自一个或多个商家的帐单和/或收据816a-h的列表。紧挨着每一个帐单可以显示附加信息，诸如访问日期、是否呈现来自多个商店的物品、最后帐单支付日期、自动支付、物品数量等。在一个例子中，可选择日期为2011年1月20日的钱包购物帐单816a。该钱包购物帐单选择可显示提供关于所选择的帐单的各种信息的用户界面。例如，用户界面可显示购买的物品816k的列表，<<816i>>，物品总数量和相应价值。例如，7个物品价值$102.54处于选择的钱包购物帐单上。用户现在可选择任何物品并选择再次购买来添加购买该物品。用户也可以从最后时间刷新报价816j来清除任何无效的报价和/或搜索可适合当前购买的新报价。如图8B中示出的，用户可选择两个物品用于重复购买。一旦添加，可显示消息816i来确认两个物品的添加，其得出处于购物车14中的物品的总数。

[0152] 参见图8C，在又一个实施例中，用户可选择地址薄选项817来浏览地址簿817a，其包括联系人817b的列表和产生任何汇款或支付。在一个实施例中，地址簿可使用联系人的姓名和可用的和/或优选的支付模式来标识每个联系人。例如，联系人Amanda G.可以是经由如图标817c表示的社交支付(例如经由FACEBOOK)来支付。在另一个示例中，钱可以经由如QR代码图标817d表示的QR代码被转送到Brian S.。在另一示例中，Charles B.可经由近场通信817e、蓝牙817f和电子邮件817g接受支付。支付也可以经由USB 817h(例如，通过两个移动设备的物理连接)和其它诸如TWITTER的社交渠道进行。

[0153] 在一种实现方式中，用户可选择JoeP.来支付。如用户界面中所示，紧挨着Joe P.的名字旁边，JoeP.具有电子邮件图标8i7g，表示Joe P.接受经由电子邮件的支付。当选择他的名字时，用户界面可显示他的联系信息，诸如电子邮件、电话等等。如果用户希望通过非电子邮件的方法对Joe P.支付，则该用户可添加另一个转帐模式817j到他的联系信息并进行支付转帐。参见图8D，用户可以配有屏幕817k，其中用户可以输入金额来发送给Joe，以及添加其它文本来将上下文提供给Joe以用于支付交易8171。用户可以通过图形用户界面元件817m选择可以联系Joe的模式(例如SMS、电子邮件、社交网络)。作为用户类型，也可以提供文本输入以便在GUI元件817n内浏览。当用户已经完成必要信息的输入时，用户可以按

下发送按钮817o来发送该社交消息给Joe。如果Joe也具有虚拟钱包应用，Joe将能在该应用内或直接在该社交网络(例如Twitter™，Facebook®等等)的网站浏览817p社交支付消息。消息可从各个社交网络以及其它源(例如SMS、电子邮件)聚集。适合于每个消息传递方式的兑换方法可以与社交支付消息一起被指示。在图8D的说明中，Joe接收的SMS 817q表示Joe可以通过答复SMS并输入散列标签值“#1234”来兑换经由SMS获得的$5。在相同说明中，Joe已经经由Facebook®接收到消息817r，其中包括Joe可以激活来启动$25支付的兑换的URL链接。

[0154] 参见图8E，在一些其它的实施例中，用户可从购物模式中的选项的列表选择商家818来浏览商家818a-e的选择列表。在一种实现方式中，列表中的商家可以与该钱包发生联系，或与钱包具有联系关系。在另一个实现方式中，商家可包括满足用户定义或其他标准的商家列表。例如，该列表可以是用户确定的(curated)一个、用户最频繁购物或花费多于x总量的金额或连续三个月购物的商家等。在一种实现方式中，用户可进一步选择一个商家，例如Amazon 818a。然后用户可以通过商家的清单导航来发现感兴趣的物品，诸如818f-j。直接通过钱包以及在没有从独立的页面访问商家站点的情况下，用户可从Amazon818a的目录选择物品818j。如图8D的用户界面的最右端所示，然后可以将所选物品添加到购物车。消息818k表示所选物品已经被添加到购物车，以及现在购物车中的物品的更新数量是13。

[0155] 参见附图8F，在一个实施例中，可以有本地邻近选项，其可以由用户选择来浏览地理上非常邻近于用户的商家列表。例如，商家819a-e的列表可以是位置接近于该用户的商家。在一种实现方式中，该移动应用可基于用户的位置进一步标识用户何时在商店中。例如，当用户非常邻近该商店时，位置图标819d可以紧挨着商店(例如，Walggreens)被显示。在一种实现方式中，如果用户离开该商店(例如，Walgreens)，该移动应用可周期性地刷新它的位置。在进一步实现方式中，用户可通过该移动应用导航选择的Walgreens商店的报价。例如，用户可使用该移动应用导航到Walgreens的走廊5上可获得的物品819f-j。在一种实现方式中，用户可从他或者她的移动应用选择玉米819i来添加到购物车819k。

[0156] 参见图8G，在另一个实施例中，本地邻近选项819可包括商店地图，尤其是实时地图特征。例如，当选择Walgreens商店时，用户可启动显示示出商店组织结构和用户位置(由黄色圆圈指示)的地图819m的走廊地图8191。在一 种实现方式中，用户可容易地配置地图来添加一个或多个其它用户(例如，用户的孩子)来共享在商店内的彼此的位置。在另一个实现方式中，用户可以具有选项来在地图中启动类似街道浏览的“商店浏览”。商店浏览819n可显示用户周围的图像/视频。例如，如果用户即将进入走廊5，商店浏览地图可显示走廊5的视图。此外，用户可使用导航工具8190操纵地图的方向来向前、向后、向右、向左，以及顺时针和逆时针方向旋转移动该商店视图。

[0157] 附图9A-F显示在SNAP的一些实施例中，说明在支付模式中的虚拟钱包应用的示例特征的用户接口图。参见图9A，在一个实施例中，该钱包移动应用可经由钱包模式910给用户提供用于支付交易的多个选项。在一种实现方式中，示出了用于进行支付的示例性用户界面911。该用户界面可清楚地标识用于该交易的金额912和货币913。该金额可以是应付金额并且该货币可包括诸如美元和欧元的真实货币，以及也包括诸如回报点的虚拟货币。交易914的金额也可以被显著地显示在该用户界面上。用户可选择资金标签916来选择一个或多个支付形式917，其可包括各个信用、借记、赠品、回报和/或预付卡。该用户也可以具有利

用回报点支付全部或部分的选项。例如，该用户界面上的图形指示符918示出了可用点的数目，该图形指示符919示出了将使用的对应付金额234.56的点数以及该点数在选择的货币(USD，例如)中的等价920。

[0158] 在一种实现方式中，该用户可从多个源组合资金来支付该交易。显示在该用户界面上的金额915可提供迄今由选择的支付形式(例如，发现卡以及回报点)所覆盖的总资金的金额的指示。用户可选择另一个支付形式或调整将从一个或多个支付形式借记的金额，直到金额915匹配应付金额914。一旦用户定下将从一个或多个支付形式借记的金额，则可开始付款授权。

[0159] 在一种实现方式中，用户可通过选择隐匿按钮922来选择交易的安全授权，来有效地隐匿或匿名一些(例如预先配置的)或全部识别信息，以便当用户选择支付按钮921的时候，交易授权是以安全且匿名的方式进行的。在另一个实现方式中，用户可选择支付按钮921，其可以使用标准授权技术用于交易处理。在另一实现方式中，当用户选择社交按钮923的时候，关于该交易的消息可以被传递到一个或多个社交网络(由用户建立的)，其可在社交论坛中发布或宣布该购买交易，诸如墙报或tweet。在一种实现方式中，用户可选择社交支付处理选项923。该指示符924可示出进行中的授权和发送社交共享数据。

[0160] 在另一个实现方式中，对于某些购买活动可以激活限制支付模式925，诸如规定购买。可以根据由发布方、保险公司、商家、支付处理方和/或其它实体定义的规则来激活该模式，来帮助特殊货物和服务的处理。在此模式中，用户可按照资金标签向下翻卷支付形式926的列表来选择特殊的帐户，诸如灵活支付帐户(FSA)927、健康储蓄帐户(HAS)等，以及将被记入选择的帐户的金额。在一种实现方式中，这种限制支付模式1925处理可禁止购买信息的社交共享。

[0161] 在一个实施例中，通过输入资金用户界面928，钱包移动应用可帮助资金的输入。例如，失业的用户可通过钱包移动应用获得失业救济资金929。在一种实现方式中，提供这些资金的实体也可以配置使用这些资金的规则，如处理指示符消息930所示。该钱包可事先读取并应用该规则，并可拒绝未能满足该规则设定的标准的利用该失业基金的任何购买。示例性标准包括，例如，商家种类编码(MCC)，交易时间，交易位置等。举例来说，与具有MCC 5411的杂货商家的交易是被批准的，而与具有MCC 5813的酒吧商家的交易是被拒绝的。

[0162] 参见附图9B，在一个实施例中，该钱包移动应用可基于诸如用户位置、偏好以及偏好的币值因素，帮助动态支付优化。例如，当用户处于美国的时候，该国指示符931可显示美国的标记并可将货币933设置为美国。在此外的实现方式，钱包移动应用可自动重排顺序，其中支付形式935被列出以反映各种形式的支付的流行程度或可接受度。在一种实现方式中，该排列可反映用户的偏好，其不能由该钱包移动应用改变。

[0163] 类似地，当德国用户在德国操作钱包的时候，该移动钱包应用用户界面可以被动态地更新来反映该国的操作932和货币934。在此外的实现方式中，钱包应用可重排顺序，其中不同的支付形式936被基于那个国家的接受水平而列出。当然，这些支付形式的顺序可以由用户更改来适应他或者她自己的偏好。

[0164] 参见附图9C，在一个实施例中，钱包移动应用用户界面中的收款人标签937可帮助用户选择一个或多个接收在资金标签中选择的资金的收款人。在一种实现方式中，该用户界面可显示全部收款人938的列表，用户已经早先与他们做过交易，或者可以用来交易。用

户然后可以选择一个或多个收款人。收款人938可包括较大商家诸如Amazon.com公司，和个人诸如Jane P.Doe。紧挨着每个收款人名字可以显示该收款人接受的支付模式的列表。在一种实现方式中，用户可选择收款人Jane P.Doe 939来接收支付。一旦选择，该用户界面可显示涉 及该收款人的附加标识信息。

[0165] 参见附图9D，在一个实施例中，模式标签1940可帮助选择该收款人接受的支付模式。多个支付模式可用于选择。示例性模式包括，蓝牙941、无线942、借助用户获得的QR代码的快拍移动943、安全芯片944、TWITTER945、近场通信(NFC)946、蜂窝947、借助用户提供的QR代码的快拍移动948、USB949和FACEBOOK 950，等等。在一种实现方式中，仅仅是由收款人接受的支付模式可以被用户选择。其它非接受的支付模式可以是禁止的。

[0166] 参见附图9E，在一个实施例中，报价标签951可提供实时报价用于用户选择，其与用户的购物车中的物品有关。用户可从适用报价952的列表选择一个或多个报价用于兑换。在一种实现方式中，一些报价可以被组合，而其它不能。当用户选择不能和其他报价组合的报价的时候，未选择的报价可以被禁止。在另一种实现方式中，由钱包应用的推荐引擎推荐的报价可以由指示符标识，诸如953所显示的那个。在另一种实现方式中，用户可通过扩展报价行来读取报价的细节，如用户界面中的954所示。

[0167] 参考图9F，在一个实施例中，社交标签955可帮助整合钱包应用与社交渠道956。在一种实现方式中，用户可选择一个或多个社交渠道956并且可以通过提供社交渠道用户名和密码957到钱包应用并且登陆958来登陆以从钱包应用选择社交渠道。用户然后可以通过整合的社交渠道来使用社交按钮959发送或接收金额。在另一种实现方式中，用户可通过整合的社交渠道发送社交共享数据，诸如购买信息或链接。在另一个实施例中，用户提供的登录凭证可允许SNAP来参加截取解析。

[0168] 图10示出了在该SNAP的一些实施例中，说明历史模式中的虚拟钱包应用的示例特征的用户接口图。在一个实施例中，用户可以选择历史模式1010来浏览先前购买历史并对那些先前购买执行各种动作。例如，用户可在检索条1011中输入商家识别信息，诸如名称、产品、MCC等。在另一个实现方式中，用户可通过点击麦克风图标1014来使用语音激活的检索特征。钱包应用可查询该移动设备或其它地方(例如，远离该移动设备的一个或多个数据库和/或表格)中的存储区域来查询匹配该检索关键词的交易。该用户界面然后可以显示诸如交易1015的查询的结果。用户界面也可以识别该交易的日期1012、涉及该交易的商家以及物品1013、确认进行了交易、该交易的金额和任何其它相关信息的收 据的条型码。

[0169] 在一种实现方式中，用户可选择例如交易1015的交易来浏览该交易的细节。例如，用户可以浏览与该交易相关联的物品的细节和每个物品的金额1016。在另一种实现方式中，用户可选择显示选项1017来浏览对于该交易或该交易中的物品用户可采取的动作1018。例如，用户可添加照片到该交易(例如用户和用户购买的iPad的图片)。在另一种实现方式中，如果用户早先通过社交渠道共享了该购买，可以产生包括该照片的帖子并发送到该社交渠道用于公布。在一种实现方式中，任何共享可以是可选择的，以及不通过社交渠道共享该购买的用户仍然可以通过他或者她直接从钱包应用的历史模式选择的一个或多个社交渠道共享该照片。在另一个实现方式中，用户可以添加该交易到群组，诸如用户建立的公司开支、家庭开支、差旅开支或其它类别。这种群组可以帮助开支的年终结算、工作开支报告的提交、增值税(VAT)退税的提交、人员开支等。在另一实现方式中，用户可以购买交易

中购买的一个或多个物品。用户然后可以在没有去往商家目录或站点来发现该物品的情况下执行交易。在另一种实现方式中，用户也可以在交易中将一个或多个物品放入购物车用于以后购买。

[0170] 在另一个实施例中，该历史模式可以提供便利以用于获得并显示该交易中的物品的评价1019。该评价的来源可以是用户、用户的朋友(例如，来自社交渠道、联系人等等)、从该网页聚集的浏览等。在一些实现方式中，该用户界面也可以允许用户张贴消息到社交渠道(例如TWITTER或FACEBOOK)的其它用户。例如，显示区域1020显示两个用户之间的FACEBOOK消息交换。在一种实现方式中，用户可通过消息1021共享链接。具有嵌入到产品的链接的这种消息的选择可允许用户浏览该产品的说明和/或直接从历史模式购买该产品。

[0171] 在一个实施例中，该历史模式也可以包括用于输出收据的工具。输出收据弹出1022可提供用于输出历史中的交易的收据的多个选项。例如，用户可以使用一个或多个选项1025，其包括保存(到本地移动存储器、到服务器、到云帐户等)、打印到打印机、传真、电子邮件等。用户可以使用他或者她的地址簿1023来查找用于输出的电子邮件或传真号码。用户也可以指定格式选项1024用于输出收据。示例性格式选项包括但不限于：文本文件(.doc，.txt，.rtf，.iif等等)、电子数据表(.csv，.xls等等)、图像文件(.jpg，.tff，.png，等等)、便携式文档 格式(.pdf)、附录(.ps)等。用户然后可以点击或轻敲输出按钮1027来启动收据输出。

[0172] 图11A-F示出了在该SNAP的一些实施例中，说明快拍模式中的虚拟钱包应用的示例特征的用户接口图。参见附图11A，在一些实施例中，用户可以选择快拍模式1101来访问快拍特征。在各种实施例中，虚拟钱包应用能够快拍并识别各种物品。例如，虚拟钱包应用能快拍并识别购买发票1103、优惠券104、钱(例如，个人对个人转帐中发送的)1105、账单(例如，公用事业，等等)1106、收据(例如用于存储，开支报告，等等)1107，支付帐户(例如，以添加新的信用/借计/预付卡到该虚拟钱包应用)1108。用户能够通过激活图形用户界面元件1102而随时返回到购物屏幕。在一些实施例中，用户能设置存储在快拍的物品应被发送到(参见1109)的用户的虚拟钱包应用内的购物车或希望列表的名称。在一些实施例中，该虚拟钱包应用可允许用户创建快拍的物品应被添加到的新的购物车或希望列表。

[0173] 在一个实施例中，用户可以选择快拍模式1110来访问它的快拍特征。该快拍模式可以处理任何机器可读的数据表示。这种数据的示例可包括线性和2D条形码，诸如UPC码和QR代码。这些代码可以在收据、产品包装等上找到。该快拍模式也可以处理和操作收据、产品、报价、信用卡或其它支付设备等的图片。图11A示出了快拍模式中的示例性用户界面。用户可以使用他或者她的移动电话来对QR代码1115和/或条型码1114拍照。在一种实现方式中，条1113和快拍框1115可以帮助用户正确地对这些代码拍快照。例如，如图所示，快拍框1115未捕捉代码1116的全部。因而，在这次浏览中捕捉的代码不是可解析，因为该代码中的信息可能是不完整的。这通过表示该快拍模式仍然在寻找代码的条1113上的消息来表示。用户可以更改照相机的变焦水平1117来促进对QR代码拍快照。当代码1116被快拍框1115完全地框住时，条消息可以被更新为例如“快拍发现”。在一种实现方式中，当找到该代码后，用户可以使用移动设备照相机来启动代码捕捉(参见1120)。在另一个实现方式中，快拍模式可以使用该移动设备照相机自动给该代码拍快照(参见1119)。在一些实现方式中，虚拟钱包应用可以在存储QR代码或在交易中使用它以前可选地应用全球定位系统标签(参见

1118)到该QR代码。

[0174] 参见图11B,在一个实施例中,快拍模式可有助于支付再分配张贴交易。例如,用户可从零售商Acme超市购买杂货和规定物品。用户可以无意中或为了结帐方便,例如,使用他或者她的Visa卡来支付杂货和规定物品。然而,该用户可能具有可用于支付规定物品的FSA帐户,以及其将提供用户税款利益。在这种情况中,该用户可以使用快拍模式来启动交易再分配。

[0175] 如图所示,用户在检索条2121中输入检索项(例如,帐单)。用户然后可以在标签1122中识别用户希望再分配的收据1123。作为替代地,用户可以直接给收据上的条型码的图片拍快照,并且快拍模式可以使用来自该条型码的信息产生并显示收据1123。现在用户可以重新分配1125。在一些实现方式中,用户也可以对交易提出质疑1124或存档该收据1126。

[0176] 在一种实现方式中,当选择了重新分配按钮1125时,钱包应用可以执行收据的光学字符识别(OCR)。收据中的每个物品然后可以被审查来识别一个或多个物品可以被记入到哪个支付设备或账户以用于税款或诸如现金返还、回报点等等的其它收益。在此例子中,如果被记入到用户的Visa卡的处方药物被记入到用户的FSA,则有税款收益。钱包应用然后可以执行该再分配作为末端。该再分配处理可以包括钱包联系支付处理方来贷记处方药物的金额到该Visa卡并借记相同金额到用户的FSA帐户。在作为替代的实施方式中,支付处理方(例如Visa or MasterCard)可获得并OCR该收据,识别物品和支付帐户以用于再分配并执行该再分配。在一种实现方式中,钱包应用可请求用户确认将所选物品的计费再分配给另一个支付帐户。在再分配处理完成以后可以产生收据1127。如所讨论的,该收据示出一些费用已经从Visa账户移动到FSA。

[0177] 参见图11C,在一个实施例中,快拍模式可以通过诸如条型码或QR代码的支付代码帮助支付。例如,用户可以对还没完成的交易的QR代码拍快照。该QR代码可以被显示在商家POS终端处、网站,或网页应用,并可以被与识别用于购买物品的信息、商家细节以及其它相关的信息一起编码。当用户快拍诸如QR代码的时候,快拍模式可以解码该QR代码中的信息并可以使用该解码的信息来产生收据1132。一旦该QR代码被识别,导航条1131可以指出支付代码被识别。现在用户可以具有选项来添加到购物车1133、利用默认支付帐户支付1134或利用钱包支付1135。

[0178] 在一种实现方式中,用户可以决定利用默认1134支付。在这个钱包示例中,钱包应用然后可以使用用户的默认支付方法来完成该购买交易。当完成该交易 后,可以自动产生收据用于证明购买。用户界面也可以被更新以提供其它选项用于处理已完成交易。示例选项包括社交1137来与别人共享购买信息,如关于图11B所讨论的重新分配1138以及存档1139来存储该收据。

[0179] 参见图11D,在一个实施例中,快拍模式也可以帮助报价识别、应用以及存储以备将来之用。例如,在一个实现方式中,用户可以快拍报价代码1141(例如,条形码、QR代码等)。钱包应用然后可以根据编码在该报价代码中的信息产生报价文本1142。用户可以对报价代码执行多个动作。例如,用户使用查找按钮1143来查找接受该报价代码的所有商家、接受该报价代码的附近商家、来自取得该报价代码资格的商家的产品等。用户也可以使用该添加到购物车按钮1144来应用该报价代码到当前在购物车中的物品。此外,用户也可以通

过选择保存按钮1145来保存该报价以备将来之用。

[0180] 在一种实现方式中，报价或优惠券1146被应用之后，用户可具有选项来使用查找来查找取得资格的商家和/或产品，该用户可以使用1148进入该钱包，以及用户也可以保存该报价或优惠券1146用于后来使用。

[0181] 参见图11E，在一个实施例中，快拍模式也可以提供便利以用于添加资金来源到钱包应用。在一个实现方式中，诸如信用卡、借记卡、预付卡、智能卡的支付卡以及其它支付帐户可具有关联代码，诸如条形码或QR代码。这种代码可具有编码在其中的支付卡信息，包括但不限于，名称，地址，支付卡类型，支付卡帐户细节，余额，花费限制，回报余额等。在一种实现方式中，该代码可以在物理支付卡的表面被发现。在另一个实现方式中，可以通过访问关联的在线帐户或另一个安全位置获得该代码。然而，在另一个实现方式中，该代码可以被打印在伴随支付卡的信封上。在一种实现方式中，用户可以快拍该代码的图片。钱包应用可以识别支付卡1151并显示编码在支付卡中的文本信息1152。该用户然后可以通过选择验证按钮1153执行该信息1152的验证。在一种实现方式中，该验证可以包括联系该支付卡的发布方用于确认解码的信息1152以及任何其它相关信息。在一种实现方式中，用户可以通过选择“添加到钱包”按钮1154来添加该支付卡到钱包。添加支付卡到钱包的指令可以促使支付卡作为按照图9A所讨论的资金标签916的支付形式之一出现。用户也可以通过选择取消按钮1155取消输入支付卡作为资金来源。当支付卡已经被添加到钱包时，用户界面可以被更新以通过通知显示1156来指示输入完成。用户然后可以访问钱包1157以开始使用添加的支付卡作为资金来源。

[0182] 参见附图11F，在一些实现方式中，该虚拟钱包应用可通过处理该QR代码识别产品，以及可提供与该产品有关的信息，以及与用于购买该产品、辅助服务等有关的信息。例如，该虚拟钱包应用可提供窗口1161，其中该虚拟钱包应用可显示图像、产品说明书、价格、商家信息等(参见1162)。在一些实现方式中，该虚拟钱包应用可提供包括所显示的信息的QR代码，以便另一个用户可以迅速地快拍该信息来输入它到另一个虚拟钱包应用中。在一些实现方式中，该虚拟钱包应用可提供特征以便用户可以请求门卫服务(例如，当购物时候的帮助)、发货服务(例如，因此用户可以在不需要携带该物品出去的情况下离开商店)，1164。在一些实现方式中，该虚拟钱包应用可提供本地商家(例如，使用用户设备的GPS位置)或因特网上的商家的竞争价格(参见1165)。在一些实现方式中，该虚拟钱包应用可向用户提供包括但不限于以下各项的特征：浏览先前快拍，快拍新代码，添加GPS标签到代码，检索早先快拍的代码来使用，手工输入与QR代码有关的信息，把该QR代码归属于对象(例如以便为了组织目的，用于家庭的家具产品的QR代码可以被分组为“卧室家具”对象)，等等(参见1166)。在一些实施例中，用户能设置存储在快拍的物品应被发送到的用户虚拟钱包应用内的购物车或希望列表的名称(参见1167)。在一些实施例中，该虚拟钱包应用可允许用户创建快拍的物品应被添加到的新的购物车或希望列表。

[0183] 图12示出了在该SNAP一些实施例中，说明报价模式中虚拟钱包应用的示例特征的用户接口图。在一些实现方式中，SNAP可允许用户从该虚拟钱包移动应用内部检索产品和/或服务的报价。例如，用户可输入文本到图形用户界面(“GUI”)元件1211中，或通过激活GUI元件1212发布语音命令并且讲出命令到设备中。在一些实现方式中，SNAP可基于用户的先前行为、人口统计、当前位置、当前购物车选择或购买物品等提供报价。例如，如果用户处于

实体店，或在线购物网站，以及离开该(虚拟)商店，那么与该商店相关联的商家可能希望提供诱惑处理来怂恿顾客返回该(虚拟)商店。商家可提供这种报价1213。例如，，该报价可提供折扣，并可以包括期满时间。在一些实现方式中，其它用户可提供赠品(例如1214)给该用户，其中该用户可以兑换。在一些实现方式中，报价部分可以包括关于对其它用户(例如1215)未完成的资金的支 付警告。在一些实现方式中，该报价部分可以包括关于从其它用户请求资金收据的警告(例如1216)。例如，这种特征可以识别从其它应用可接收的资金(例如邮寄，日程表，任务，注释，提醒程序，警告等等)，或通过由用户人工输入到该虚拟钱包应用中。在一些实现方式中，报价部分可从SNAP中的参与商家提供报价，例如1217-1219，1220。这些报价可以有时使用参与商家的组合而聚集，例如1217。在一些实现方式中，SNAP本身可以从虚拟钱包应用内为用户随使用特定的支付形式的用户而提供报价，例如1220。

[0184] 图13A-B显示在SNAP的一些实施例中，说明在安全和隐私模式中虚拟钱包应用的示例性特征的用户界面图。参见图13A，在一些实现方式中，用户能浏览和/或更改用户简档和/或用户的设置，例如通过激活用户接口元件。例如，用户能浏览/修改用户名(例如1311a-b)、帐号(例如1312a-b)、用户安全访问码(例如1313-b)、用户pin(例如1314-b)、用户地址(例如，1315-b)、与用户相关联的社会安全号码(例如1316-b)、当前设备GPS位置(例如1317-b)、用户当前所处商店的商家的用户帐户(例如1318-b)、用户的回报帐户(例如1319-b)等。在一些实现方式中，用户能选择哪些数据字段和它们的关联值应被传输从而帮助该购买交易，因此为用户提供增强的数据安全性。例如，在图13A中的示例性说明中，用户已经选择姓名1311a、帐号1312a、安全代码1313a、商家帐户ID 1318a和回报帐户ID 1319a作为将被作为通知的一部分而发送的字段来处理该购买交易。在一些实现方式中，该用户可以套接这些字段和/或数据值，其作为通知的一部分被发送来处理该购买交易。在一些实现方式中，应用可以为用户提供数据字段和/或存储的关联值的多个屏幕来选择为购买定单传输的一部分。在一些实现方式中，应用可以给SNAP提供用户的GPS位置。基于用户的GPS位置，SNAP可以确定用户的环境(例如，用户是否处于商店，医生办公室，医院，邮政办公室等等)。基于该环境，用户应用可以呈现适当字段给用户，用户根据其可以选择字段和/或字段值来作为购买定单传输的一部分发送。

[0185] 例如，用户可能进入医生办公室并希望支付医生预约的共付医疗费。除基本交易信息之外，诸如帐号和名称，该应用可以给用户提供能力来选择传送病历、健康信息，其可以被提供给医疗供应商、保险公司，以及交易处理方来对账当事人之间的支付。在一些实现方式中，该记录可以以符合轻便和义务的健 康保险行动(HIPAA)的数据格式发送并加密，以及只有被授权浏览这种记录的接收方可以具有适当解密密钥来解密并浏览该私人用户信息。

[0186] 参见图13B，在一些实现方式中，在用户的设备上执行的应用可以提供“VerifyChat”特征用于防欺诈。例如，SNAP可以检测出不寻常的和/或可疑的交易。该SNAP可使用该Verifychat特征来与用户通信，并验证该购买交易的发起人的真实性。在各个实现方式中，SNAP可以发送电子邮件消息、文本(SMS)消息、Facebook®消息、Twitter™的tweet、文本聊天、语音聊天、视频聊天(例如，苹果FaceTime)等来与该用户通信。例如，SNAP可以为用户启动视频询问，例如1321。例如，用户可需要通过视频聊天呈现他/她自己，例如1322。在一些实现方式中，客户服务代表例如代理1324可以使用该用户的视频人工地确定

该用户的真实性。在一些实现方式中，SNAP可以使用面部、生物测定等识别方法(例如使用模式分类技术)来确定用户的身份。在一些实现方式中，应用可以提供基准标记(例如十字线、目标框等等)例如1323，以便用户可以提供视频以帮助用户的SNAP的自动识别。在一些实现方式中，用户可能尚未启动交易，例如该交易是欺诈的。在这种实现方式中，用户可以取消该询问。SNAP然后可以取消该交易，和/或代表该用户启动欺诈调查过程。

[0187] 在一些实现方式中，SNAP可以使用文本询问过程来确定用户的真实性，例如1325。例如，SNAP可以通过文本聊天、SMS消息、电子邮件、Facebook®消息、Twitter™的tweet等与用户通信。SNAP可以对用户提出询问问题，例如1326。该应用可以提供用户输入界面元件(例如虚拟键盘1328)来回答SNAP提出的询问问题。在一些实现方式中，该询问问题可以由SNAP自动随机地选择；在一些实现方式中，客户服务代表可以人工地与用户通信。在一些实现方式中，用户可能尚未启动该交易，例如该交易是欺诈的。在这种实现方式中，用户可以取消该文本询问。SNAP然后可以取消该交易，和/或替代表用户启动欺诈调查过程。

[0188] SNAP控制器

[0189] 图14显示说明SNAP控制器1401的实施例的框图。在此实施例中，SNAP控制器1401可用来聚集、处理、存储、检索、服务、识别、命令、产生、匹配、和/或通过各种技术帮助与计算机交互，和/或其它相关数据。

[0190] 通常，例如1433a的用户，其可以是人员和/或其它系统，可以接合信息技术系统(例如计算机)来帮助信息处理。反之，计算机采用处理器来处理信息；这种处理器1403可以被称为中央处理单元(CPU)。处理器的一个形式被称为微处理器。CPU使用通信电路来传递二进制编码信号，其作为指令来允许各种操作。这些指令可以是在各种可访问的处理器和可操作存储区1429(例如寄存器、高速缓冲存储器、随机存取存储器等等)中的包含和/或引用其它指令和数据的操作和/或数据指令。这种通信指令可以作为程序和/或数据分量分批(例如批指令)存储和/或传输来帮助所需操作。这些存储的指令代码，例如程序，可以接合CPU电路元件以及其它母板和/或系统组件来执行所需操作。一种程序类型是计算机操作系统，其可以是由计算机上的CPU执行的；该操作系统允许并帮助用户访问和运行计算机信息技术和资源。信息技术系统中可以采用的一些资源包括：通过其数据可进出计算机的输入和输出机制；数据可保存在其中的存储器；以及信息可以通过其处理的处理器。这些信息技术系统可以被用来收集数据以用于以后的检索、分析、以及操作，其可通过数据库程序来辅助。这些信息技术系统提供允许用户访问并运行各种系统元件的接口。

[0191] 在一个实施例中，SNAP控制器1401可以被连接至和/或与实体通信，所述实体诸如但不局限于：来自用户输入设备1411的一个或多个用户；外围设备1412；可选加密处理器设备1428；和/或通信网络1413。例如，SNAP控制器1401可以连接至和/或与用户通信，例如1433a，运行客户端设备，例如1433b，客户端设备包括但不限于：个人计算机、服务器和/或各种移动设备，包括但不限于蜂窝电话、智能电话(例如iPhone®，Blackberry®，基于安卓操作系统的电话等等)、平板计算机(例如，Apple iPad™，HP Slate™，摩托罗拉Xoom™等等)、eBook阅读器(例如Amazon Kindle™、Barnes以及Noble的Nook™eReader等等)、膝上型计算机、笔记本、上网本、游戏控制台(例如XBOX Live™，任天堂®DS、索尼PlayStation® Portable等等)、便携式扫描仪等。

[0192] 通常认为网络包括客户端、服务器、以及图形拓扑中的中间节点的互连和互操作。

应该注意的是，本申请始终使用的术语“服务器”通常指的是计算机、其它设备、程序或它们的组合，其处理并响应穿过通信网络的远程用户的请求。服务器使用他们的信息来请求“客户端”。正如此处使用的那样，术语“客户端” 通常指代计算机、程序、其它设备、用户和/或它们的组合，其能够处理并产生请求以及获得和处理任何从服务器穿过通信网络的响应。帮助信息处理和请求，和/或将信息片段从源用户发送到目标用户的计算机、其它设备、程序、或它们的组合通常称为“节点”。网络通常被认为帮助从源点到目的地的信息转输。具体来讲，从来源推动信息片段到目的地的任务的节点通常被叫作“路由器”。存在许多网络形式，诸如局域网(LANs)、微微网、广域网(WANs)，无线网络(WLANs)，等等。例如，因特网通常被接受为多个网络的互连，借此远程客户端和服务器可以彼此访问和互操作。

[0193] SNAP控制器1401可以是基于计算机系统的，其可包括但不局限于诸如连接至存储器1429的计算机系统1402的组件。

[0194] 计算机系统

[0195] 计算机系统1402可包括时钟1430、中央处理单元(“CPU”和/或“处理器”(这些术语在整个公开里可互换的使用除非相反地注释))1403、存储器1429(例如，只读存储器(ROM)1406、随机存取存储器(RAM)1405，等等)，和/或接口总线1407，并且几乎经常，尽管不一定，全部互联和/或通过一个或多个具有导电和/或其它方式的传输电路路径(指令(例如，二进制编码信号)通过其可传输来实现通信、操作、存储，等等)的(母)板1402上的系统总线1404传递。该计算机系统可以被连接至电源1486；例如，可选地，该电源可以是内部的。可选地，加密处理器1426和/或收发器(例如，IC)1474可以被连接至系统总线。在另一个实施例中，加密处理器和/或收发器可以通过接口总线I/O被连接为内部和/或外部外围设备1412。收发器又可以被连接至天线1475，由此实现各种通信的无线发射和接收和/或传感器协议；例如，天线可以连接至：Texas Instruments WiLink WL1283收发器芯片(例如，提供802.11n，蓝牙3.0，FM，全球定位系统(GPS)(由此允许SNAP控制器确定它的位置))；Broadcom BCM4329FKUBG收发器芯片(例如，提供802.11n，蓝牙2.1+EDR，FM，等等)；Broadcom BCM4750IUB8接收器芯片(例如，GPS)；Infineon Technologies X-Gold 618-PMB9800(例如，提供2G/3G HSDPA/HSUPA0通信)等。系统时钟通常具有晶体振荡器并通过该计算机系统的电路路径产生基准信号。时钟通常被连接到系统总线以及将增减基准操作频率用于该计算机系统中互联的其它部件的各种时钟倍乘器。计算机系统中的时钟和各种部件驱动 实现遍及该系统的信息的信号。这种实现遍及计算机系统的信息的指令的发送和接收通常可以称为通信。这些通信指令此外可以被传输、接收，以及促使超出实例计算机系统返回和/或应答通信到：通信网络、输入设备、其他的计算机系统、外围设备等。应该理解的是，在替换实施例中，任何上述部件可以被互相直接连接、连接至CPU和/或按照各种计算机系统举例说明的很多变化来组织。

[0196] CPU包括至少一个足以执行用于执行用户和/或系统产生的请求的程序部件的高速数据处理器。处理器本身往往将包括各种专业化处理单元，诸如但不局限于：集成系统(总线)控制器、存储器管理控制单元、浮点单元，并且甚至类似图形处理单元的专业化处理子单元、数字信号处理单元等。此外，处理器可包括内部快速存取可寻址存储器，并能够映射和寻址处理器本身以外的存储器1429；内存可包括但不局限于：快速寄存器，各级高速缓冲存储器(例如1、2、3级，等等)，RAM等等。处理器可以通过使用通过指令地址可访问的存储

地址空间访问这些存储器，处理器可以构造并解码所述指令，允许它访问去往具有存储状态的具体存储地址空间的电路路径。CPU可以是微处理器，诸如：AMD的Athlon，Duron和/或Opteron；ARM的应用，嵌入式安全处理器；IBM和/或Motorola的DragonBall以及PowerPC；IBM和Sony的Cell处理器；Intel的Celeron，Core(2)Duo，Itanium，Pentium，Xeon，和/或Xscale等处理器。CPU通过根据常规数据处理技术穿过导电和/或传输渠道(例如(印刷)电子和/或光学电路)以执行存储指令(换言之，程序代码)的指令传递与存储器进行交互。这种指令传递帮助了SNAP控制器内的和穿过各种界面以外的通信。如果处理要求规定较大速度和/或容量，可以类似采用分布式处理器(例如，分布式SNAP)，大型机，多核，并联，和/或超级计算机体系结构。作为替代地，如果配置需要规定较大的可移值性，则可以采用小型个人数字助理(PDA)。

[0197] 根据特定的实现方式，SNAP的特征可以通过实施诸如CAST的R8051XC2微控制器的微控制器、Intel的MCS 51(即，8051微控制器)等来实现。同时，为实施SNAP的某些特征，一些特征实现方式可依赖嵌入式部件，诸如：专用集成电路(“ASIC”)，数字信号处理(“DSP”)，现场可编程门阵列(“FPGA”)，和/或类似的嵌入式技术。例如，任何SNAP部件集(分布式等)和/或特征可以 通过微处理器实现和/或通过嵌入式部件实现；例如，通过ASIC，协处理器，DSP，FPGA等。作为替代地，SNAP的一些实现方式可以利用被配置并用于实现各种特征或信号处理的嵌入式部件实现。

[0198] 根据该特定的实现方式，嵌入式部件可包括软件解决方案，硬件解决方案，和/或硬件/软件解决方案的组合。例如，在此讨论的SNAP特征可以通过实现FPGA来实现，FPGA是包含叫做“逻辑块”的可编程序逻辑部件的半导体器件，和可编程互联，诸如高性能FPGA Virtex系列和/或Xilinx生产的低成本Spartan系列。在FPGA被制造之后，逻辑块和互联可以由顾客或设计者编程来实施任何SNAP特征。可编程互联的的层级允许逻辑块根据SNAP系统设计者/管理者的需要被互相连接，有点像单片可编程面包板。FPGA的逻辑块可以被编程为执行基本逻辑门的运算，诸如AND和XOR，或更多诸如解码器或简单数学操作的复杂的组合运算符。在大部分的FPGA中，逻辑块还包括存储元件，其可以是电路触发器或存储器的更完整的块。在一些情况下，SNAP可以在规则FPGA上研发，然后移植到更类似ASIC实现方式的固定版本中。作为替代的或协同的实现方式可以迁移SNAP控制器特征到最后的ASIC而不是FPGA，或除FPGA之外还迁移SNAP控制器特征到最后的ASIC。根据前述嵌入式部件的所有实现方式，微处理器可以设想为用于SNAP的“CPU”和/或“处理器”。

[0199] 电源

[0200] 电源1486可以是用于给小型电子电路板设备供电的任何标准形式，诸如下列电池：碱性的，氢化锂，锂离子，锂聚合物，镉镍，太阳能电池等。也可以使用其它类型的交流或直流电源。在太阳能电池的情况下，在一个实施例中，该情况提供孔隙，太阳电池通过其可捕获光子能量。该电池1486与至少一个互联的SNAP的随后部件相连，由此提供电流到所有随后部件。在一个例子中，电源1486与系统总线部件1404相连。在可替代的实施例中，通过穿过I/O 1408界面的连接提供外部电源1486。例如，USB和/或IEEE 1394连接运送数据和功率穿过该连接并因此是合适的电源。

[0201] 接口适配器

[0202] 接口总线1407可接受、连接、和/或传递到多个接口适配器，尽管通常不一定以适

配卡的形式，诸如但不局限于：输入输出接口(I/O)1408，存储接口1409，网络接口1410等。可选的，加密处理器接口1427类似地可以连接至接口总线。该接口总线为彼此以及计算机系统的其它部件提供接口适配器的通信。接口适配器适用于兼容式接口总线。接口适配器通常与接口总线通过插槽结构连接。可以采用传统插槽结构，诸如但不局限于：加速图形端口(AGP)，卡总线，(扩展的)工业标准结构((E)ISA)，微通道结构(MCA)，NuBus，外围部件互联(扩展的)(PCI(X))，PCI直通，个人计算机存储器卡国际联合会(PCMCIA)，等。

[0203] 存储接口1409可接受、传递、和/或连接至多个存储设备，诸如但不局限于：存储设备1414，可移除磁盘设备等。存储接口可采用连接协议，诸如但不局限于：(超)(串行)先进技术附件(分组接口)((超)(串行)ATA(PI))，(增强的)集成驱动电子线路((E)IDE)，电气与电子工程师协会(IEEE)1394，光纤信道，小型计算机系统接口(SCSI)，通用串行总线(USB)，等。

[0204] 网络接口1410可接受、传递和/或连接至通信网络1413。通过通信网络1413，SNAP控制器可由用户1433a通过远程客户端1433b(例如，具有网络浏览器的计算机)访问。网络接口可采用连接协议，诸如但不局限于：直接连接，以太网(厚，薄，双绞线10/100/1000 10/100/1000Base T等)，令牌环网，诸如IEEE8o2.11a-x的无线连接等。如果处理要求规定较大的总速度和/或容量，可类似地采用分布式网络控制器(例如，分布式SNAP)、结构来汇聚、负载平衡和/或提高SNAP控制器需要的通信带宽。通信网络可以是下列任何一个和/或组合：直接互连；因特网；局域网(LAN)；城域网(MAN)；作为因特网上的节点的运行任务(OMNI)；自定义安全连接；广域网(WAN)；无线网络(例如，采用诸如但不局限于：无线应用协议(WAP)，I-模式等的协议)等。网络接口可以被视为输入输出接口的专用形式。此外，多个网络接口1410可用来与各种通信网络类型1413接合。例如，可以采用多个网络接口来允许经由广播、多播、和/或单播网络的通信。

[0205] 输入输出接口(I/O)1408可接受、传递和/或连接至用户输入设备1411，外围设备1412，加密处理器设备1428等。I/O可采用连接协议，诸如但不局限于：音频：模拟，数字，单耳，RCA，立体声等；数据：苹果台式总线(ADB)，IEEE 1394a-b，串行，通用串行总线(USB)；红外；游戏杆；键盘；midi；光学；PC AT；PS/2；并联；无线电；视频接口：苹果台式连接器(ADC)，BNC，同轴，部件，合成，数字，数字视频接口(DVI)，高清晰度多媒体接口(HDMI)，RCA，RF天线，S-Video，VGA，等；无线收发器：802.11a/b/g/n/x；蓝牙；蜂窝(例如，码分多址(CDMA)，高速包存取(HSPA(+))，高速下行链路包存取(HSDPA)，全球移动通信系统(GSM)，长期演化(LTE)，WiMax，等等)；等。一种典型输出设备可包括视频显示器，其典型地包括基于阴极射线管(CRT)或液晶显示器(LCD)的监视器，具有从视频接口接受信号的接口(例如DVI电路和电缆)。视频接口合成由计算机系统产生的信息并基于合成的信息在视频存储框架中产生视频信号。另一个输出设备是电视机，其从视频接口接受信号。通常，视频接口通过接受视频显示接口(例如，接受RCA复合视频电缆的RCA复合视频连接器；接受DVI显示电缆的DVI连接器，等等)的视频连接接口提供复合视频信息。

[0206] 用户输入设备1411往往是一种外围设备1412(参见下文)并可包括：卡读取器，保护锁，指纹读取器，手套，图形写字板，游戏杆，键盘，麦克风，鼠标，远程控制器，视网膜读取器，触摸屏(例如，电容性的，电阻性的，等等)，轨迹球，轨迹板，传感器(例如，加速度计，环境光，GPS，陀螺仪，邻近等等)，输入笔等。

[0207] 外围设备1412可被连接和/或传递到I/O和/或其他的类似装备，诸如网络接口，存储接口，直接到接口总线，系统总线，CPU等。外围设备可以是外部的，内部的和/或SNAP控制器的一部分。外围设备可以包括：天线，音频设备(例如，线路输入，线路输出，麦克风输入，扬声器，等等)，照相机(例如，静态，视频，网络摄像机，等等)，保护锁(例如，用于拷贝保护，利用数字签名确保安全交易等)，外部处理器(用于附加的容量；例如，加密装置1428)，力反馈设备(例如，振动马达)，网络接口，打印机，扫描仪，存储设备，收发器(例如，蜂窝，GPS，等等)，视频设备(例如，护目镜，监视器，等等)，视频源，头盔等。外围设备经常包括各种类型的输入设备(例如，摄像机)。

[0208] 应该注意的是，尽管可以采用用户输入设备和外围设备，SNAP控制器可以体现为嵌入式、专用和/或更少监视器(即无头的)设备，其中将经由网络接口连接提供访问。

[0209] 加密单元诸如但不局限于：微控制器，处理器1426，接口1427，和/或设备1428，可以附着在和/或与该SNAP控制器通信。由摩托罗拉公司制造的MC68HC16微控制器可以用于和/或在加密单元内。MC68HC16微控制器以16 MHz配置的方式使用16位乘法和加法指令以及需要不到1秒来执行512位RSA私钥运算。加密单元支持来自交互代理以及允许不记名交易的通信的认证。加密单元也可以被配置为CPU的一部分。也可以使用等价微控制器和/或处理器。其他的可以购买到的专用加密处理器包括：Broadcom的CryptoNetx以及其它安全处理器；Ncipher的nShield，SafeNet的Luna PCI(例如，7100)系列；Semaphore Communication的40MHzRoadrunner 184；Sun的加密加速器(例如，加速器6000PCIe板，加速器500Daughtercard)；Via纳米处理器(例如，L2100，L2200，U2400)线，其能够执行500+MB/s的加密指令；VLSITechnology的33MHz 6868等。

[0210] 存储器

[0211] 通常，允许处理器实行存储和/或检索信息的任何机制和/或实施例都可看作存储器1429。然而存储器是可代替的技术和资源，因此可以互相替代或结合地采用多个存储器实施例。应该理解的是，SNAP控制器和/或计算机系统可以采用各种形式的存储器1429。例如，计算机系统可以被配置，在其中片上CPU存储器(例如，寄存器)，RAM，ROM和任何其它存储设备的操作是由纸张穿孔带或纸张穿孔卡片机制提供的；然而，这种实施例将导致非常慢的操作速度。在典型配置中，存储器1429将包括ROM 1406，RAM 1405，和存储设备1414。存储设备1414可以是任何传统计算机系统存储器。存储设备可以包括鼓；(固定和/或可移除的)磁盘驱动器；磁光驱动器；光驱(即，蓝光，CD/ROM/RAM/可记录(R)/可写(RW)，DVD R/RW，HD DVD R/RW等等)；设备阵列(例如，独立盘的冗余阵列(RAID))；固态存储器设备(USB存储器，固态驱动(SSD)等等)；其它处理器可读存储介质；和/或其他类似的设备。因此，计算机系统通常需要并使用存储器.

[0212] 部件集

[0213] 存储器1429可包含程序和/或数据库部件和/或数据的集合，诸如但不局限于：操作系统部件1415(操作系统)；信息服务器部件1416(信息服务器)；用户接口部件1417(用户接口)；网页浏览器部件1418(网页浏览器)；数据库1419；邮件服务器部件1421；邮件客户端部件1422；加密服务器部件1420(加密服务器)；SNAP部件1435等(即，合称为部件集)。这些部件可以从存储设备和/或从通过接口总线可访问的存储设备存储并访问。尽管非传统程序部件，诸如 部件集合的那些，通常被存储在本地存储设备1414中，但他们也可以通过通

信网络、ROM、各种形式的存储器等被载入和/或存储在诸如外围设备、RAM、远程存储设施的存储器中。

[0214] 操作系统

[0215] 操作系统部件1415是使SNAP控制器的操作变得容易的可执行程序部件。通常，操作系统有助于I/O、网络接口、外围设备、存储设备等的访问。操作系统可以是高度容错、可扩展和安全的系统，诸如苹果Macintosh计算机OS X(服务器)；AT&T Plan 9；Be OS；Unix和Unix-like系统分发(诸如AT&T的UNIX；Berkley软件分布程序(BSD)变体，诸如FreeBSD，NetBSD，OpenBSD等；Linux分布，诸如Red Hat，Ubuntu等)；和/或类似操作系统。然而，也可以采用更多限制和/或更少安全性的操作系统，诸如苹果Macintosh计算机OS，IBM OS/2，Microsoft DOS，Microsoft Windows2000/2003/3.1/95/98/CE/Millenium/NT/Vista/XP(服务器)，Palm OS等。操作系统可单向和/或双向与部件集中的其他的部件通信，包括本身，等。操作系统最通常与其他的程序部件、用户接口和/或类似部件通信。例如，操作系统可包含、传递、产生、获得、和/或提供程序部件、系统、用户、和/或数据通信、请求和/或响应。一旦由CPU执行，操作系统可允许与通信网络、数据、I/O、外围设备、程序部件、存储器、用户输入设备等交互。操作系统可提供通信协议，其允许SNAP控制器通过通信网络1413与其他的实体通信。SNAP控制器可以使用各种通信协议作为用于交互的副载波传输机制，诸如但不局限于：多播，TCP/IP，UDP，单播等。

[0216] 信息服务器

[0217] 信息服务器部件1416是存储的由CPU执行的程序部件。信息服务器可以是传统因特网信息服务器，诸如但不局限于Apache软件基础的Apache，微软公司的因特网信息服务器等。信息服务器可通过一些设施允许程序部件的执行，诸如：有效服务器页(ASP)，ActiveX，(ANSI)(Objective-)C(++)，C#和/或.NET，公共网关接口(CGI)脚本，动态(D)超文本标记语言(HTML)，FLASH，Java，JavaScript，实际提取报告语言(PERL)，超文本预处理器(PHP)，管道，Python，无线应用协议(WAP)，WebObjects等。信息服务器可支持安全通信协议，诸如但不局限于：文件传输协议(FTP)；超文本传输协议(HTTP)；安全超文本传输协议(HTTPS)，安全套接层(SSL)，消息传递协议(例如美国在线服务公司(AOL)的即时消息器(AIM)，应用交换(APEX)，ICQ，因特网多线交谈(IRC)，微软网络(MSN)消息器服务，存在和即时消息协议(PRIM)，因特网工程任务组的(IETF的)会话启动协议(SIP)，用于即时消息和存在影响扩展的SIP(SIMPLE)，开放式基于XML的可扩展消息和存在协议(XMPP)(即Jabber或开放的移动联盟的(OMA的)即时消息和存在服务(IMPS))，雅虎即时消息器服务等。信息服务器提供网页形式的结果到网页浏览器，并且允许通过与其它程序部件交互的网页的受控生成。在HTTP请求的域名系统(DNS)解析部分被解决为特定的信息服务器之后，信息服务器基于HTTP请求的其余部分，在SNAP控制器上的指定位置解析对信息的请求。例如，诸如http://123.124.125.126/myInformation.html的请求可能具有请求的IP部分“123.124.125.126”，其通过DNS服务器被解析为那个IP地址处的信息服务器；那个信息服务器此外可能又解析请求的“/myInformation.html”部分的http请求并且将它解析为包含信息“myInformation.html”的存储器中的位置。此外，用作协议的其它信息可以跨各种端口来采用，例如，跨端口的FTP通信等。信息服务器可以单向和/或双向地与部件集中的其它部件通信，包括本身，和/或类似设施。大部分的信息服务器经常与SNAP数据库1419，操作系

统，其他的程序部件，用户接口，网页浏览器等通信。

[0218] 对SNAP数据库的访问可以通过多个数据库桥接机制实现，诸如通过如以下列举的脚本语言(例如，CGI)以及通过如以下列举的应用间通信信道(例如CORBA，WebObjects，等等)。通过网页浏览器的任何数据请求通过该桥接机制被解析为如SNAP需要的适当语法。在一个实施例中，信息服务器将提供网页浏览器可访问的网页表格。网页表格中被填进所提供的字段的条目被标志为已经被输入特定的字段并且因而被解析。输入的术语然后被随着字段标签传递，其命令分析器产生指向适当表格和/或字段的查询。在一个实施例中，基于标志的文本条目，分析器可以通过利用适当的join/select命令实例化检索串而产生标准SQL方式的查询，其中经由桥接机制提供结果命令到SNAP作为查询。当根据该查询产生查询结果后，该结果被经由桥接机制传递，并且可以由该桥接机制解析以用于格式化以及新结果网页的生成。这种新结果网页然后被提供到信息服务器，信息服务器可以将它提供到发出请求的网页浏览器。

[0219] 同样，信息服务器可包含、传递、产生、获得和/或提供程序部件、系统、用户、和/或数据通信、请求、和/或响应。

[0220] 用户接口

[0221] 计算机接口在某些方面与汽车操作接口相似。汽车操作接口元件，诸如方向盘，变速器，以及速度计有助于汽车资源和状态的访问，操作以及显示。计算机交互接口元件，诸如复选框，光标，菜单，卷轴和窗口(合称为以及通常称为窗口小部件)类似地有助于数据和计算机硬件和操作系统资源和状态的访问，容量，操作，和显示。操作接口通常被叫做用户接口。图形用户接口(GUI)提供图形地向用户访问和显示信息的基线和装置，GUI诸如是苹果Macintosh计算机操作系统的Aqua，国际商业机器公司的OS/2，微软公司的Windows2000/2003/3.1/95/98/CE/Millenium/NT/XP/Vista/7(即Aero)，Unix的X-Windows(例如，其可包括附加Unix图形接口库以及诸如K台式环境(KDE)的层，mythTV以及GNU网络对象模型环境(GNOME))，网页接口库(例如，ActiveX，AJAX，(D)HTML，FLASH，Java，JavaScript等等，接口库诸如但不局限于，Dojo，jQuery(UI)，MooTools，Prototype，script.aculo.us，SWFObject，雅虎用户接口，任何可以被使用的)。

[0222] 用户接口部件1417是由CPU执行的存储程序部件。用户接口可以是由例如已经讨论的操作系统和/或操作环境提供的和/或在已经讨论的操作系统和/或操作环境之上的传统图形用户接口。用户接口可以允许通过文本和/或图形设施显示，执行，交互，处理，和/或操作程序部件和/或系统设施。用户接口提供设施，用户通过其能实施、相互作用和/或运行计算机系统。用户接口可以单向和/或双向地与部件集内的其他部件通信，包括本身，和/或类似设施。大部分的用户接口经常与操作系统、其他的程序部件等通信。该用户接口可包含、传递、产生、获得和/或提供程序部件、系统、用户、和/或数据通信、请求、和/或响应。

[0223] 网页浏览器

[0224] 网页浏览器部件1418是由CPU执行的存储程序部件。网页浏览器可以是传统超文本浏览应用，诸如Microsoft Internet Explorer或Netscape Navigator。安全网页浏览可以通过HTTPS，SSL等利用128位(或更多)加密来提供。网页浏览器允许程序部件通过设施的执行，诸如ActiveX，AJAX，(D)HTML，FLASH，Java，JavaScript，网页浏览器插件APIs(例如，FireFox，Safari Plug-in 等API)等。网页浏览器和类似信息访问工具可以被集成到PDA，

蜂窝电话，和/或其他的移动设备。用户网页浏览器可以单向和/或双向地与部件部件集内的其他部件通信，包括本身，和/或类似设施。大部分的网页浏览器经常与信息服务器，操作系统，集成的程序部件(例如插件)等通信；例如，它可包含、传递、产生、获得和/或提供程序部件、系统、用户和/或数据通信、请求和/或响应。同样，代替网页浏览器和信息服务器，也可以开发组合应用来执行二者的相似操作。组合应用类似地实施从支持SNAP的节点实施信息的获得和提供信息到用户，用户代理等。该组合应用可以在采用标准网页浏览器的系统上是无关紧要的。

[0225] 邮件服务器

[0226] 邮件服务器部件1421是由CPU 1403执行的存储程序部件。邮件服务器可以是传统因特网邮件服务器，诸如但不局限于sendmail、Microsoft Exchange等。邮件服务器可通过一些设施允许程序部件的执行，诸如ASP，ActiveX，(ANSI)(Objective-)C(++)，C#_和/或.NET，CGI脚本，Java，JavaScript，PERL，PHP，pipes，Python，WebObjects等。邮件服务器可支持通信协议，诸如但不局限于：Internet消息访问协议(IMAP)，消息应用编程接口(MAPI)/Microsoft Exchange，post office protocol(POP3)，简单邮件传送协议(SMTP)等。邮件服务器可以路由，转发和处理输入和输出邮件消息，其已经被发送，中继和/或穿越通过和/或到该SNAP。

[0227] 对SNAP邮件的访问可以通过由单个网页服务器部件和/或操作系统提供的多个API实现。

[0228] 同时，邮件服务器可包含、传递、产生、获得和/或提供程序部件、系统、用户、和/或数据通信、请求、信息和/或响应。

[0229] 邮件客户端

[0230] 邮件客户端部件1422是由CPU 1403执行的存储程序部件。邮件客户端可以是传统邮件浏览应用，诸如：Apple Mail，Microsoft Entourage，Microsoft Outlook，Microsoft Outlook Express，Mozilla，Thunderbird等。邮件客户端可支持多个转输协议，诸如：IMAP，Microsoft Exchange，POP3，SMTP等。邮件客户端可单向和/或双向地与部件集中的其他的部件通信，包括本身，和/或类似设施。大部分的邮件客户端经常与邮件服务器、操作系统、其它邮件客 户端等通信；例如，它可包含、传递、产生、获得和/或提供程序部件、系统、用户和/或数据通信、请求、信息和/或响应。邮件客户端通常提供设施来编写并传输电子邮件消息。

[0231] 加密服务器

[0232] 加密服务器部件1420是由CPU 1403、加密处理器1426、加密处理器接口1427、加密处理器设备1428等执行的存储程序部件。加密处理器接口将允许加密元件请求的加密和/或解密的加速；然而，作为选择，加密元件可以运行在传统CPU上。加密元件允许所提供数据的加密和/或解密。加密元件允许对称的和非对称的(例如，Pretty Good Protection(PGP))加密和/或解密。加密元件可采用的加密技术诸如但不局限于：数字证书(例如，X.509认证框架)，数字签名，双重签名，信封，密码存取保护，公钥管理等。加密元件将有助于很多(加密和/或解密)安全协议，诸如但不局限于：校验和，数据加密标准(DES)，椭圆曲线加密(ECC)，国际数据加密算法(IDEA)，消息摘要(MD5，其是散列运算的一种方式)，密码，Rivest Cipher(RC5)，Rijndael，RSA(其是使用1977年由Ron Rivest，Adi Shamir和

Leonard Adleman开发的算法的因特网加密和认证系统)，安全散列算法(SHA)，安全套接层(SSL)，安全超文本传输协议(HTTPS)等。采用这些加密安全协议，SNAP可以加密所有输入和/或输出通信并可以利用更宽的通信网络用作虚拟专用网络(VPN)内的节点。加密元件有助于“安全授权”的处理，借此通过安全协议禁止对资源的访问，其中，该加密元件实施对安全资源的授权访问。此外，加密元件可提供内容的唯一标识符，例如采用以及MD5散列来为数字音频文件获得唯一签名。加密元件可以单向和/或双向地与部件集内的其他部件通信，包括本身，和/或类似设施。如果需要，加密元件支持允许信息穿过通信网络的安全传输来允许SNAP部件参加安全交易的加密机制。加密元件有助于SNAP上的资源的安全访问以及有助于远程系统上的安全资源的访问；即它可以作为安全资源的客户端和/或服务器。大部分的加密元件经常与信息服务器，操作系统，其他的程序部件等通信。该加密元件可包含、传递、产生、获得和/或提供程序部件、系统、用户和/或数据通信、请求、和/或响应。

[0233] SNAP数据库

[0234] SNAP数据库部件1419可以被嵌入在数据库及其所存储的数据中。数据库 是存储程序部件，其由CPU执行；存储程序部件部分配置CPU来处理所存储的数据。数据库可以是传统、容错、关联、可扩展、安全的数据库，诸如Oracle或Sybase。关系数据库是平面文件的扩展。关系数据库包含一系列相关表。表通过键字段互相连接。键字段的使用允许通过相对于键字段的索引而组合表；即，键字段作为用于各种表的组合信息的维数支点。关系通常借助于匹配初级键来识别表之间的链接。初级键表示唯一地识别关系数据库中的表行的字段。更确切的说，他们唯一地识别一对多关系的“一”侧的表行。

[0235] 可替代地，SNAP数据库可以使用各种标准数据结构实现，诸如阵列，散列，(链)表，结构，结构文本文件(例如XML)，表格等。这些数据结构可以存储在存储器和/或(结构)文件中。在另一个替换中，可以使用面向对象的数据库，诸如Frontier，ObjectStore，Poet，Zope，等。对象数据库可包括多个对象集合，其通过公共属性被分组和/或链接起来；他们通过一些公共属性与其它对象集合相关。面向对象数据库与关系数据库类似地执行，除了其对象不只是数据片段，而可以具有给定对象内封装的功能的其他类型。如果SNAP数据库实现为数据结构，则SNAP数据库1419的使用可以被集成到另一个部件中，诸如SNAP部件1435。同样，数据库可以实现为数据结构、对象以及关系结构的混合。数据库可以通过标准数据处理技术以无数的变化被合并和/或分布。数据库的一些部分，例如表格，可以被输出和/或输入并因此分散和/或集成。

[0236] 在一个实施例中，该数据库部件1419包括若干表格1419a-o。用户表格1419a可包括字段，诸如但不局限于：user_id，ssn，dob，first_name，last_name，age，state，address_firstline，address_secondline，zipcode，devices_list，contact_info，contact_type，alt_contact_info，alt_contact_type，等。用户表格可支持和/或追踪SNAP上的多个实体帐户。设备表格1419b可包括字段，诸如但不局限于：device_ID，device_name，device_IP，device_MAC，device_type，device_model，device_version，device_OS，device_apps_list，device_securekey，wallet_app_installed_flag，等。Apps表格1419c可包括字段，诸如但不局限于：app_ID，app_name，app_type，app_dependencies，等。帐户表格1419d可包括字段，诸如但不局限于：account_number，account_security_code，account_name，issuer_acquirer_flag，issuer_name，acquirer_name，account_address，routing_number，

access_API_call,linked_wallets_list等。商家表格1419e可包括 字段,诸如但不局限于:merchant_id,merchant_name,merchant_address,ip_address,mac_address,auth_key,port_num,security_settings_list,等。发布方表格1419f可包括字段,诸如但不局限于:issuer_id,issuer_name,issuer_address,ip_address,mac_address,auth_key,port_num,security_settings_list等。收单机构表格1419g可包括字段,诸如但不局限于:account_firstname,account_lastname,account_type,account_num,account_balance_list,billingaddress_linei,billingaddress_line2,billing_zipcode,billing_state,shipping_preferences,shippingaddress_linei,shippingaddress_line2,shipping_zipcode,shipping_state等。支付网关表格1419b可包括字段,诸如但不局限于:gateway_ID,gateway_IP,gateway_MAC,gateway_secure_key,gateway_access_list,gateway_API_call_list,gateway_services_list,等。交易表格1419i可包括字段,诸如但不局限于:order_id,user_id,timestamp,transaction_cost,purchase_details_list,num_products,products_list,product_type,product_params_list,product_title,product_summary,quantity,user_id,client_id,client_ip,client_type,client_model,operating_system,os_version,app_installed_flag,user_id,account_firstname,account_lastname,account_type,account_num,account_priority_account_ratio,billingaddress_linei,billingaddress_line2,billing_zipcode,billing_state,shipping_preferences,shippingaddress_linei,shippingaddress_line2,shipping_zipcode,shipping_state,merchant_id,merchant_name,merchant_auth_key等。批表格1419j可包括字段,诸如但不局限于:batch_id,transaction_id_list,timestamp_list,cleared_flag_list,clearance_trigger_settings等。分类账表格1419k可包括字段,诸如但不局限于:request_id,timestamp,deposit_amount,batch_id,transaction_id,clear_flag,deposit_account,transaction_summary,payor_name,payor_account等。产品表格1419l可包括字段,诸如但不局限于:product_ID,product_title,product_attributes_list,product_price,tax_info_list,related_products_list,offers_list,discounts_list,rewards_list,merchants_list,merchant_availability_list等。报价表格1419m可包括字段,诸如但不局限于:offer_ID,offer_title,offer_attributes_list,offer_price,offer_expiry,related_products_list,discounts_list,rewards_list,merchants_list, merchant_availability_list,等。行为数据表格1419n可包括字段,诸如但不局限于:user_id,timestamp,activity_type,activity_location,activity_attribute_list,activity_attribute_values_list等。分析表格1419o可包括字段,诸如但不局限于:report_id,user_id,report_type,report_algorithm_id,report_destination_address等。

[0237] 在一个实施例中,SNAP数据库可以与其它数据库系统交互。例如,采用分布式数据库系统,通过检索SNAP部件进行的查询以及数据访问可以处理SNAP数据库、集成的数据安全层数据库的组合为单个数据库实体。

[0238] 在一个实施例中,用户程序可包含各种用户接口图元,其可用来更新SNAP。同样,根据SNAP可能需要服务的环境以及客户端类型,各种帐户可能需要自定义数据库表。应该注意的是,任何唯一字段可以被指定为通篇的键字段。在作为替代的实施例中,这些表格已

经被分散到他们自己的数据库和它们各自的数据库控制器中(即,用于每一个上述表格的单个数据库控制器)。采用标准数据处理技术,人们可以进一步经由若干计算机系统和/或存储设备分发该数据库。类似地,通过合并和/或分布各种数据库部件1419a-o,分散的数据库控制器的配置可以被改变。SNAP可以被配置为通过数据库控制器跟踪各种设置、输入和参数。

[0239] SNAP数据库可以单向和/或双向地与部件集内的其他部件通信,包括本身,和/或类似设施。大部分的SNAP数据库经常与SNAP部件、其他的程序部件等通信。数据库可包含、维持和提供关于其它节点和数据的信息。

[0240] SNAP

[0241] SNAP部件1435是由CPU执行的存储程序部件。在一个实施例中,SNAP部件包括在前面附图中讨论的SNAP的各方面的任何一个和/或所有组合。因而,SNAP跨各种通信网络实施信息、服务、交易等的访问,获得和供应。

[0242] SNAP部件可通过SNAP部件转换实时产生的商家-产品快速响应代码为基于虚拟钱包卡的交易购买通知等和SNAP的使用。在一个实施例中,SNAP部件1435进行输入(例如,结帐输入411;产品数据414;支付输入419;发布方服务器数据423;用户数据427a-n等),并通过SNAP部件转换输入(例如,SMPE 1441;QRCP 1442等)为输出(例如,QR支付代码417;卡授权请求421;授权响应429a-n;授权成功消息433a-b;批附加数据435;购买收据436 等)。

[0243] 允许节点间信息访问的SNAP部件可以通过采用标准开发工具和语言开发,诸如但不局限于:Apache部件,Assembly,ActiveX,可执行的二进制,(ANSI)(Objective-)C(++),C#_和/或.NET,数据库适配器,CGI脚本,Java,JavaScript,绘图工具,面向过程和对象的开发工具,PERL,PHP,Python,shell脚本,SQL命令,网页应用服务器扩展,网页开发环境和库(例如,微软公司的ActiveX;Adobe AIR,FLEX&FLASH;AJAX;(D)HTML;Dojo,Java;JavaScript;jQuery(UI);MooTools;Prototype;script.aculo.us;简单对象存取协议(SOAP);SWFObject;雅虎用户接口等),WebObjects等。在一个实施例中,SNAP服务器采用加密服务器来加密和解密通信。SNAP元件可单向和/或双向地与部件集内的其他部件通信,包括本身,和/或类似设施。大部分的SNAP部件经常与SNAP数据库、操作系统、其他的程序部件等通信。SNAP可包含、传递、产生、获得和/或提供程序部件、系统、用户和/或数据通信、请求和/或响应。

[0244] 分布式SNAP

[0245] 任何SNAP节点控制器部件的结构和/或操作可以以任意多种方式组合、合并和/或分布来帮助开发和/或配置。类似地,可以以任意多种方式组合部件集以帮助部署和/或开发。为实现这一点,可以集成部件到公共代码基础中或到可以按需以集成的方式动态地加载部件的设施中。

[0246] 部件集可以被以无数的变化通过标准数据处理和/或开发技术而合并和/或分布。程序部件集中的程序部件的任一项的多个实例可以被实例化在单个节点上,和/或跨多个节点以通过负载平衡和/或数据处理技术提高性能。此外,单个实例也可以是跨多个控制器和/或存储设备分布的;例如,数据库。一起工作的所有程序部件实例和控制器可以通过标准数据进程通信技术这样做。

[0247] SNAP控制器的配置将取决于系统部署的环境。这些因素诸如但不局限于:预算,容

量，位置和/或底层硬件资源的使用可以实施部署要求和配置。不考虑配置是否导致更多合并和/或集成程序部件，导致更多分布的程序部件系列，和/或导致合并和分布式配置间的组合，数据可以被传递，获得，和/或提供。根据程序部件集，合并到公共代码基础中的部件实例可以传递，获得，和/或提供数据。这些可通过应用内数据处理通信技术来实现，诸如但不局限于：数据引用(例如指针)，内部消息传递，对象实例变量通信，共享存储器空间，变量传递等。

[0248] 如果部件集部件是相互分立的、独立的和/或外部的，那么传递、获得和/或提供数据与和/或到其他的部件可以通过应用内数据处理通信技术实现，诸如但不局限于：应用程序接口(API)信息传递；(分布式)部件对象模型((D)COM)，(分布式)对象链接与嵌入((D)OLE)等)，公共对象请示代理体系结构(CORBA)，Jini本地和远程应用程序接口，Javascript对象注释(JSON)，远程方法引用(RMI)，SOAP，进程管道，共享文件等。应用间内通信的分立部件之间或在应用内通信的单个部件的存储空间内部发送的消息可以有助于语法的创建和解析。语法可以使用开发工具开发，诸如lex，yacc，XML等，其允许语法生成和解析功能，其又可以形成部件内部和之间的通信消息的基础。

[0249] 例如，语法可以设置为识别HTTP张贴指令的令牌，例如：

[0250] w3c-post http://...Value1

[0251] 其中Value1识别为一种参数，因为“http://”是语法体系的一部分，并且后续被认为是张贴值的一部分。类似地，利用这种语法，变量“value1”可以插入到“http://”张贴命令中然后被发送。语法体系本身可以呈现为结构化数据，其被解释和/或用于产生解析机制(例如lex，yacc等等处理的语法描述文本文件)。同样，一旦产生和/或实例化了解析机制，它本身处理和/或解析结构化数据，诸如但不局限于：描绘文本的字符(例如标签)，HTML，结构化文本流，XML等结构化数据。在另一个实施例中，应用间数据处理协议本身可具有集成和/或容易地可用的解析器(例如，JSON，SOAP，等解析器)，其可以用于解析(例如，通信)数据。此外，解析语法可以被使用在消息解析之上，但也可以用于解析：数据库，数据集，数据存储，结构化数据等。再次，期望的配置将取决于语境，环境，以及系统开发的需要。

[0252] 例如，在一些实现方式中，SNAP控制器可以是通过信息服务器执行实现安全套接层(“SSL”套接服务器)的PHP脚本，其侦听客户端可以发送数据(例如以JSON格式编码的数据)的服务器端口上的输入通信。一旦识别输入通信，PHP脚本可以从客户端设备读取输入消息，解析该接收的JSON编码的数据以便从JSON编码的文本数据提取信息到PHP脚本变量中，并在使用结构化查询语言(“SQL”)可访问的关系数据库中存储该数据(例如，客户端识别信息，等等)和/或提取的信息。基本上以PHP/SQL命令的形式写入，来通过SSL连接从客户端设备接受JSON编码的输入数据、解析数据以便提取变量，并存储数据到数据库的示例性列表如下提供：

[0253]

```
<?PHP
header('Content-Type: text/plain');

// set ip address and port to listen to for incoming data
$address = '192.168.0.100';
$port = 255;

// create a server-side SSL socket, listen for/accept incoming communication
$sock = socket_create(AF_INET, SOCK_STREAM, 0);
socket_bind($sock, $address, $port) or die('Could not bind to address');
socket_listen($sock);
$client = socket_accept($sock);

// read input data from client device in 1024 byte blocks until end of message
do {
    $input = "";
    $input = socket_read($client, 1024);
    $data .= $input;
} while($input != "");

// parse data to extract variables
$obj = json_decode($data, true);

// store input data in a database
mysql_connect("201.408.185.132",$DBserver,$password); // access database server
mysql_select("CLIENT_DB.SQL"); // select database to append
mysql_query("INSERT INTO UserTable (transmission)
VALUES ($data)"); // add data to UserTable table in  a CLIENT database
mysql_close("CLIENT_DB.SQL"); // close connection to database
?>
```

[0254] 同样,下列资源可用来提供示关于SOAP解析器实现方式的示例性实施例:

[0255] http://www.xav.com/perl/site/lib/SOAP/Parser.html

[0256] http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic＝/com.ibm

[0257] .IBMDI.doc/referenceguide295.htm

[0258] 以及其它解析器实现方式:

[0259] http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic-/com.ibm

[0260] .IBMDI.doc/referenceguide259.htm

[0261] 因此通过引用将所有这些包括在此。

[0262] 为了解决各种问题并发展技术,用于快拍移动支付装置、方法和系统(包括封面,标题,小标题,技术领域,背景技术,发明内容,附图说明,具体实施方式,权利要求,摘要,附图,附录和/或其他)的本申请的全部通过各种示意图实施例显示,其中所要求的创新可以被实行。本申请的优点和特征仅是实施例的代表性示例,不是穷举和/或排他的。他们存在仅仅用于帮助理解和教导如权利要求所述的原理。应该理解的是,他们不是代表所有如权利要求所述的创新。因而公开内容的某些方面没有在此论述。替代性的实施例未必已经被呈 现用于本发明的具体部分或此外未描述的替代性的实施例可以被可获得用于设想替代性的实施例的放弃的部件。将理解的是,许多那些未描述的实施例采用本发明相同原理及其他是等价的。因此,应该理解的是,在不脱离该公开内容的范围和/或精神的情况下可以使用其它实施例以及产生功能逻辑,操作,组织的,结构和/或拓扑修改。因而,在整个公开内容中,所有示例和/或实施例被认为是非限制的。没有推断应被引起考虑在此论述的那些

实施例相对于在此未论述的那些，除为了降低空间以及重复起见以外的。例如，应该理解的是，任何程序部件(部件集合)的任何群组的逻辑和/或拓扑结构，如附图和/或全部所描述的其它部件和/或提供部件设置不局限于固定的运行顺序和/或排列，而是任何公开的顺序是示例性以及都等价，不考虑顺序是该公开内容设想的。此外，应该理解的是，这种部件不局限于串行执行，而是多个线程，处理，服务，服务器，和/或那些能异步地、同步、并行、同时，同步执行的那些，等是该公开内容设想的。因而，一些部件可以相互对立的，因为们不能同时存在于单个实施例中。类似地一些部件适用于本发明的一种方面，以及不适用的其它方面。此外，公开内容包括其它目前未要求的新方法。对目前未经要求的新方法申请人保留所有权利，包括要求这种新方法、文件增补申请、继续、部分地继续、分割和/或它的同类的权利。因而，应该理解的是，该公开内容的优势，实施例，示例，功能，部件，逻辑操作，组织，结构，拓扑和/或其它方面不是设想限制在权利要求书所定义的公开内容上或限制在相当于权利要求书上。应该理解的是，根据SNAP个人和/或企业用户，数据库配置和/或关系模型，数据类型，数据传输和/或网络框架，语法结构等的特定的需要和/或特性，SNAP的各种实施例可以被实施，其允许许多灵活性和定制。例如，SNAP的各方面可以修改以适合于饭店订餐，在线购物，在实体店中购物，安全信息处理，保健信息系统等。然而当SNAP的各种实施例和讨论已经指向电子购买交易时，应该理解的是，此处的实施例可以被容易地配置和/或自定义用于各式各样的其它应用和/或实现方式。

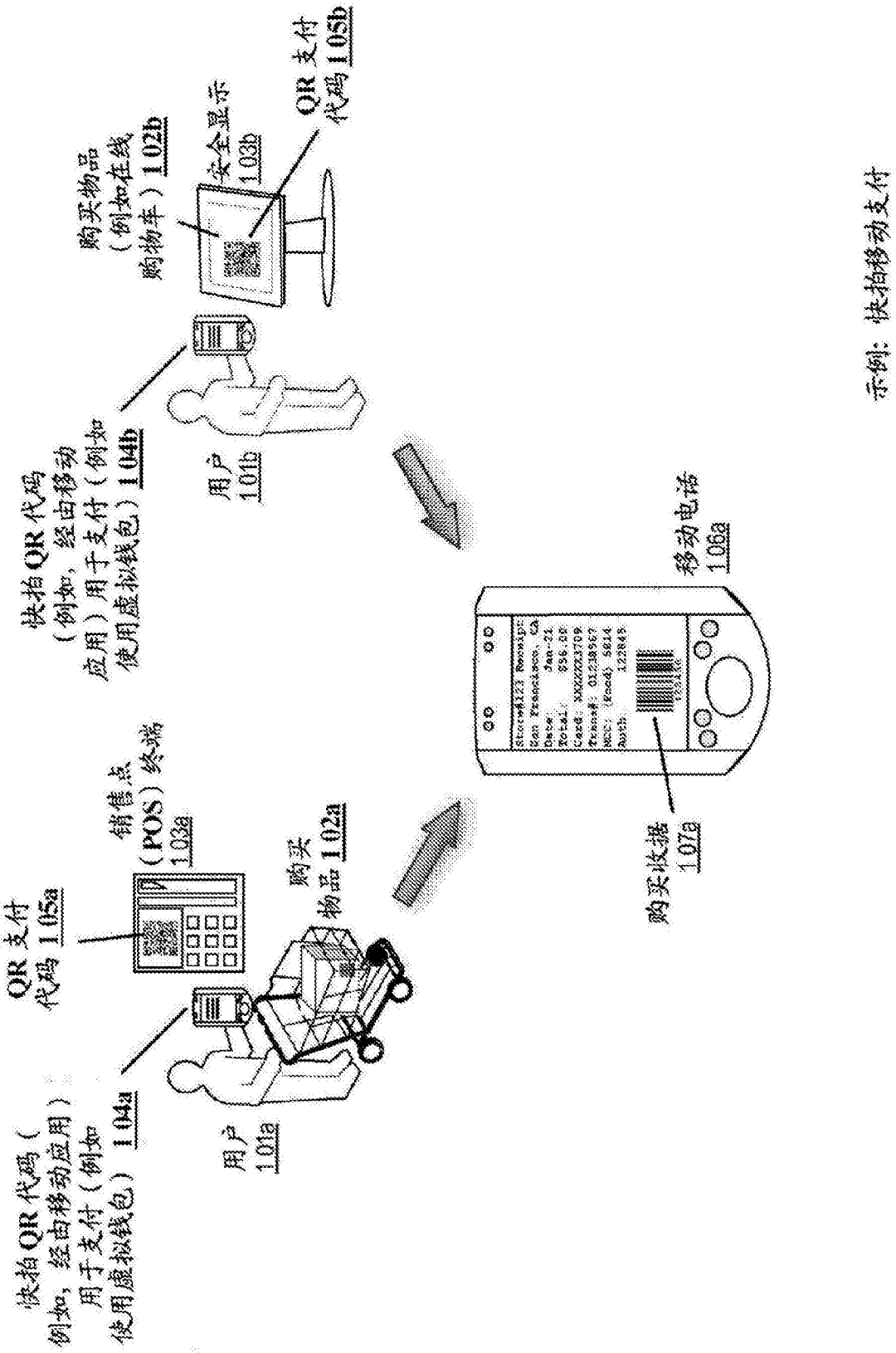


图1A

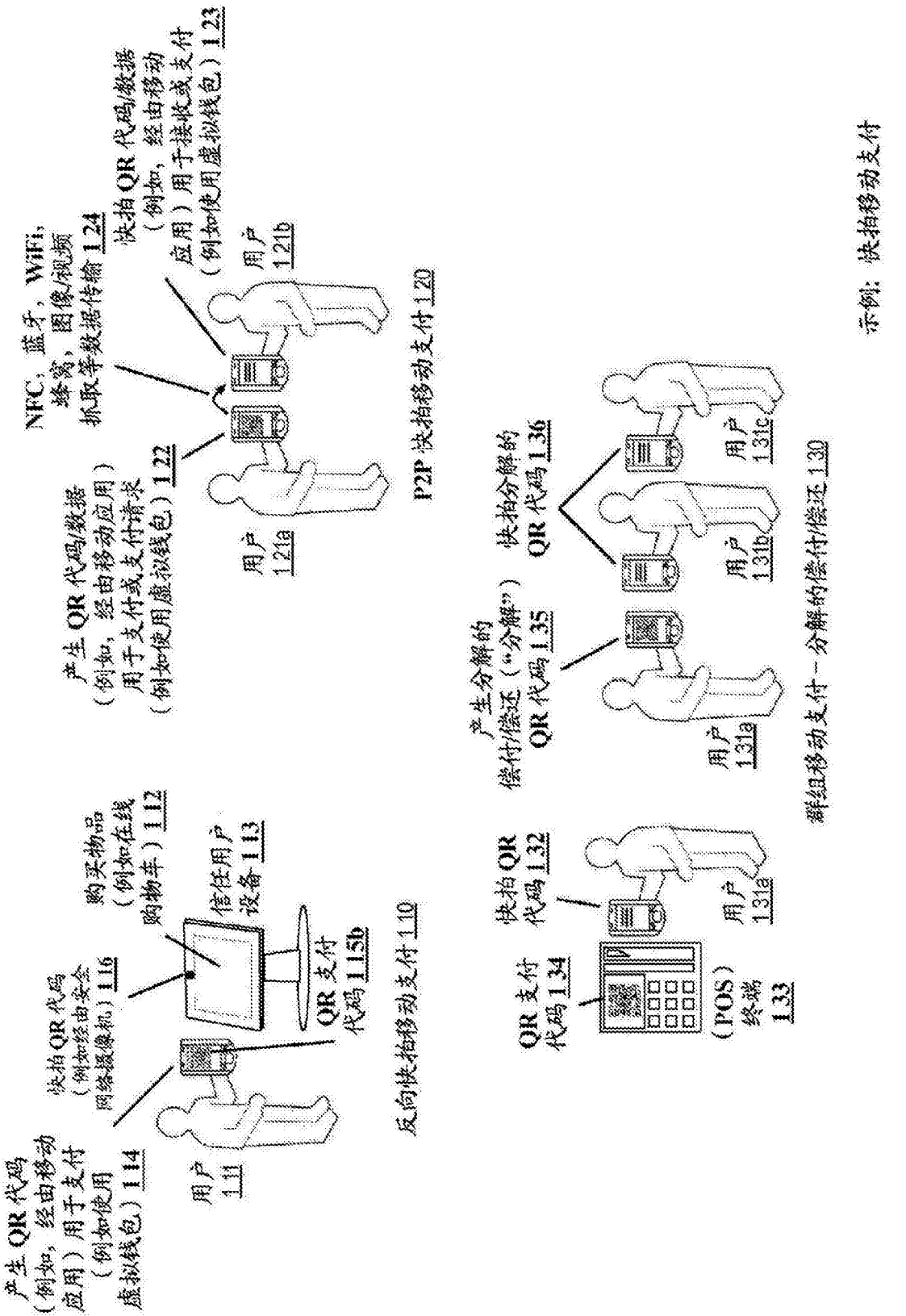


图1B

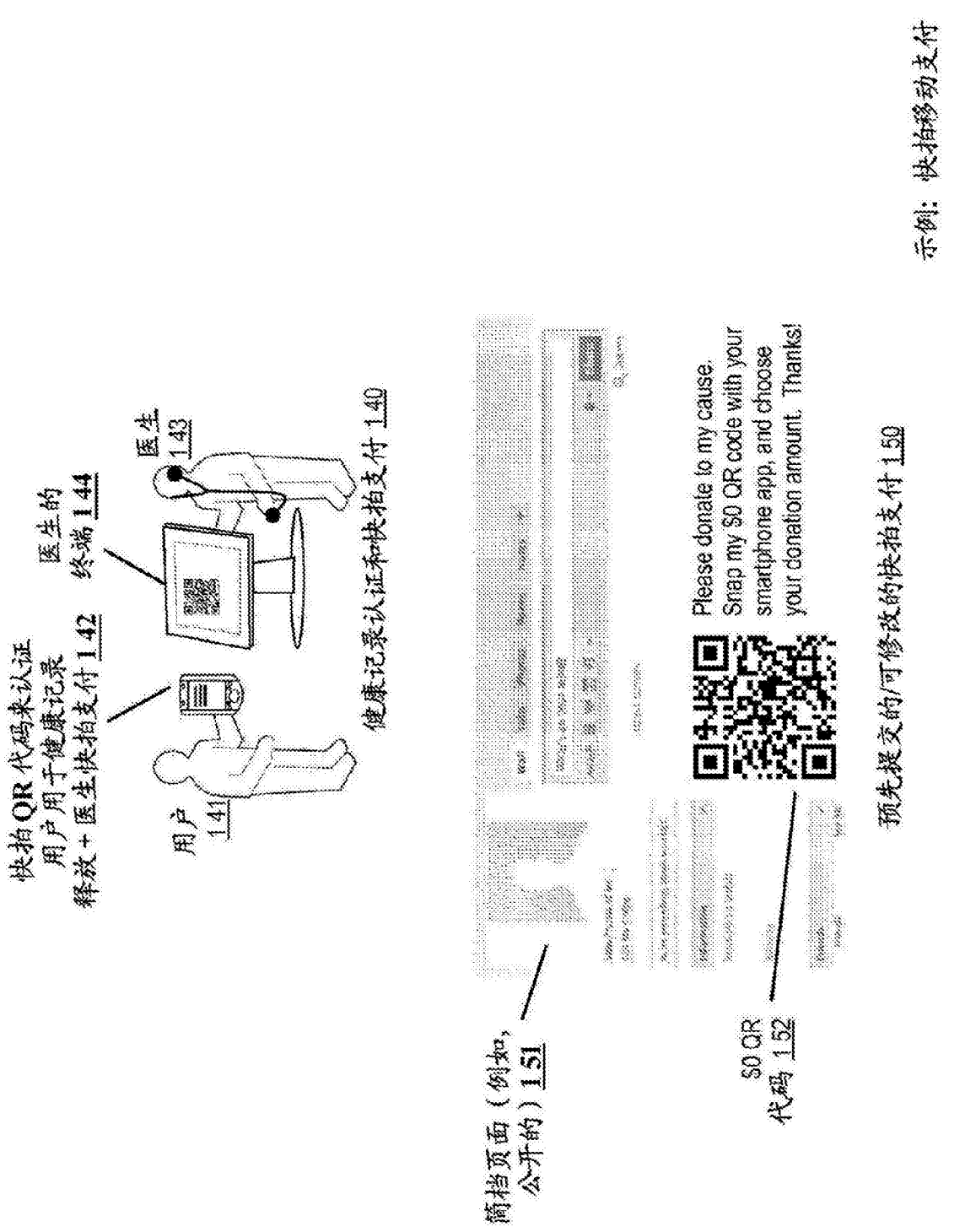


图1C

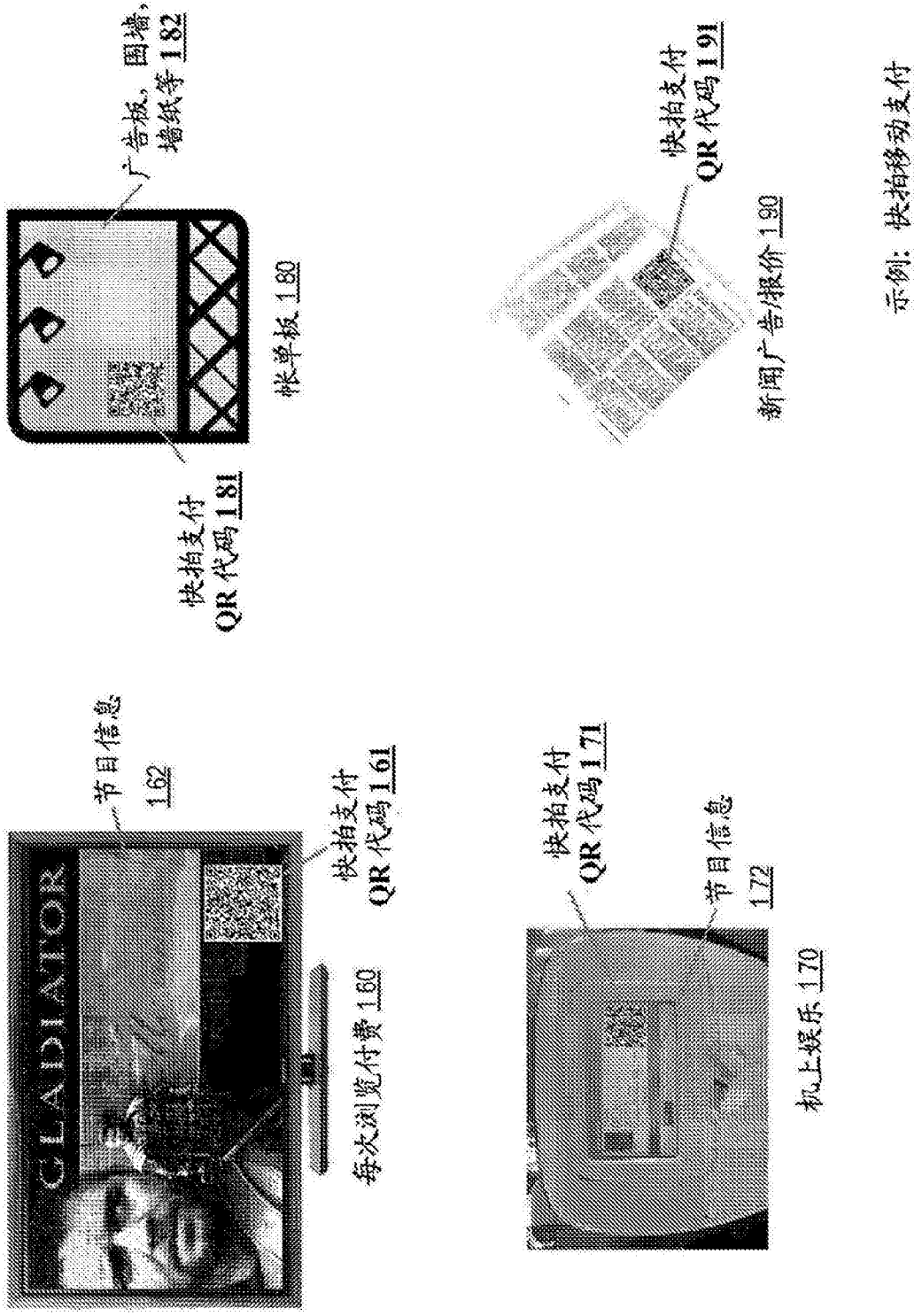


图1D

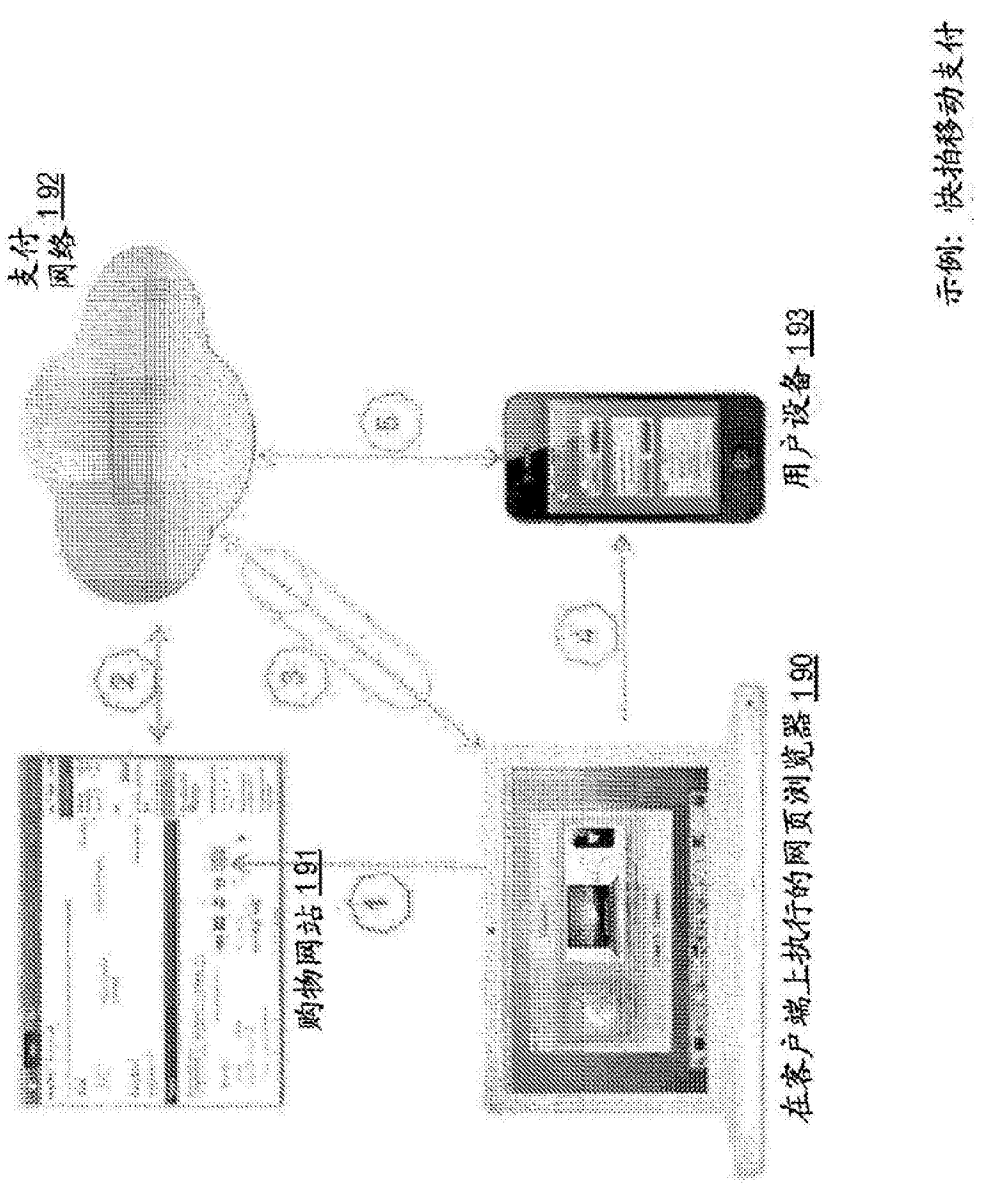


图1E

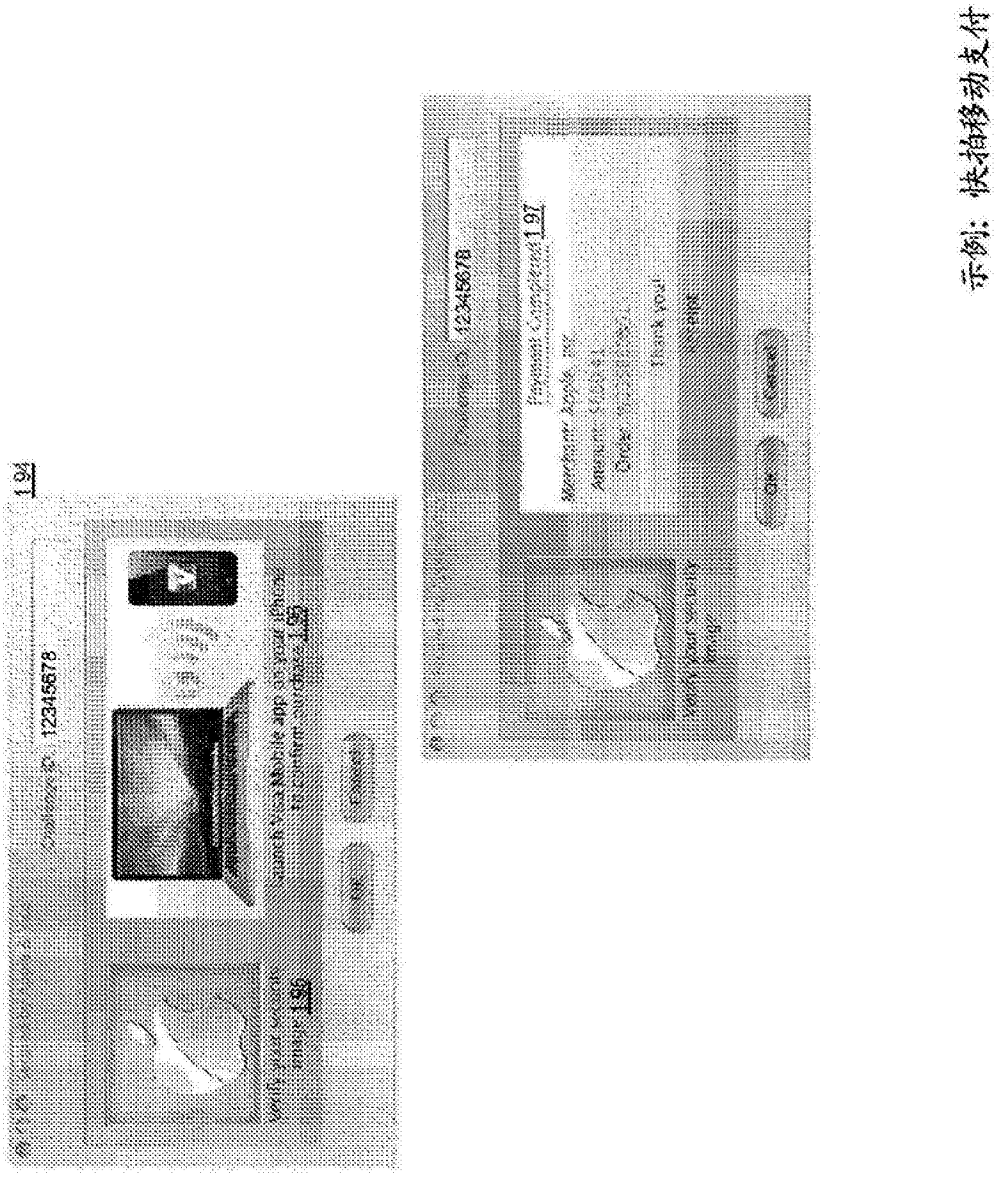
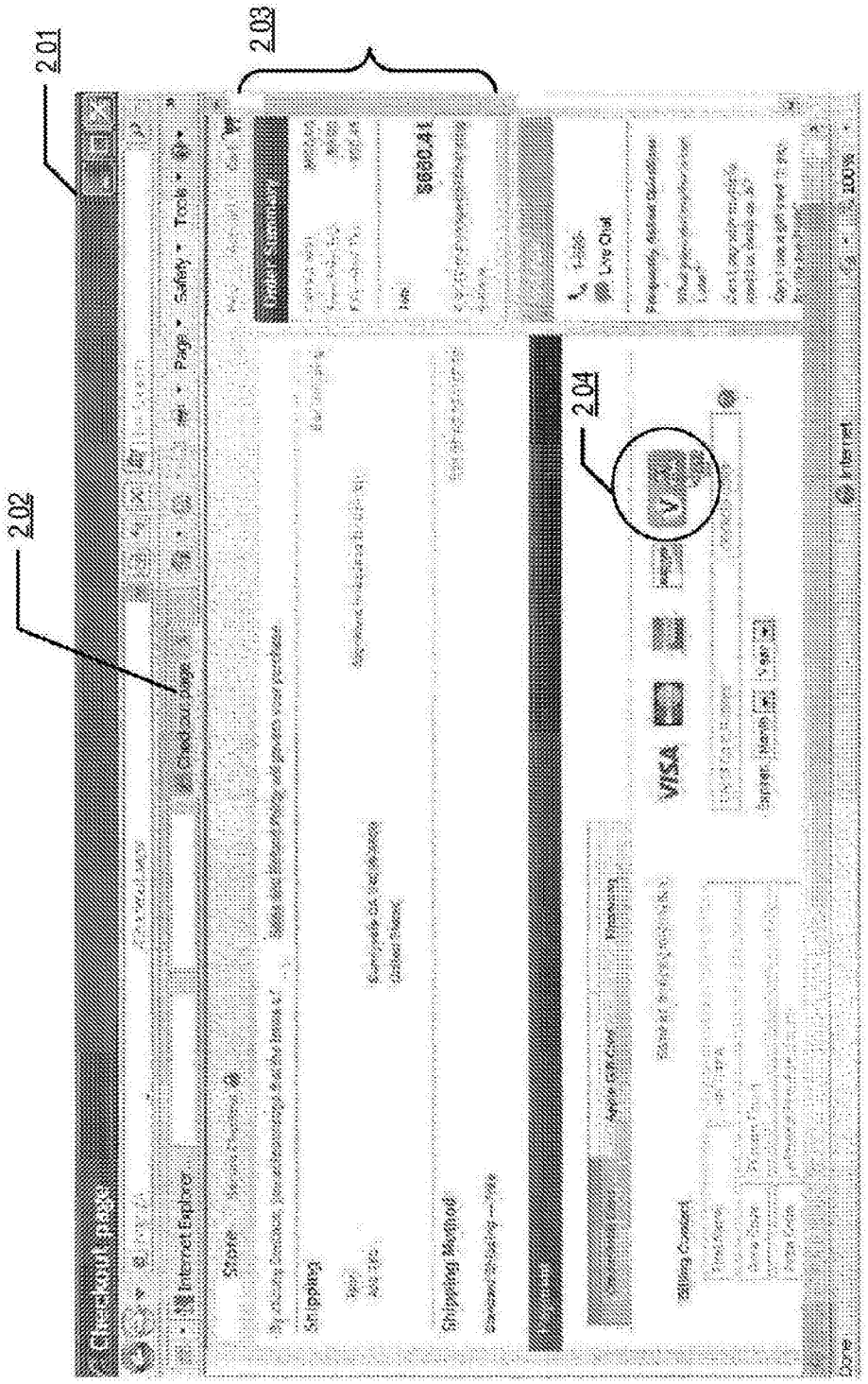
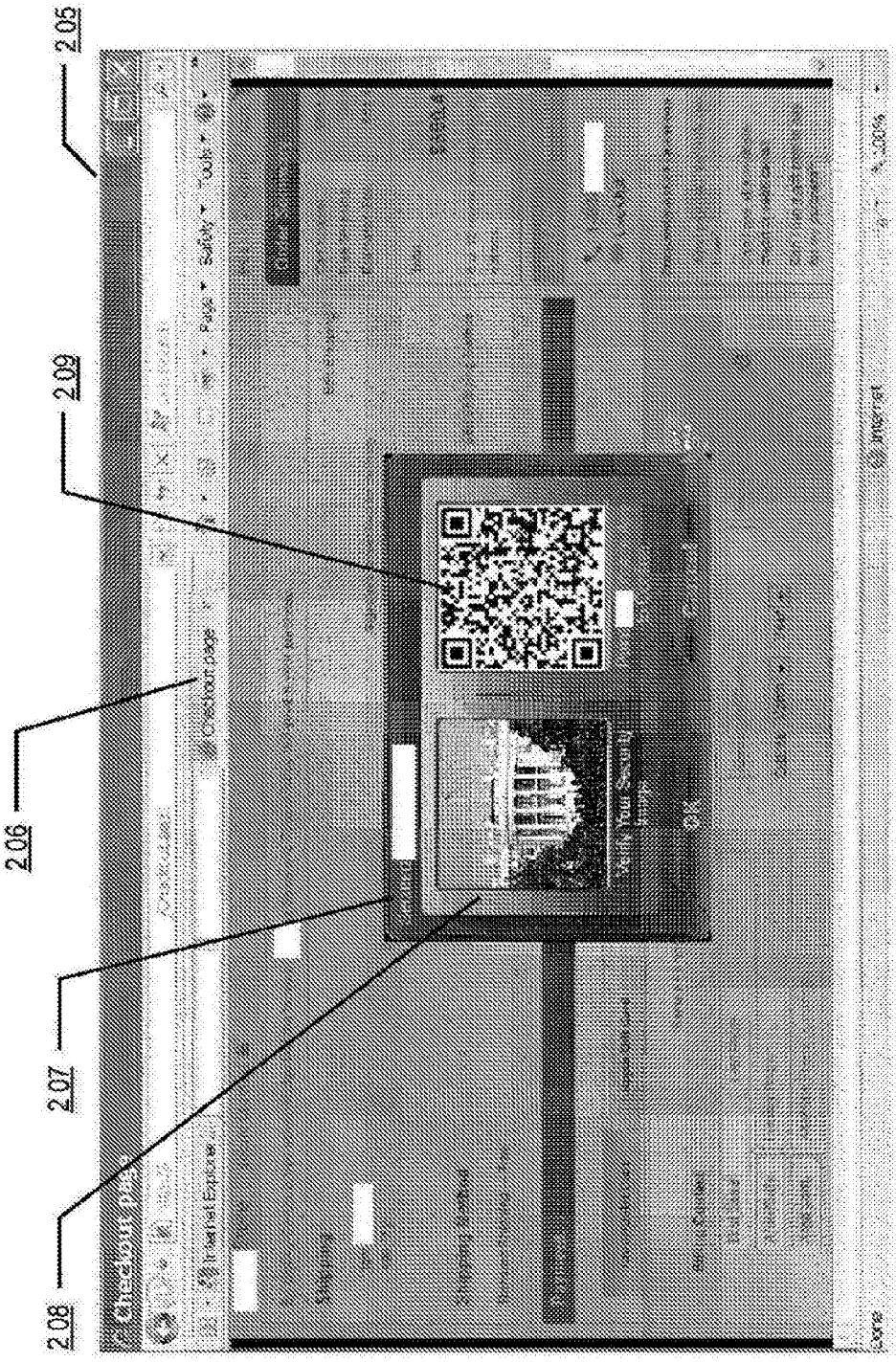


图1F



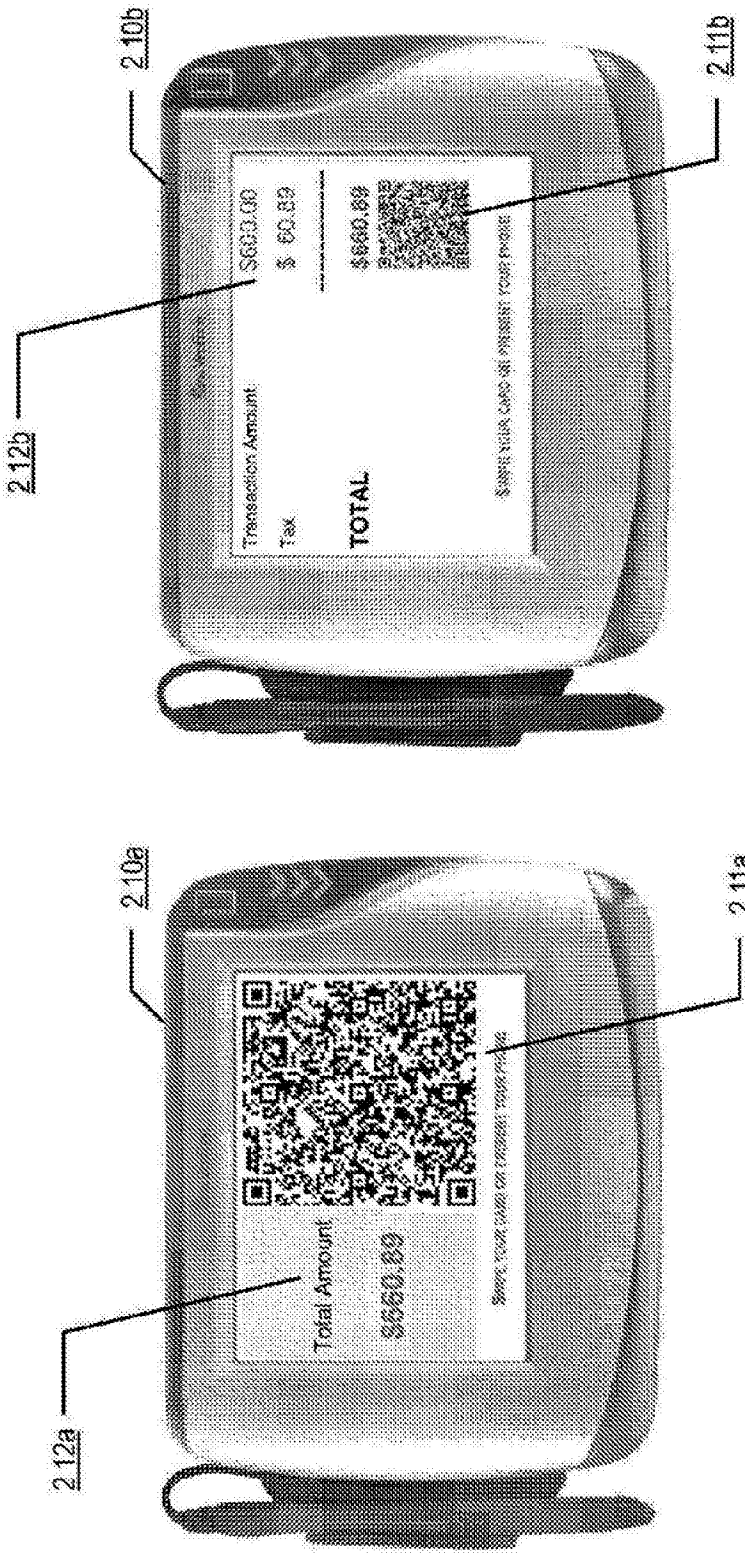
示例：快拍移动支付用户界面

图2A



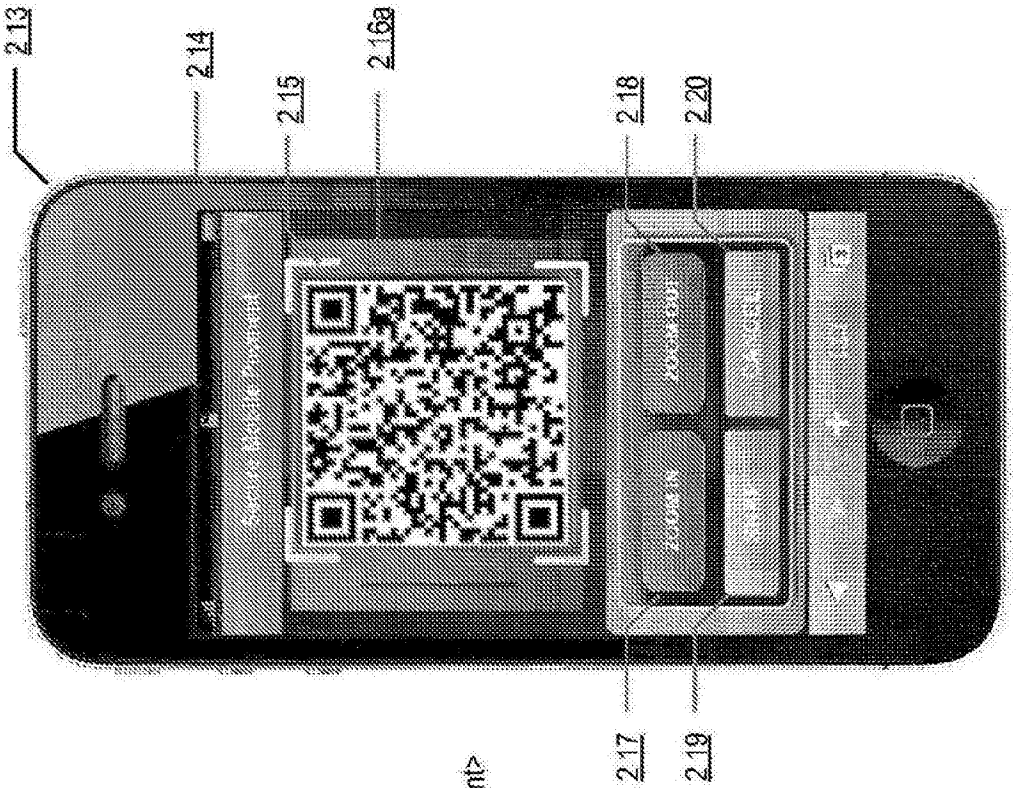
示例：快拍移动支付网络界面

图2B



示例：快拍移动支付POS终端界面

图2C



示例 QR 代码数据内容 2.16b

```
<data>
    <merchant_id>AE783</merchant_id>
    <merchant_name>Acme, Inc.</merchant_name>
    <store_id>88234</store_id>
    <store_url>www.shop.acme.com</store_url>
    <terminal_id>userdevice1</terminal_id>
    <transaction_id>AFE12133444</transaction_id>
    <timestamp>2011-04-01:23:59:59</timestamp>
    <transaction_amount>$660.89</transaction_amount>
    <digital_sign>
        45a2085fa20496c91df574dc5652e145
    </digital_sign>
</data>
```

图2D

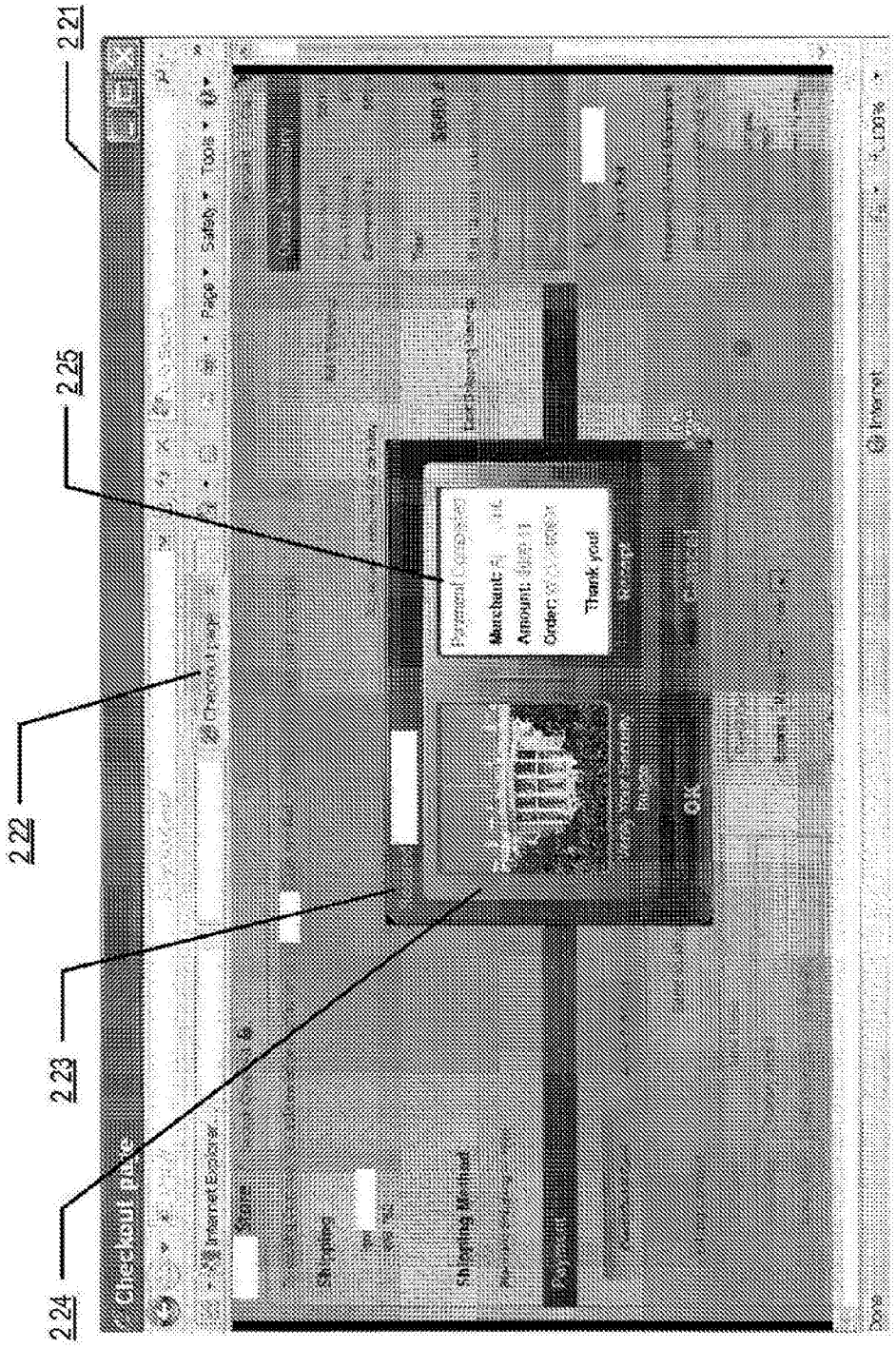


图2E

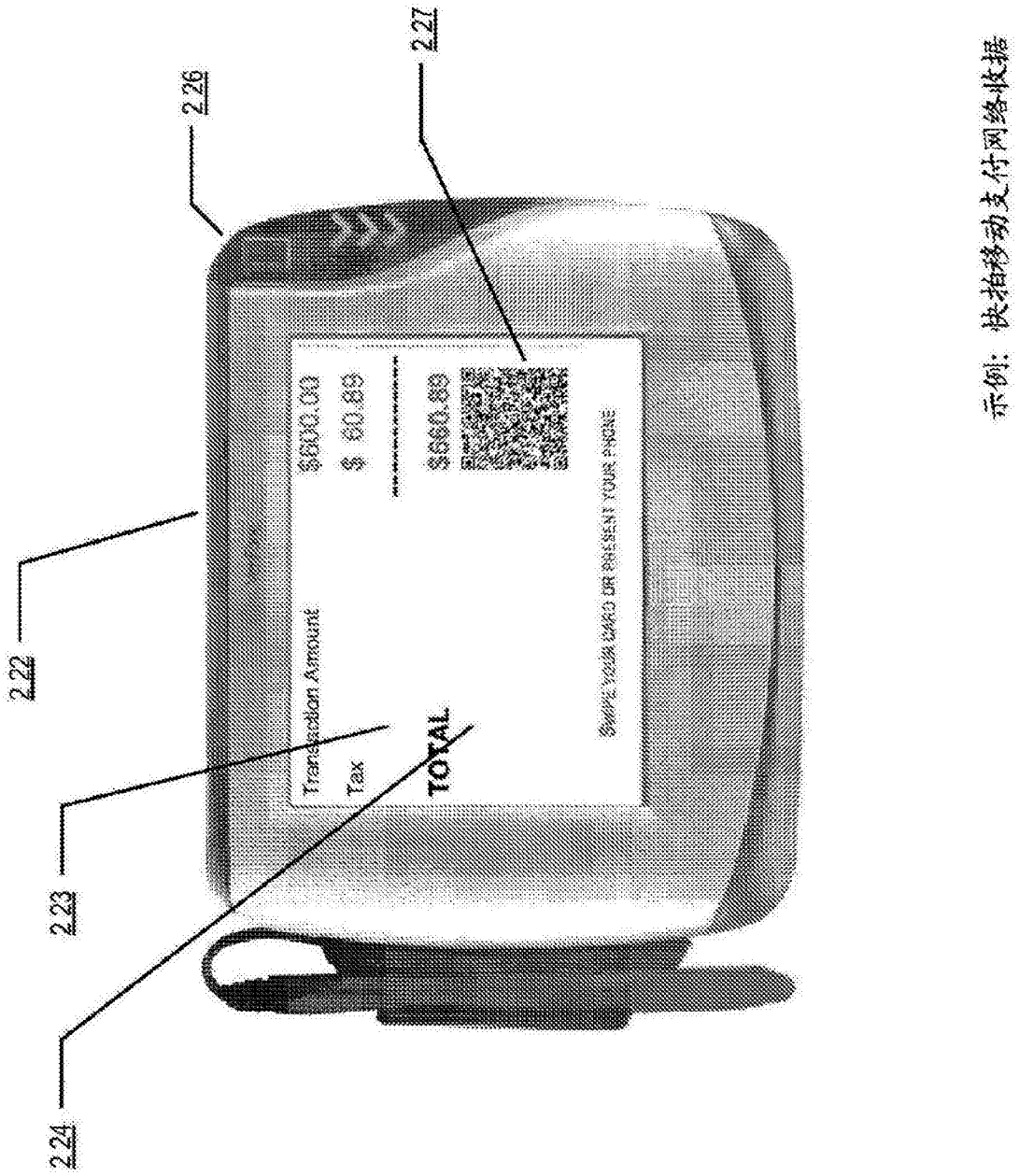


图2F

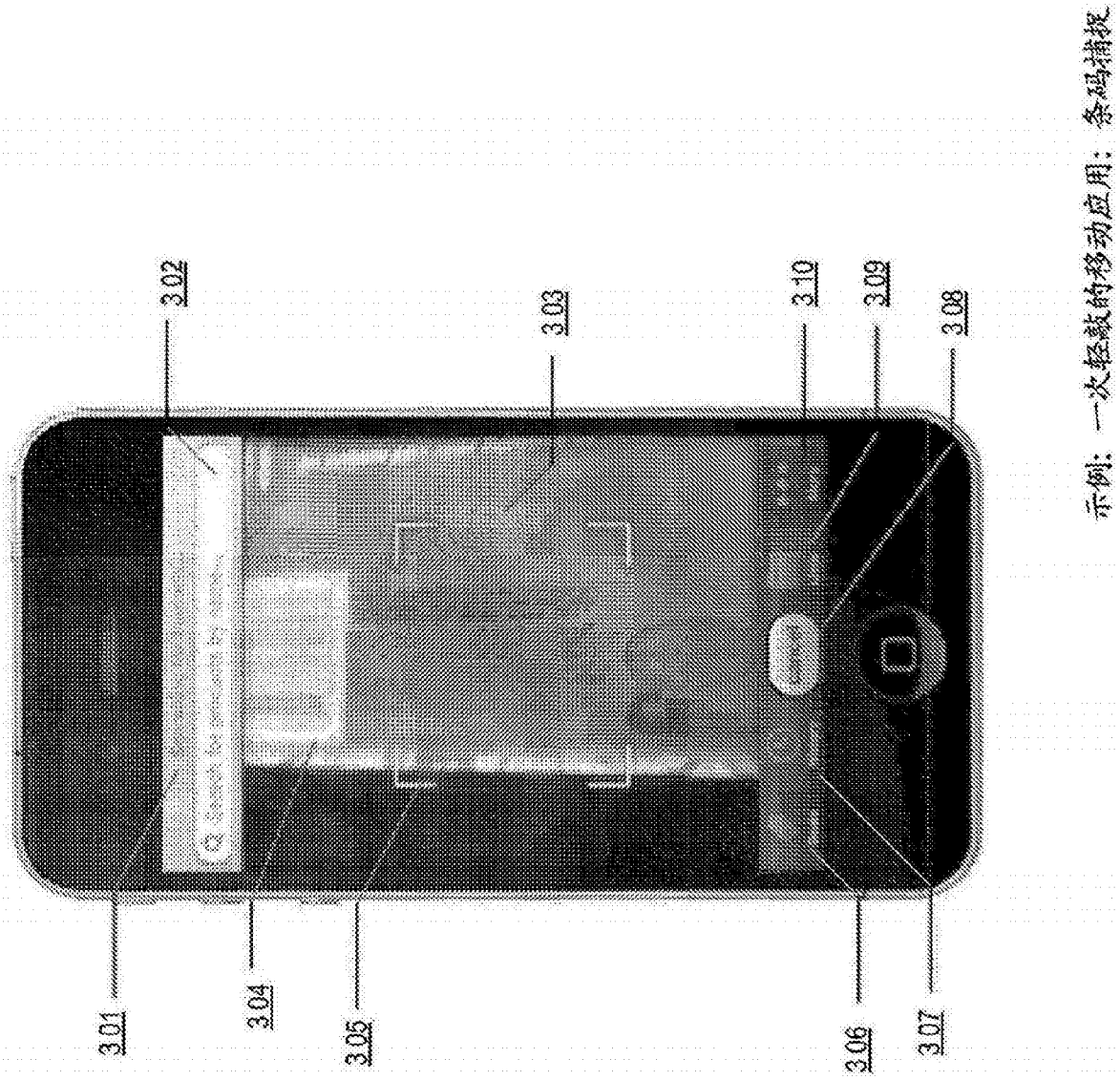


图3A

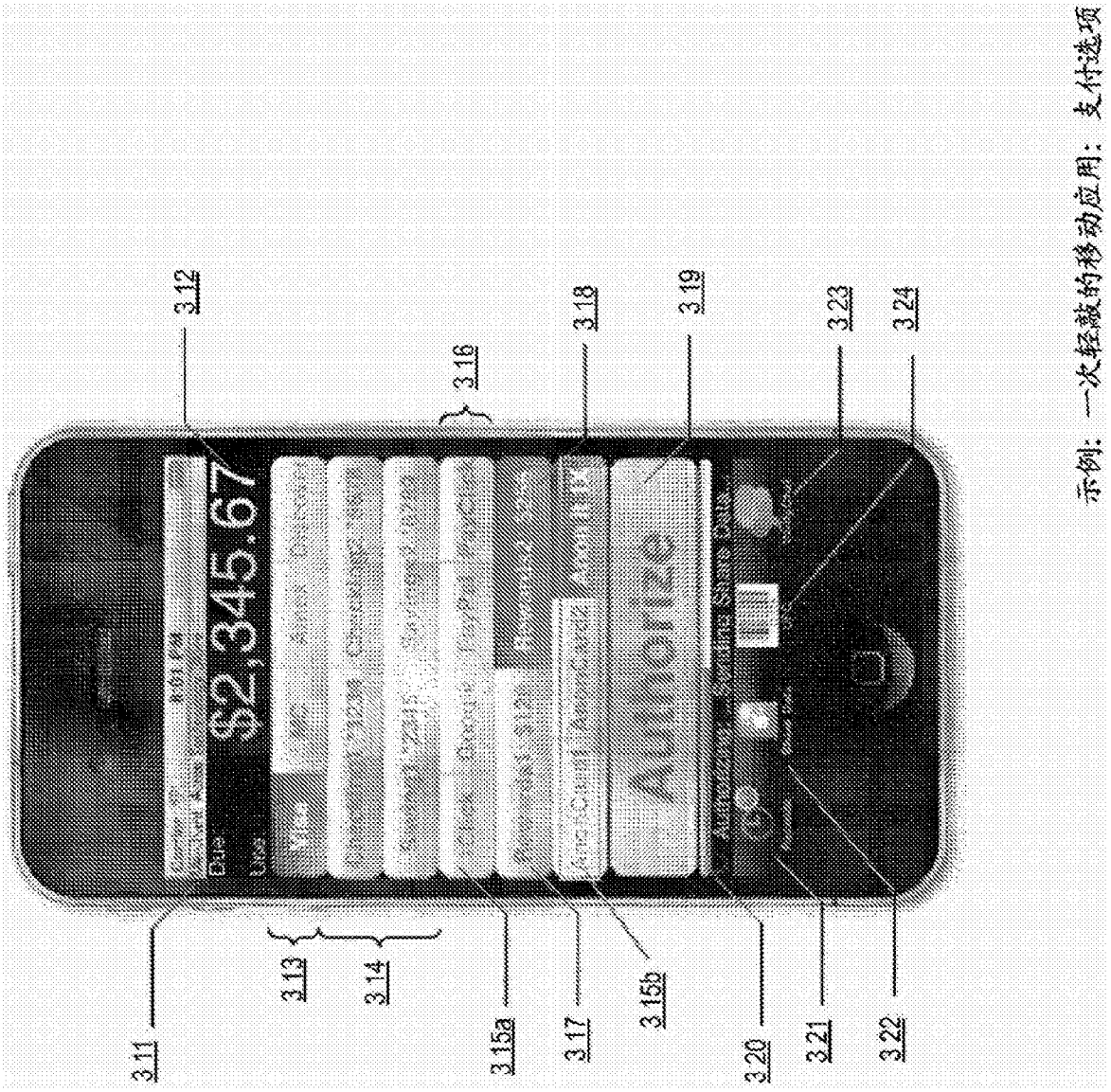
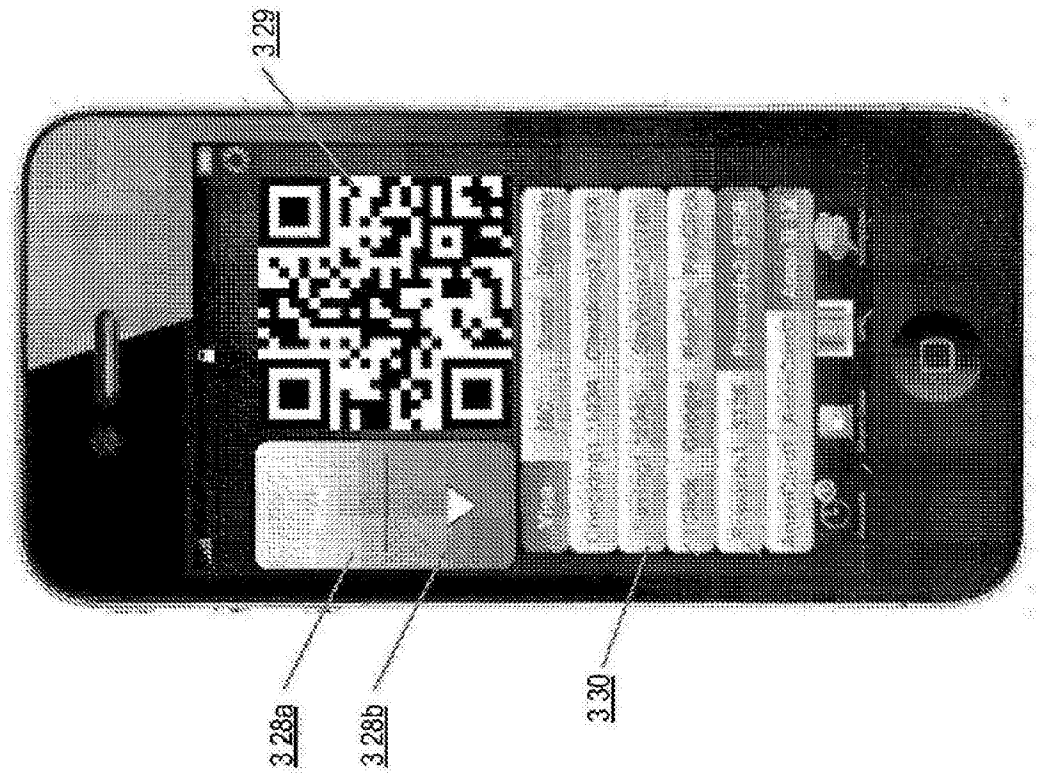


图3B



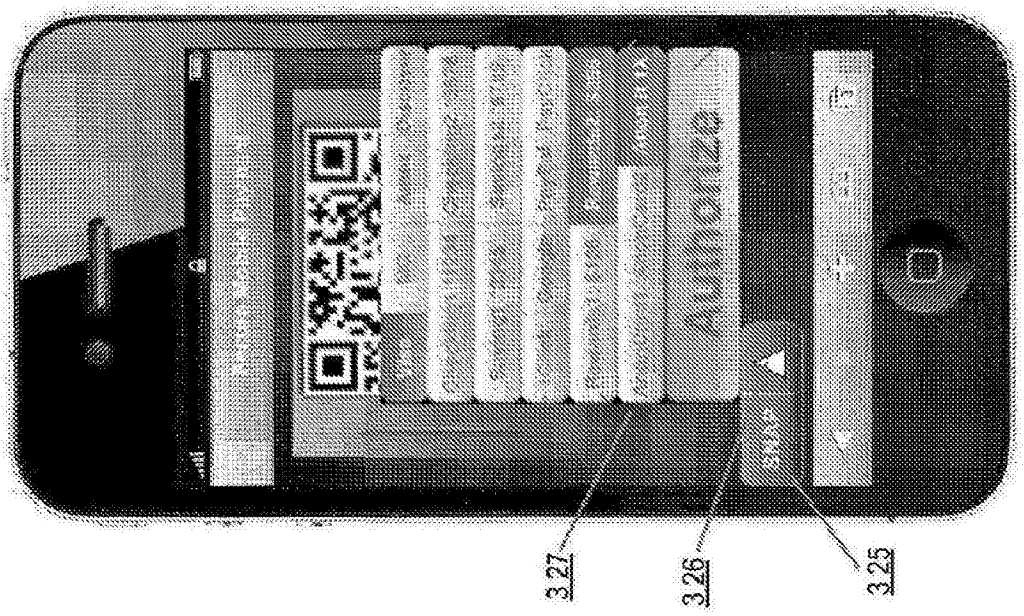


图3C