be updated immediately after the enrollment application server **220** receives new or updated information, or periodically (e.g., every hour, at the end of the day, etc.).

[0065] The alert trigger records are then sent to the system which will be detecting the trigger for the alert so that the system knows under what conditions the consumer **205** would like an alert. These trigger records may be sent on demand (e.g., when the consumer **205** makes a change) or periodically (e.g., hourly, daily, etc.). In one embodiment, the system detecting the alert may be a payment processing network **240**. In another embodiment the system detecting the alert may be an issuer **210**.

[0066] In some embodiments, alerts may be sent after other certain conditions are met. For example, the conditions associated with a particular purchase transaction may first be evaluated by a payment processing organization or issuer to determine if an alert is to be sent. For example, a payment processing organization or issuer may determine that the particular transaction being evaluated is a mail order-telephone order type of purchase (i.e., a MOTO transaction), is a risky transaction (e.g., because the transaction is being conducted by a merchant who has had risk issues in the past), and/or is over a certain dollar limit (e.g., over $30 in value). In such embodiments, it may be that the alert is only sent if these conditions are met. Such conditions may be set by the payment processing organization or the issuer, with or without the participation or knowledge of the consumer.

[0067] FIG. 3 shows a flowchart including a general method according to an embodiment of the invention. The method can be described with reference to the block diagram in FIG. 2.

[0068] In a typical transaction a consumer **205** may use the portable consumer device **200** to make a purchase via a payment processing network **240**. For example, the consumer **205** may use a portable consumer device (step **300**), such as a credit card, to pay $5000 for a flat screen television. Once the consumer **205** uses the portable consumer device **200** (e.g., swipes his credit card at a merchant as shown in FIG. 1(a) and described earlier), an authorization request message passes to the payment processing network **240**. The payment processing network **240** checks to see if the characteristics of the transaction that has been

made with the portable consumer device **200** matches a condition (e.g., notification event trigger) under which a consumer wants to be alerted (step **310**).

[0069] There are a number of examples of notification event triggers. Examples of notification event triggers include the following: a transaction is over a certain amount of money (e.g. over $5000); any transaction conducted with a particular portable consumer device; a spending threshold (e.g., a daily or monthly spending limit) has been reached for a particular portable consumer device; a transaction is made outside a particular geographic location (e.g., outside the country that the consumer resides in); a risky transaction is being conducted ("risky" may be predefined by the consumer and/or the issuer), a transaction is made without the physical portable consumer device (e.g., Internet, mail, or telephone order); a cash transaction or withdrawal; an online account has been accessed; a person has used the portable consumer device to enter a certain location (e.g., a secure area, a business after-hours); a payment is due within a certain amount of time; a payment is overdue; a child or spouse has conducted a transaction; a balance on the portable consumer device is exceeded; a particular type of transaction is being conducted (e.g., purchases for airline tickets, lodging, auto rental, restaurants, medical, etc.), etc. Thus, embodiments of the invention are flexible enough to allow for many types of notification event triggers.

[0070] If there is no notification event trigger, then the notification process ends (step **315**). If there is a notification event trigger, the payment processing network **240** sends the trigger information to the notification server **250**. The notification server **250** checks the SQL DB Server **230** to see how (or even if) the consumer **205** would like to be notified about the credit card transaction (step **320**). If the consumer **205** does not want to be alerted about this particular type of transaction, the notification process ends (step **325**).

[0071] If the consumer **205** would like to be notified about this particular type of transaction, then an alert is then sent to the consumer **205** via the communication mode (e.g., via a specific communication channel) specified by the consumer **205** (step **330**). Examples of communication modes include voice, mobile, SMS, e-mail, instant message, IVR (interactive voice response). etc.

[0072] As noted above, consumer may specify one or more communication mode per notification event trigger. For example, a consumer may want to be notified when a purchase is made that is over $5000 by mobile phone and e-mail. In addition, a consumer may specify one or more contacts for each communication mode. For example, a consumer **205** can have multiple mobile numbers (e.g., the consumer's personal mobile phone, work mobile phone, spouse's mobile phone number), multiple phone numbers (e.g., home phone, work phone), multiple SMS addresses (e.g., mobile phone, PDA, secretary's PDA), or multiple e-mail addresses (e.g., work e-mail, personal e-mail), etc. A consumer may also customize the time that he wants to receive each or all alerts. For example, the consumer may want to be notified immediately of the transaction, only during certain hours (e.g., between 9 a.m. and 5 p.m.), may specify different communication modes for different times of the day or types of transactions, or may choose not to be notified during certain hours (e.g., between 1 a.m. and 6 a.m.).

[0073] Thus, a consumer can specify that he wants to receive a notification if his portable consumer device is used for a transaction over a certain amount of money (e.g., over $5000), via his work phone number and spouse's e-mail if it is during the day, and by SMS and home phone if the transaction occurs on the evening or weekend. The alert may be sent to a notification device **290** via a gateway **260** and aggregator **280** using the specified communication mode. The alert text or message may also be customized to the consumer, such as, "Mark, your credit card account ending in 9999 was just used for a purchase by phone for $500.00. Please contact 555-555-5555 if this is incorrect."

[0074] A consumer may also want the alert to be escalated if the alert was not received. An alert may not be received if it could not be delivered (e.g., the mobile phone network was down, the consumer's number has been de-listed), or the consumer does not acknowledge the alert message within a certain time (e.g., respond to the message, listen to the voicemail, open the SMS message or e-mail). A status message regarding whether or not a consumer has received the alert is sent to the notification server **250** via aggregator **280** and gateway **260**, and is stored in the SQL DB Server **230**. The notification server **250** evaluates whether or not the alert should be escalated (e.g., whether the alert was received and whether the consumer has specified that he wants the alert to be escalated). If the alert was not

received, then the notification server **250** can retry the same communication mode or try a different communication mode based on the consumer preference or default settings. For example, a consumer may have an alert set for a purchase made out of the country in which he resides. He may want the alert be sent to his PDA that he generally carries with him. However, if he does not receive the message on his PDA either because the PDA service is down or he does not have it with him, he can specify that the alert then be sent to a different contact or to each of his other contacts until the system knows that he has received the alert.

[0075] The system may also include timers to send status messages so that the consumer **205** knows whether or not the portable consumer device has been used for a transaction. For example, a consumer **205** may want a timer that alerts him daily at 7 a.m. that he used portable consumer device **200** twice the day before or for certain types of purchases made with the portable consumer device **200**.

[0076] Further, the consumer **205** may want to be alerted if the portable consumer device **200** is used to access a certain location. This can be characterized as an access transaction. For example, a portable consumer device **200** can be an access device to gain entrance to a building or other location. An employee may enter a particular business after-hours or enter a secure area of that business. The consumer **205** may want to receive an alert that the employee has used the portable consumer device **200** to enter the secure area. For example, if Joe Employee enters the secure server room after business hours, the consumer **205** may receive an SMS message on his mobile phone that says "Joe Employee has entered secure area A (the server room)."

[0077] Embodiments of this invention have a number of advantages. First, a consumer can completely customize how, when, and if he wants an alert for some or all transactions made with the portable consumer device, and thus has complete control over the notifications for his portable consumer device. This also allows a better chance of detecting a potentially fraudulent act because the consumer will likely receive the alert in a timely manner so that he can respond to the alert if necessary. Also, there is a better chance at stopping back to back fraudulent acts since the consumer can react quickly to the alert. Further, the consumer can track access of secure areas or general employee activity of using the portable consumer

device. The consumer can also track activity of a child or spouse using the portable consumer device. Finally, the consumer is assured of receiving the alert through the escalation process if he does not receive the alert on the first communication mode or contact it is sent to.

[0078] It should be understood that the present invention as described above can be implemented in the form of control logic using computer software in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement the present invention using hardware and a combination of hardware and software.

[0079] Any of the server computers, client computers, and even some portable consumer devices described above may utilize any suitable number of subsystems. Examples of such subsystems or components are shown in FIG. 5. The subsystems shown in FIG. 5 are interconnected via a system bus **775**. Additional subsystems such as a printer **774**, keyboard **778**, fixed disk **779**, monitor **776**, which is coupled to display adapter **782**, and others are shown. Peripherals and input/output (I/O) devices, which couple to I/O controller **771**, can be connected to the computer system by any number of means known in the art, such as serial port **777**. For example, serial port **777** or external interface **781** can be used to connect the computer apparatus to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via system bus allows the central processor **773** to communicate with each subsystem and to control the execution of instructions from system memory **772** or the fixed disk **779**, as well as the exchange of information between subsystems. The system memory **772** and/or the fixed disk **779** may embody a computer readable medium.

[0080] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such

as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0081] The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0082] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0083] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving information that a transaction associated with a portable consumer device is occurring; and

providing an alert to a consumer associated with the portable consumer device, wherein the alert indicates that the transaction is occurring, wherein the alert is sent to the consumer according to a time or communication mode previously specified by the consumer using an interface that allows the user to specify the time and communication mode for receiving the alert.

2. The method of claim 1 wherein the alert is sent to the consumer if the transaction that is occurring is over a predetermined amount, the transaction is of a predetermined type, the transaction is made outside a geographic location specified by the consumer, the transaction is determined to be a risky transaction, the transaction being conducted without the portable consumer device being physically present at a point of sale, the transaction is a cash transaction, the transaction is a particular type of user-defined transaction, the transaction involves account access, the transaction indicates that a person is entering or exiting a location, the transaction indicates that a payment is due or overdue, or the transaction indicates that a specified person is conducting the transaction.

3. The method of claim 1 wherein the alert is sent to the consumer according to the time and communication mode previously specified by the consumer.

4. The method of claim 1 wherein a portable consumer device is in the form of a card, and wherein the alert is sent to a phone operated by the consumer.

5. The method of claim 1 wherein the alert is a first alert, and wherein a second alert is sent to the consumer through another communication mode.

6. The method of claim 1 further comprising:

receiving, via an interface, a user-specified time and communication mode for receiving the alert.

7. The method of claim 1 wherein the communication mode includes using at least one of a phone call, voicemail, SMS, instant message, and an e-mail.

8. The method of claim 1 wherein the consumer previously provided a trigger specifying a condition under which the alert would be sent.

9. A computer readable medium comprising:

code for receiving information that a transaction associated with a portable consumer device is occurring; and

code for providing an alert to a consumer associated with the portable consumer device, wherein the alert indicates that the transaction is occurring, wherein the alert is sent to the consumer according to a time or communication mode previously specified by the consumer using an interface that allows the user to specify the time and communication mode for receiving the alert.

10. The computer readable medium of claim 9 wherein the alert is a first alert, and wherein the computer readable medium further comprises code for sending the second alert to the consumer through another communication mode.

11. The computer readable medium of claim 9 wherein the information is received via a payment processing network, and wherein the payment processing network is configured to process credit and debit card transactions.

12. The computer readable medium of claim 9 wherein the alert is in the form of a phone call.

13. A server computer comprising the computer readable medium of claim 9.

14. The server computer of claim 13 wherein the server computer is in communication with a payment processing network.

15. The server computer of claim 13 wherein the alert is a first alert, and wherein the computer readable medium further comprises code for sending the second alert to the consumer through another communication mode.

16. A client computer comprising a processor, and a computer readable medium, wherein the computer readable medium comprises instructions for executing a method comprising:

receiving information on how to be notified if a predetermined activity is occurring with respect to a portable consumer device, wherein an alert is provided in manner consistent with the information provided if the predetermined activity is occurring wherein the information provided is a result of a consumer's choice to customize an alert for each predetermined activity by using an interface that allows a user to customize the alert according to at least communication mode and time; and

sending the information to a notification server.

17. The client computer of claim 16 further comprising a display coupled to the processor, wherein the display displays an interface showing the consumer customized times, communication modes, and triggers for alerts.

18. The client computer of claim 16 wherein the interface is a Web interface.

19. The client computer of claim 16 wherein the alert is in the form of a phone call.

20. A method comprising:

providing information on how to be notified if a predetermined activity is occurring with respect to a portable consumer device; and

receiving an alert in manner consistent with the information provided if the predetermined activity is occurring wherein the information provided is a result of

the consumer's choice to customize an alert for each predetermined activity by communication mode and time.

21. The method of claim 20 wherein the information provided includes a time when a consumer wants to be notified.

22. The method of claim 20 wherein the information provided includes a date when a consumer wants to be notified.

23. The method of claim 20 wherein the information provided includes a communication mode by which a consumer wants to be notified.

24. The method of claim 20 wherein the communication mode includes a phone call, voicemail, SMS, instant message, and e-mail.

25. The method of claim 20 wherein the alert is initiated after conditions set by an issuer or payment processing organization are met.

26. A phone comprising a processor, and a computer readable medium coupled to the processor, wherein the computer readable medium comprises code for receiving an alert, wherein the alert indicates that the transaction is occurring, wherein the alert is sent to the consumer according to a time or communication mode previously specified by the consumer using an interface that allows the consumer to specify the time and communication mode for receiving the alert.

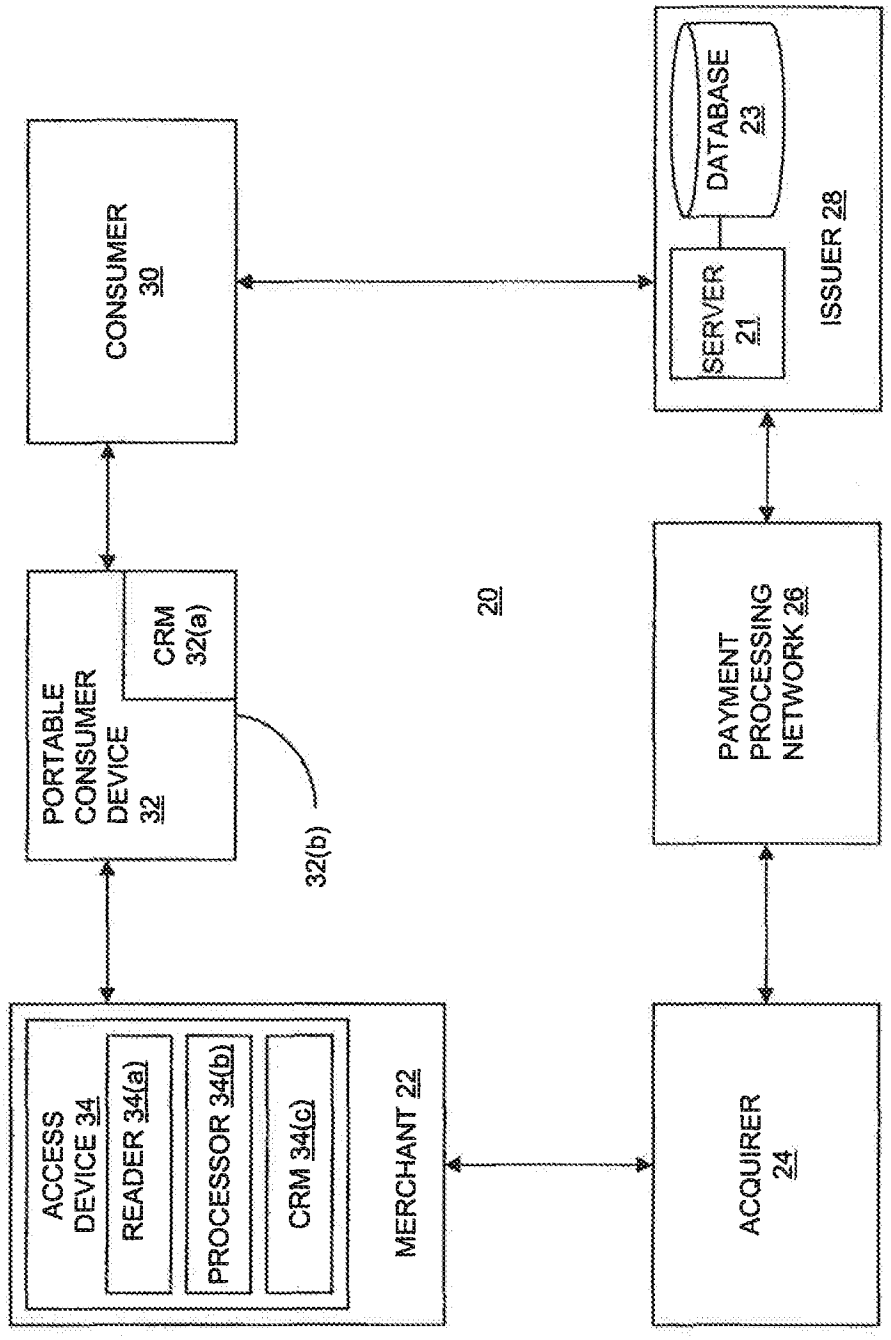

CONSUMER
30
DATABASE
23
SERVER
21
ISSUER 28
PORTABLE
CONSUMER
DEVICE
32
CRM
32(a)
32(b)
20
PAYMENT
PROCESSING
NETWORK 26
ACCESS
DEVICE 34
READER 34(a)
PROCESSOR 34(b)
CRM 34(c)
MERCHANT 22
ACQUIRER
24

FIG. 1(a)

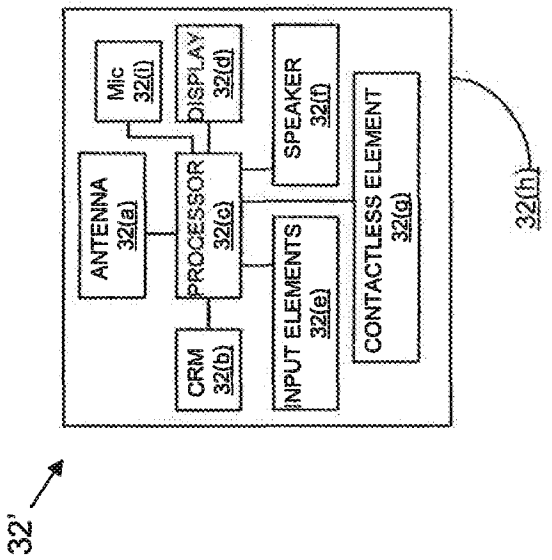

32'
ANTENNA 32(a)
Mic 32(i)
DISPLAY 32(d)
PROCESSOR 32(c)
SPEAKER 32(f)
CRM 32(b)
INPUT ELEMENTS 32(e)
CONTACTLESS ELEMENT 32(g)
32(h)

FIG. 1(b)

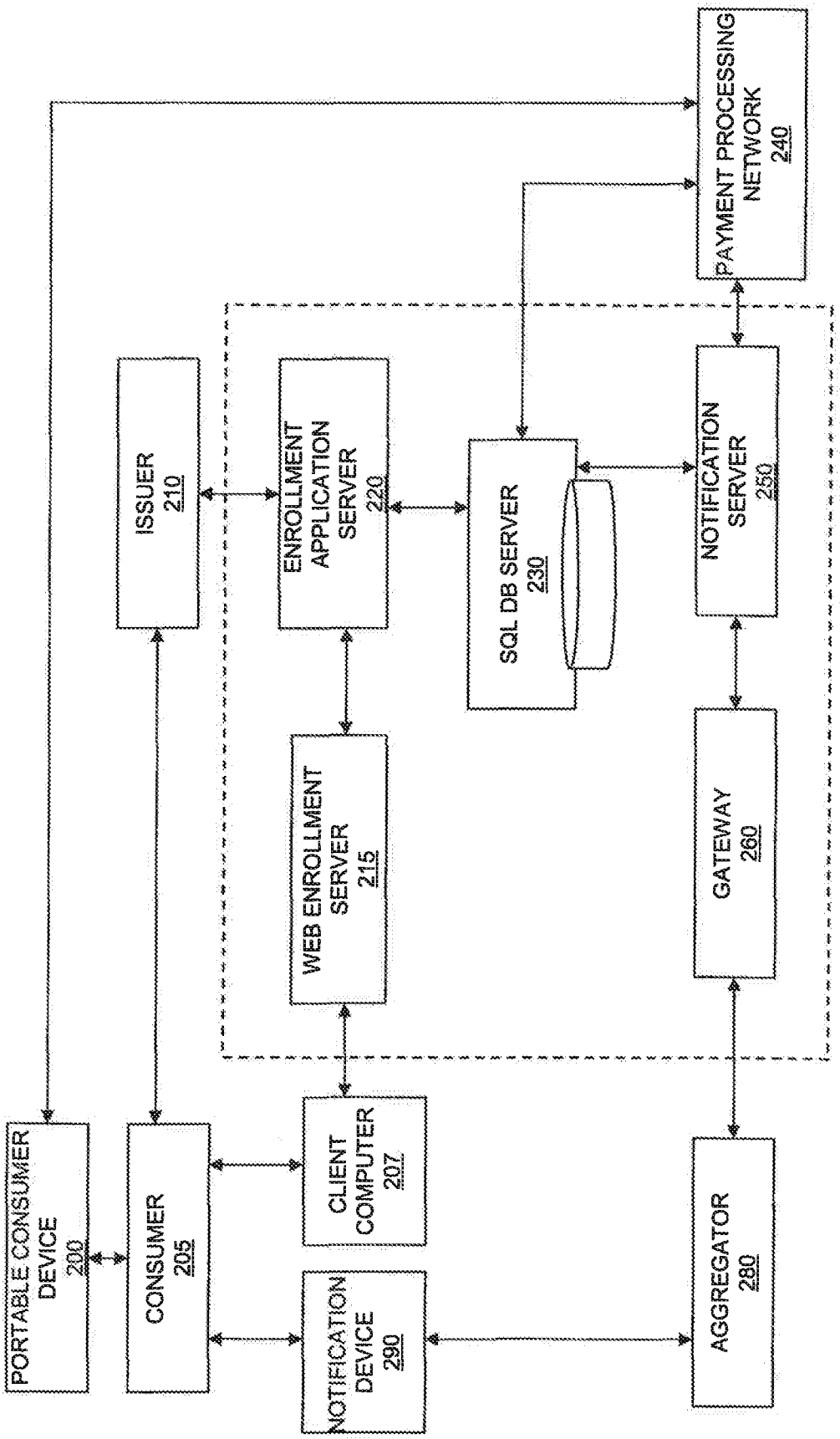

PAYMENT PROCESSING NETWORK 240
ISSUER 210
ENROLLMENT APPLICATION SERVER 220
SQL DB SERVER 230
NOTIFICATION SERVER 250
WEB ENROLLMENT SERVER 215
GATEWAY 260
PORTABLE CONSUMER DEVICE 200
CONSUMER 205
CLIENT COMPUTER 207
NOTIFICATION DEVICE 290
AGGREGATOR 280

FIG. 2

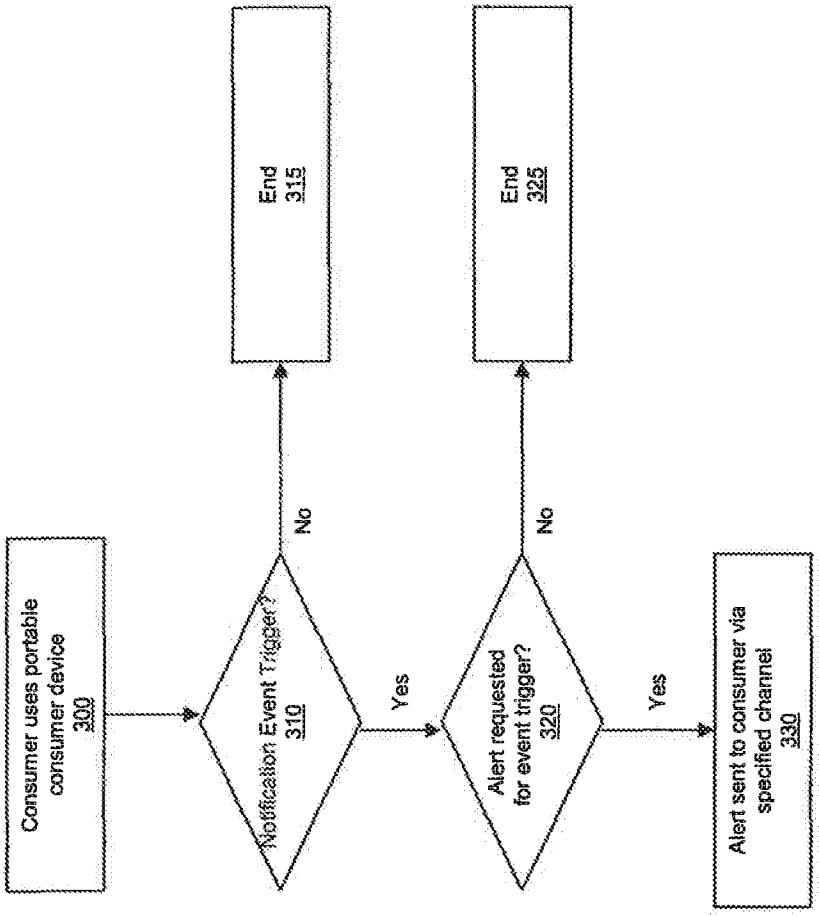

Consumer uses portable consumer device 300
Notification Event Trigger? 310
No
End 315
Yes
Alert requested for event trigger? 320
No
End 325
Yes
Alert sent to consumer via specified channel 330

FIG. 3

Customized Notification Page

Account Number: 12345678

Alert Mode	Alert times	Alert trigger
Cell Phone 415-555-5555	7 am to 10 pm	Over $100
Home Phone 415-555-5555	10:01 pm to 6:59 am	Any amount
Mobile e-mail device	All day	Over $100

FIG. 4

Petitioner Exhibit 1002-0594

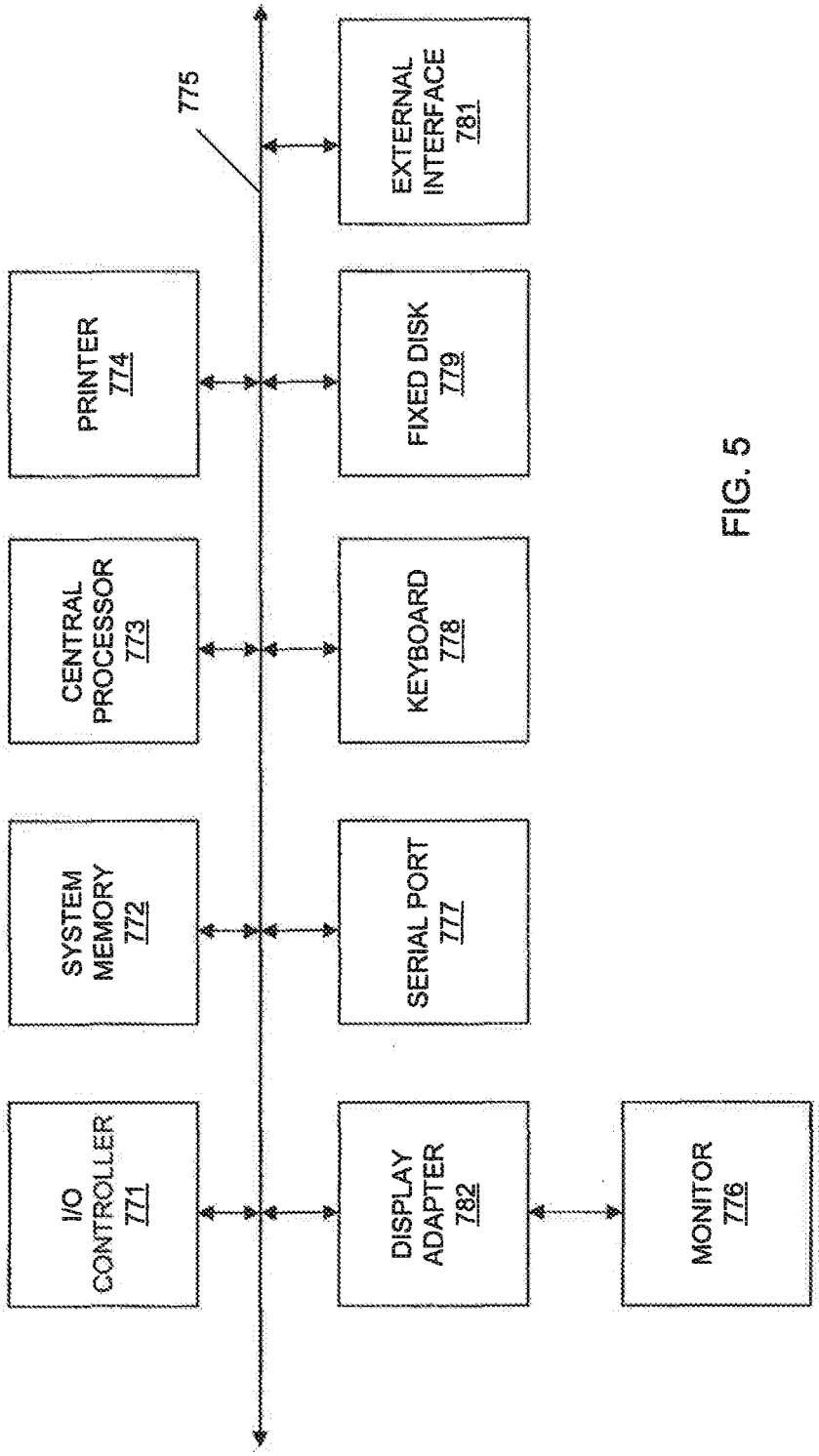

775
EXTERNAL INTERFACE 781
PRINTER 774
FIXED DISK 779
CENTRAL PROCESSOR 773
KEYBOARD 778
SYSTEM MEMORY 772
SERIAL PORT 777
I/O CONTROLLER 771
DISPLAY ADAPTER 782
MONITOR 776

FIG. 5

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 July 2008 (10.07.2008)

PCT

(10) International Publication Number
WO 2008/083089 A1

(51) International Patent Classification:
G06Q 40/00 (2006.01)

(21) International Application Number:
PCT/US2007/088615

(22) International Filing Date:
21 December 2007 (21.12.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/871,898 26 December 2006 (26.12.2006) US

(71) Applicants *(for all designated States except US)*: **VISA U.S.A. INC.** [US/US]; P.O. Box 8999, MS M3-2B, San Francisco, California 94128 (US). **VISA INTERNATIONAL SERVICE CORPORATION** [US/US]; 900 Metro Center Boulevard, Foster City, California 94404 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **CARLSON, Mark** [US/US]; 153 Miramontes Avenue, Half Moon Bay, California 94019 (US).

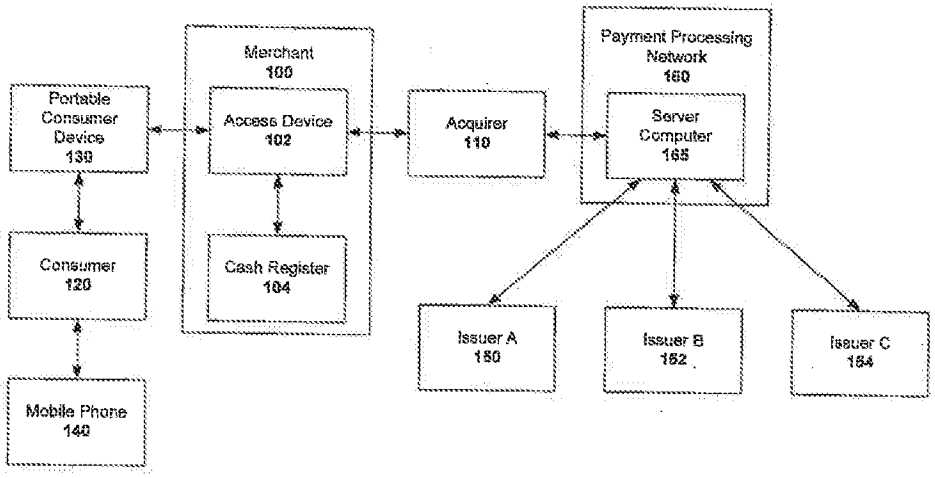
(74) Agents: **FARRELL, John J.** et al.; TOWNSEND AND TOWNSEND AND CREW LLP, Two Embarcadero Center, 8th Floor, San Francisco, California 94111 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(54) Title: COUPON OFFERS FROM MULTIPLE ENTITIES



(57) Abstract: Offers from multiple entities provide an incentive for consumers to behave in a manner that is beneficial to the offer provider. Each offer is associated with rules that establish conditions that must be met for the offer to be valid. For example, a rule may be established to promote the use a specific form of payment, such as a particular credit card. Thus, the offer would only be valid if the consumer paid for the merchandise using the particular credit card. A merchant may generate its own offers or receive offers from a variety of sources (e.g., a payment processing organization, an issuer, or other external sources).

WO 2008/083089 A1

Petitioner Exhibit 1002-0596

COUPON OFFERS FROM MULTIPLE ENTITIES

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] The present application claims priority from U.S. Provisional Patent Application No. 60/871,898, filed December 26, 2006, which is incorporated by reference herein in its entirety.

BACKGROUND

[0002] A coupon is a ticket or a document that can be exchanged for a financial discount or rebate when purchasing a product. Coupons provide a popular method to promote the sale of goods and services. Customarily, coupons are issued by manufacturers of consumer packaged goods or by retailers to be used in retail stores as a part of sales promotions. Coupons are often widely distributed through mail, magazines, newspapers, the Internet, and mobile devices such as cell phones.

[0003] To redeem a coupon, a consumer presents merchandise to be purchased to a cashier at a retail outlet. After the merchandise is scanned for purchase, the consumer provides the coupon to the cashier. The cashier then scans or keys in the coupon at a cash register. Conventional coupons only relay a limited amount of information to the cash register. Examples of data relayed to the cash register include a coupon number, an expiration date, a number of redeemed coupons, and the product for which the coupon is applicable. The cash register uses this information to access a local database and accept or reject the offer provided by the coupon. The coupons corresponding to the accepted offers are applied to the corresponding goods.

[0004] Coupons are generally issued by merchants and manufacturers to promote particular goods. However, other entities may also wish to influence consumer behavior. What is needed is a method to provide different entities such as a merchant, a payment processing organization, and an issuer with a means to provide offers to a consumer.

BRIEF SUMMARY

[0005] Embodiments of the invention are directed to providing coupon offers from multiple entities to consumers. The offers provide an incentive for consumers to behave in a manner that is beneficial to the offer provider. Each offer is associated with rules that establish conditions that must be satisfied for the offer to be valid. For example, a rule may be established to promote the use of a specific form of payment, such as a particular credit card. Thus, the offer would only be valid if the consumer paid for the merchandise using the particular credit card. A merchant may generate its own offers or receive offers from a variety of sources (e.g., a payment processing organization, an issuer, or other external sources). Such offers may be generated in real time or during the transaction in embodiments of the invention.

[0006] Illustratively, a consumer shops for goods in a store. A merchant computer (e.g., a cash register) retrieves a SKU or barcode value associated with the goods to be purchased, or data associated with the goods to be purchased is manually entered into the merchant computer. The consumer provides at least one coupon that may be scanned or manually entered into the merchant computer. A server computer communicates with the merchant computer and a computer associated with the entity which provides the coupon to determine if rules associated with the coupon are satisfied. If the rules are satisfied, the savings provided by the coupon is subtracted from a total of the cost of the goods to be purchased. The new total is then presented to the consumer.

[0007] In an illustrative example, the consumer may have a coupon that provides an incentive to purchase the goods using a particular form of payment. For example, the goods to be purchased may be associated with one total that applies to a cash payment, a lower total if payment is made using a payment processing organization-sponsored card (e.g., a Visa card), and another lower total if payment is completed with a particular issuer's credit card. After the goods are scanned at the cash register, the consumer presents the coupon that provides a discount offer if a particular credit card is used. The consumer may then swipe the particular credit card at a point of sale terminal associated with the cash register. The merchant computer accesses a computer associated with the offer provider to determine

Petitioner Exhibit 1002-0598

whether the rules associated with the offer are satisfied. For example, the merchant computer access a rules engine in a computer associated with the particular credit card issuer to determine that the credit card swiped by the consumer at the point of sale corresponds to the particular credit card. After the rules engine determines that the rules associated with the offer are satisfied, the discounted total is presented to the consumer at the point of sale terminal. The point of sale terminal may also prompt the consumer to submit payment. The consumer then selects to pay for the goods such that the discounted total is charged to the particular credit card.

[0008] One embodiment of the invention is directed to a method including receiving a consumer identifier and an offer during a transaction. A validated offer is received from an entity which provides the offer, such as a payment processing organization or an issuer, when rules associated with the offer are satisfied. The offer is validated based on the consumer identifier. A selection of the valid offer is received to complete the transaction.

[0009] Another embodiment of the invention is directed to a method including receiving an offer and a consumer identifier for a consumer during a transaction and receiving a validated offer. The offer is validated by an entity which provides the offer when rules associated with the offer are satisfied. The offer is validated based on the consumer identifier. A selection of the validated offer is received to complete the transaction.

[0010] Another embodiment of the invention is directed to a system including an access device and a server computer in communication with the access device. The access device or the server computer is configured to: receive a consumer identifier and an offer during a transaction conducted with the access device and the server computer; receive a validated offer from an entity which provides the offer, wherein the offer is validated when rules associated with the offer are satisfied, the offer being validated based on the consumer identifier, wherein the entity is a payment processing organization or an issuer; and receive a selection of the valid offer to complete the transaction..

[0011] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. 1 shows an exemplary block diagram of a system for providing offers from multiple entities to a consumer according to embodiments of the invention.

[0013] FIG. 2 shows an exemplary block diagram of some elements that may be present in a mobile phone according to an embodiment of the invention.

[0014] FIG. 3 shows an exemplary block diagram of some elements that may be present in a server computer according to an embodiment of the invention.

[0015] FIG. 4 shows an exemplary block diagram of some elements that may be present in an access device according to an embodiment of the invention.

[0016] FIG. 5 shows a flow diagram of a method for providing offers to a consumer according to embodiments of the invention.

[0017] FIG. 6 shows a screen shot of an access device displaying different totals based on a particular payment method according to an embodiment of the invention.

DETAILED DESCRIPTION

[0018] Different entities may attempt to influence consumer behavior for different reasons. For example, a first party may include an issuing bank who may only care if a credit card being used is issued from the issuing bank. A second party may include a payment processing organization (e.g., Visa, a third party processor, etc.) who may only care if the payment processing organization's card is used. A third party may be a merchant who may only care if purchases are made at that merchant.

[0019] Embodiments of the invention can be used to introduce different types of coupon offers or other types of offers during a transaction. Such offers may include issuer coupons, payment processing organization coupons (e.g., acquirer coupons), merchant coupons, manufacturer coupons, etc.

[0020] In accordance with embodiments of the present invention, a point of sale terminal is configured to provide and/or redeem coupons only if appropriate rules are satisfied. For example, a payment processing organization offer may be redeemable by a consumer or provided to a consumer only if a payment processing organization branded credit card is used. In another example, an issuer (e.g., Citibank) may provide or redeem an offer if the consumer uses an issuer-specific credit card. In response to receiving various offers from the merchant, payment processing organization, or issuer, the consumer could then select a particular form a payment based upon the best offer that is provided to the consumer, and/or provide offers to encourage the consumer to buy specific products.

[0021] Some specific examples of coupon offers from different entities are provided below. In some embodiments of the invention, these different types of offers can be processed by a single access device (e.g., point of sale terminal), or could be processed by a server computer (e.g., residing at a payment processing organization or another location). The access device or the server computer could communicate with each of these entities during a payment transaction to determine which offers are valid.

- Partner merchant issued offers: Here, a merchant sets the goals of an offer. Although the merchant may care about the type of payment form that is used (e.g., cash vs. credit card), the merchant is generally not concerned with the brand of payment that is being used by a consumer as long as the consumer accepts that brand of payment. The merchant's goal is to persuade consumers to buy the merchant's products or services, and to potentially purchase specific products or services (e.g., items that are overstocked).
- Payment processing organization (e.g., acquirer) issued offers: The payment processing organization's goal may be to increase brand usage. The payment processing organization may only provide and redeem an offer if the consumer pays with a portable consumer device branded with the payment processing organization's service mark.
- Offers issued by an issuer: The issuer is generally not concerned with the particular payment processing organization that a portable consumer device is affiliated with. For example, an issuer such as Bank of America may issue credit cards using the Visa and Mastercard brands. Typically, the issuer may

be less concerned with whether the consumer uses a Visa or Mastercard branded credit card, as long as the consumer uses a card that is issued by Bank of America.

[0022] As used herein, a "transaction" may include, but is not limited to, the time when the consumer has selected goods or services to purchase and is ready to pay for them. For example, an exemplary transaction may include a time when a consumer selects products to purchase in a grocery store, and the selected products are scanned at a point of sale terminal such as a cash register. The consumer also provides at least one coupon at the point of sale terminal. The consumer is identified at the point of sale terminal by, for example, scanning a portable consumer device such as a credit or debit card. This scanned information (e.g., a SKU or stock keeping unit, an NLU or coupon identification number, an account number that identifies the consumer, etc.) may then be transmitted to a server computer. The server computer may then communicate with the entity associated with the offer (e.g., the merchant, payment processing organizations, and various issuers) to determine if rules associated with the offer are satisfied. If the rules are satisfied, the offer is applied to the goods to be purchased (e.g., the consumer is presented with a reduced total).

[0023] Illustratively, embodiments of the present invention are directed to offers from a variety of different entities that provide incentives to influence consumer behavior. Each offer is associated with certain rules that establish conditions to be satisfied in order for the offer to be valid. The merchant receives offers from a variety of sources (e.g., an acquirer, an issuer, or other external sources). The merchant may also generate its own offers to provide to consumers.

[0024] After a consumer selects goods in a store, the consumer approaches a point of sale terminal (e.g., a cash register or self-service check out terminal) to scan or otherwise enter the goods into a merchant computer. The consumer also provides a consumer identifier (e.g., a credit card number, alias, e-mail address, etc.) so that the identity of the consumer may be determined. The merchant computer retrieves a SKU or barcode value associated with the scanned goods, and any information associated with the consumer identifier. The consumer also provides at least one offer that may apply to the transaction. A server computer communicates

with an entity associated with the offer (e.g. the merchant computer, an acquirer computer, and/or various issuer computers) to determine if the rules associated with the offer are satisfied. If the rules associated with the offer are satisfied, the offer is validated and a discounted total is presented to the consumer at the point of sale terminal. The point of sale terminal may also prompt the consumer to submit payment. The consumer then selects to pay for the goods.

[0025] FIG. 1 shows an exemplary block diagram of a system for providing offers from multiple entities to a consumer in accordance with embodiments of the invention. The system includes a merchant **100** and an acquirer **110** associated with the merchant **100**. In a typical payment transaction, a consumer **120** may purchase goods or services at the merchant **100** using a portable consumer device **130** or a mobile phone **140**. FIG. 2 shows an exemplary block diagram of some elements that may be present in the mobile phone **140** according to an embodiment of the invention. The acquirer **130** can communicate with issuers (A, B, and C) **150**, **152**, **154** via a payment processing network **160** having a server computer **165**.

[0026] The acquirer **130** is typically a bank that has a merchant account. The issuers **150**, **152**, **154** may each also be a bank, but could be any business entity such as a retail store. Some entities are both acquirers and issuers, and embodiments of the invention include such entities. Each issuer **150**, **152**, **154** may operate its own server computer (not shown), which may have a computer readable medium comprising code for performing the functions that the issuer **150**, **152**, **154** performs. An issuer database (not shown) comprising account number information and other information may be operatively coupled to the server computer **165**.

[0027] The consumer **120** may be an individual or an organization such as a business that is capable of purchasing goods or services.

[0028] The portable consumer device **130** may be in any suitable form. For example, suitable portable consumer devices can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket. Example portable consumer devices may include smart cards, ordinary credit or debit cards (with a magnetic strip and without a microprocessor), keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. Other examples of portable consumer devices include cellular phones, personal digital assistants (PDAs),

pagers, contactless cards (e.g., an RFID card), payment cards, security cards, access cards, smart media, transponders, and the like. The portable consumer devices can also be debit devices (e.g., a debit card), credit devices (e.g., a credit card), or stored value devices (e.g., a stored value card).

[0029] The payment processing network **160** may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network may include VisaNet™. Payment processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services.

[0030] The server computer **165** of the payment processing network **160** is typically a powerful computer or cluster of computers. For example, the server computer **165** can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer **165** may be a database server coupled to a Web server. FIG. 3 shows an exemplary block diagram of some elements that may be present in the server computer **165** according to an embodiment of the invention. The payment processing network **160** may use any suitable wired or wireless network, including the Internet.

[0031] The merchant **100** includes an access device **102** that can interact with the portable consumer device **130** and the mobile phone **140**. FIG. 4 shows an exemplary block diagram of some elements that may be present in the access device **102** according to an embodiment of the invention. The merchant also includes a cash register **104** coupled to the access device **102**.

[0032] In a typical purchase transaction, the consumer **120** purchases goods or services at the merchant **100** using the portable consumer device **130**. The consumer's portable consumer device **130** interacts with the access device **102**. For example, the consumer **120** may swipe a credit card through a reader of the access device **102**. Alternatively, the reader may include a contactless reader, and the

portable consumer device **130** may be a contactless device such as the mobile phone **140**.

[0033] An authorization request message is then forwarded to the acquirer **110**. After receiving the authorization request message, the acquirer **110** sends the authorization request message to the payment processing network **160**. The server computer **165** forwards the authorization request message to the issuer **150**, **152** or **154** of the portable consumer device **130**.

[0034] After the issuer **150**, **152** or **154** receives the authorization request message, the issuer **150**, **152** or **154** sends an authorization response message back to the payment processing network **160** to indicate whether or not the current transaction is authorized. The server computer **165** forwards the authorization response message back to the acquirer **110**. The acquirer **110** sends the response message back to the merchant **100**.

[0035] After the merchant **100** receives the authorization response message, the access device **102** may provide the authorization response message to the consumer **120**. The authorization response message may be displayed on a touch screen, or may be printed out on a receipt.

[0036] At the end of the business day, a clearing and settlement process may be conducted by the payment processing network **160**. The clearing process exchanges financial details between the acquirer **110** and the issuer **150**, **152**, **154** to facilitate posting to a consumer's account and reconciliation of the consumer's settlement position.

[0037] Some of the embodiments described below may use a payment processing system like the one described above, or any suitable combination of components in the payment processing system.

[0038] In accordance with embodiments of the present invention, the system for providing coupon offers from multiple entities to a consumer is described below with reference to FIG. 1. The offers may be provided by the merchant **100**, the acquirer **110**, the issuer **150**, **152**, **154**, or any other entity seeking to influence consumer behavior such as the manufacturer of goods offered for sale by the merchant **100**.

[0039] Each issuer **150**, **152**, **154** may provide offers. The acquirer **110** may also generate offers. The merchant **100** may receive offers from other external sources such as from a manufacturer of goods offered for sale at the merchant **100**. The merchant **100** may also generate its own offers to provide to the consumer **120**. In one embodiment, the merchant **100** decides which offers to accept and which offers to decline. For example, an acquirer offer may conflict with an issuer offer. Thus, the merchant **100** may decide to provide only the acquirer offer to consumers.

[0040] Each offer is associated with one or more rules. The rules establish conditions to be satisfied for the offer to be valid. For example, an offer may be provided to a consumer that is valid only when the consumer uses a particular credit card. By using the credit card that corresponds to the offer, the consumer may receive a reduced price for the purchased goods or other incentives such as frequent flyer points. In another example, the rules may establish that an offer is only valid for a particular time period. Specifically, to provide an incentive for consumers to shop during off-peak hours, an offer may correspond to a particular time of day (e.g., the first two hours of retail operation). In another embodiment, the offer may correspond to the identity of the consumer combined with a particular day of the week or month (e.g., senior citizen discount on the third Tuesday of the month). Similarly, an offer may be provided for seasonal items after the season has ended. For example, summer merchandise discount offers may be valid during the months of September and October in an attempt to unload overstocked items.

[0041] The consumer **120** initiates a transaction by scanning merchandise that may be purchased at the merchant **100**. For example, after selecting goods to purchase at a retail outlet, the consumer **120** may approach a cashier or self-service check-out terminal to pay for the items. The transaction may be initiated when the consumer **120** or a cashier scans or keys in the items to be purchased using the cash register **104**. Any coupons or other offers may also be submitted using the cash register **104** or the access device **102**. For example, paper coupons may be scanned at the cash register **104** and electronic offers stored on the mobile phone **140** may be provided to the access device **102**.

[0042] A consumer identifier is provided during the transaction to identify the consumer. In one embodiment, the consumer **120** is identified at the access device

Petitioner Exhibit 1002-0606

102 by the mobile phone **140**. In another embodiment, the consumer **120** is identified by scanning the portable consumer device **130** (e.g., a credit card, a savings card associated with the merchant, a contactless card, etc.) at the access device **102**. The consumer identifier may correspond to the account number associated with the scanned payment card. In another embodiment, the consumer **120** identifies himself by entering a personal identification code at the access device **102** using a touch screen or some other input/output device.

[0043] After the consumer identifier and the item information are entered into the access device **102**, the offers are validated. The access device **102** identifies the entity associated with an applicable offer, and may then route the appropriate message to the entity associated with the applicable offer. The logic to do this may reside in hardware and/or software in the access device **102** or at a computer (e.g., a backend merchant computer) accessible to the access device **102**. In one embodiment, more than one offer may apply to the same item. If the offer is associated with the merchant **100**, the offer is validated at the merchant **100** to determine whether the rules that apply to the offer are satisfied. If the offer is associated with the acquirer **110**, the offer and the consumer identifier are forwarded to the acquirer **110** and a determination is made whether the offer is valid. Similarly, if the offer is provided by an issuer **150**, **152**, **154**, the offer and the consumer identifier are forwarded to the corresponding issuer **150**, **152**, **154** via the server computer **165** to determine the validity of the offer. In one embodiment, an offer is validated when the terms of the offer are satisfied. This may be done by matching conditions associated with the offer to a rules engine (not shown). The rules engine may be located at the merchant **100**, the acquirer **110**, the server computer **165**, and/or the issuers **150**, **152**, **154**.

[0044] For example, an offer provided by an issuer may only be valid if the consumer **120** purchases a quantity of three or more of a particular item. After the consumer **120** provides an offer indicator (e.g., an electronic coupon code) to the access device **102**, it retrieves the three or more item rule from the rules engine from the issuer which provides the offer via the server computer **165**, and then accesses the cash register **104** to identify whether three or more items have been purchased. The offer will not be validated if less than three of that item have been purchased.

[0045] In one embodiment, more than one rule may apply to an offer. For example, an offer may only be valid for a specific form of payment when an account balance associated with the specific form of payment is more than a predetermined amount. Thus, if the consumer **120** uses a different form of payment or if an account balance associated with the valid form of payment is less than the predetermined amount, the offer will not be validated.

[0046] Any number of rules may be associated with any offer. Example rules include: the type of payment, the time of day, the day of the week, the day of the month, the month of the year, the total quantity of items to be purchased, the quantity of a particular item to be purchased, consumer characteristics (e.g., age, gender, resident address, income level), etc. As one having ordinary skill in the art would appreciate, the list of example rules is not exhaustive and additional rules could be associated with an offer without departing from the spirit and scope of embodiments of the invention.

[0047] In accordance with one type of offer, the offer may be associated with the type of portable consumer device **130** that the consumer **120** used to identify himself (e.g., a credit card). The offer is validated by determining that the credit card that the consumer swiped at the access device **102** corresponds to the credit card that is associated with the offer. In one embodiment, the access device **102** may display a discounted amount to provide an incentive to pay using the credit card associated with the offer. Thus, the user is prompted to submit payment using the previously swiped credit card. Alternatively, the consumer **120** may be informed that the discount will be applied to the consumer's monthly credit card statement.

[0048] In one embodiment, the access device **102** may display different amounts based on the form of payment used by the consumer 120. Specifically, the access device **102** may display one amount if a particular credit card is used, another amount if a different credit card is used, and still another amount if payment is made by cash, check or a debit card. The consumer **120** then selects a payment method at the access device **102**. If the consumer **120** presents a new form of payment at the access device **102** (e.g., a credit card that had not been previously used at the merchant **100**), information associated with the new form of payment is stored at the merchant **100**. Thus, if the same form of payment is used at a later

Petitioner Exhibit 1002-0608

date, the access device **102** will recognize the consumer **120** and may provide offers associated with that form of payment.

[0049] In another example, the offer may provide incentives such as free or discounted items, or reward points based on a particular item that the consumer **120** has selected for purchase. Specifically, the consumer **120** may purchase ground coffee and the access device **102** provides this product information to an issuer that seeks to provide offers to consumers who purchase coffee. The issuer may then provide an offer to the consumer **120** at the access device **102** to receive a free cup of coffee at a nearby coffee retailer. The consumer **120** may accept the offer at the access device **102**. In one embodiment, the number of accepted offers is limited. For example, an offer for a free cup of coffee may be limited to thirty accepted offers on any given day.

[0050] The access device **102** sends the payment information provided by the consumer **120** to the cash register **104** to complete the purchase transaction. The access device **102** may begin reconciling the remittance for the offer. For example, if the offer was provided by an issuer **150**, **152** or **154**, the merchant **100** may request and retrieve the amount corresponding to the offer (e.g., the discounted amount) from that issuer. In one embodiment, offer remittance occurs at the end of the day during the clearing and settlement process.

[0051] FIG. 2 shows a block diagram of some components of the mobile phone **140**. The phone **140** may comprise a computer readable medium **200** and a body **210**. The computer readable medium **200** may be present within the body **210**, or may be detachable from it. The body **210** may be in the form of a plastic substrate, housing, or other structure. The computer readable medium **200** may be a memory that stores data and may be in any suitable form including a magnetic stripe, a memory chip, etc.

[0052] The computer readable medium **200** may comprise code for performing any of the functions described herein. For example, the computer readable medium **200** may comprise code for identifying a consumer at an access device. The computer readable medium **200** may also comprise code for communicating with an access device to identify offers corresponding to items scanned by the phone **140**.

[0053] The phone **140** may further include a contactless element **220**, which is typically implemented in the form of a semiconductor chip (or other data storage element) with an associated wireless transfer (e.g., data transmission) element, such as an antenna. Data or control instructions transmitted via a cellular network may be applied to the contactless element **220** by a contactless element interface (not shown). The contactless element interface functions to permit the exchange of data and/or control instructions between the mobile device circuitry (and hence the cellular network) and the contactless element **220**.

[0054] The contactless element **220** is capable of transferring and receiving data using a near field communications ("NFC") capability (or near field communications medium) typically in accordance with a standardized protocol or data transfer mechanism (e.g., ISO 14443/NFC). Near field communications capability is a short-range communications capability, such as RFID, Bluetooth™, infra-red, or other data transfer capability that can be used to exchange data between the phone **140** and the payment processing network **160** or it can be used to exchange data between the phone **140** and the access device **102**. Thus, the phone **140** is capable of communicating and transferring data and/or control instructions via both cellular network and near field communications capability.

[0055] The phone **140** may also include a processor **230** (e.g., a microprocessor) for processing the functions of the phone **140** and a display **240** to allow the consumer to view offers associated with items that may be purchased and other information and messages. The phone **140** may further include input elements **250** to allow a user to input information into the phone **140**, a speaker **260** to allow the user to hear voice communication, music, etc., and a microphone **270** to allow the user to transmit her voice through the phone **140**. The phone **140** may also include an antenna **280** for wireless data transfer (e.g., data transmission).

[0056] FIG. 3 shows an exemplary block diagram of some elements that may be present in the computer server **165** according to an embodiment of the invention. The subsystems shown in FIG. 3 are interconnected via a system bus **300**. Additional subsystems such as a printer **310**, a keyboard **320**, a fixed disk **330**, a monitor **340**, which is coupled to a display adapter **350**, and others are shown. Peripherals and input/output (I/O) devices, which couple to an I/O controller **360**, can

be connected to the computer system by any number of means known in the art, such as a serial port **370**. For example, the serial port **370** or an external interface **380** can be used to connect the computer apparatus to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via the system bus **300** allows a central processor **390** to communicate with each subsystem and to control the execution of instructions from a system memory **395** or the fixed disk **330**, as well as the exchange of information between subsystems. The system memory **395** and/or the fixed disk **330** may embody a computer readable medium.

[0057] FIG. 4 shows an exemplary block diagram of some elements that may be present in the access device **102** according to an embodiment of the invention. The access device **102** may comprise a processor **400**, a computer readable medium **410**, a network interface **420**, an output device **430**, a reader **440**, and a keypad **450** operatively coupled to the processor **400**.

[0058] The processor **400** may be embodied by one or more microprocessors, and the computer readable medium **410** may use any suitable electrical, magnetic or optical means of data storage. The computer readable medium **410** may store computer code for performing the functions of the access device **102**. For example, the computer readable medium **410** may store instructions or code for communicating with the issuer of the consumer's portable consumer device, the payment processing organization associated with the consumer's portable consumer device, the merchant selling the item to be purchased, and the manufacturer of the item, during the transaction, or even before the transaction, after it receives a consumer identifier such as a payment card account number.

[0059] The network interface **420** may be any suitable interface that will allow the access device **102** to communicate with external apparatuses. The network interface **420** allows the access device **102** to communicate with the acquirer **110** and the payment processing network **160**.

[0060] The reader **440** may include any suitable contact or contactless mode of operation. For example, exemplary card readers can include RF (radio frequency) antennas, magnetic stripe readers, etc. to interact with the portable consumer device **130** such as a credit card or a debit card. The reader **440** may be used to enter bill information into the access device **102**.

[0061] The keypad **450** may be an ordinary keypad that is associated with a point of sale terminal. The keypad **450** may be embodied by a number of depressible buttons, or could be embodied on a touch screen on a display. The keypad **450** may be used to enter bill information into the access device **102**.

[0062] FIG. 5 shows a flow diagram of a method for providing offers to a consumer in accordance with embodiments of the invention. The offers may be provided by any entity that seeks to provide an incentive to consumers to purchase a product or service, to shop at a particular time, to use a particular form of payment, or to otherwise influence consumer behavior. Each offer is associated with one or more different rules that establish conditions to be satisfied for the offer to be valid.

[0063] Offers may be associated with an issuer. The acquirer may also generate offers. The merchant may generate offers to provide to the consumer. Offers may also be provided to the merchant from other external sources such as a product manufacturer or a service provider such as a payment processing organization. The provider of the offer determines which rules apply to the offer. In one embodiment, the merchant determines which offers to provide to consumers and which offers to decline. For example, if an external source and the merchant provide an offer for the same item, the merchant may decline to validate the external source offer in order to promote its own offer for that item.

[0064] The consumer shops for goods at a retail outlet. The goods are scanned by the consumer or a cashier at a point of sale terminal (e.g., cash register or self-service checkout terminal) (step **500**). Information corresponding to items to be purchased are entered via a bar code reader or by keying in the item information directly into a cash register.

[0065] The consumer is identified at the point of sale terminal using an access device or a mobile phone (step **510**). For example, the consumer may identify himself using a consumer identifier (e.g., a mobile phone unique identifier or an account number associated with a payment card). The consumer identifier may also be directly entered at the point of sale terminal as, for example, a personal identification number.

[0066] The consumer may provide offers to the access device (step **520**). The offers may be paper coupons, electronic coupons stored on the mobile device, or any other type of offer that may be provided at the merchant.

[0067] The offers are then validated based on rules associated with the offers (step **530**). The offers are validated by accessing a rules engine associated with the entity which provides the offer to ensure that the conditions established by the rules are satisfied. In accordance with one type of offer, a determination may be made whether the credit card provided to identify the consumer corresponds to the credit card applicable to the offer. If the credit cards do not correspond, the offer is not validated. Thus, the consumer cannot take advantage of the incentive associated with the offer. In another example, a rule may be established to provide an offer for a particular consumer. After the rule is retrieved from the rules engine of the entity which provides the offer, a determination is made whether the consumer corresponds to the target consumer of the offer. Illustratively, an offer may only be valid for a consumer living within a particular geographic location. Thus, the offer cannot be validated until the consumer's current resident address is verified.

[0068] In one embodiment, the consumer identifier such as a payment card account number is used to validate offers associated with the consumer. For example, the access device may receive a consumer identifier such as a payment card account number, and may communicate with the issuer associated with the payment card account number. Information regarding the consumer's identity may then be sent from the issuer to the access device. The access device may identify the consumer as being over the age of sixty-five. Thus, any offers associated with senior citizens would be validated.

[0069] After the offers are validated (or invalidated), the valid offers are presented to the consumer (step **540**). The applicable offers may be provided to the consumer by, for example, the access device or the mobile phone. In accordance with one type of offer, the access device or the mobile phone may display the offers that are applicable to the consumer and the goods selected for purchase. In accordance with another type of offer, as shown in FIG. 6, the output device **430** of the access device **102** displays one amount if a payment card associated with a particular payment processing organization (e.g., Payment Processing Organization

Petitioner Exhibit 1002-0613

Z) is used, another amount if a payment card by a particular issuer is used (e.g., Issuer A), another amount if a particular payment card by a particular issuer and by a particular payment processing organization is used, and still another amount if payment is made by cash or check. The consumer may then select a particular form of payment to accept the offer (e.g., pay using a card that is branded with Issuer A and Payment Processing Organization Z) or may select to decline the offer (e.g., pay by cash).

[0070] The consumer selects the valid offers to accept and pays for the goods (step **550**). For example, using a touch screen on the access device, the consumer may select an offer corresponding to the payment card used to identify the consumer to accept the discounted amount that would apply when payment is made using that payment card. In another example, the consumer may select a coupon for a discount on goods or services associated with a purchased item.

[0071] The valid offers are remitted by requesting payment associated with the incentive from the entity which provided the offer (step **560**). For example, if the offer was provided by an issuer, the merchant may request and retrieve the amount corresponding to the offer (e.g., the discounted amount) from that issuer. In one embodiment, offer remittance occurs at the end of the day during the clearing and settlement process.

[0072] As can be seen from the above description, embodiments of the invention have a number of advantages. For example, multiple entities may provide coupon offers to a consumer. The coupon offers provide incentives to influence consumer behavior in such a way that benefits the offer provider. The offers may be established to provide non-traditional incentives. Such offers may be issuer coupons, acquirer coupons, merchant coupons, or coupons from other external sources (e.g., a manufacturer of goods that the merchant offers for sale, other retailers located in the vicinity of the merchant). The provider of the offer associates the offer with certain rules that establish conditions to be fulfilled for the offer to be valid. An access device is configured to provide or redeem the offer coupons only if the rules are satisfied.

[0073] It should be understood that the present invention as described above can be implemented in the form of control logic using computer software in a

Petitioner Exhibit 1002-0614

modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement the present invention using hardware and a combination of hardware and software.

[0074] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0075] The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0076] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0077] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving a consumer identifier and an offer during a transaction

receiving a validated offer from an entity which provides the offer, wherein the offer is validated when rules associated with the offer are satisfied, the offer being validated based on the consumer identifier, wherein the entity is a payment processing organization or an issuer; and

receiving a selection of the valid offer to complete the transaction.

2. The method of claim 1, wherein receiving the consumer identifier and receiving the selection of the valid offer are performed by a point of sale terminal, and wherein the transaction is a payment transaction.

3. The method of claim 1, wherein receiving the validated offer is performed by a point of sale terminal or a computer in communication with the point of sale terminal, and wherein the point of sale terminal or computer is configured to communicate with at least two of a merchant, the issuer, and the payment processing organization to determine if offers provided by the merchant, the issuer, and the payment processing organization are valid.

4. The method of claim 1, further comprising receiving a product identifier, wherein the product identifier is associated with a product that a consumer has purchased using a portable consumer device, and wherein the offer relates to the product.

5. The method of claim 1, wherein the offer is associated with a consumer.

6. The method of claim 1, wherein the consumer identifier is an identifier associated with a portable consumer device.

7. The method of claim 6, wherein the portable consumer device is a payment card.

8. The method of claim 1, wherein the consumer identifier is an account number associated with a portable consumer device associated with a consumer.

9. The method of claim 1, wherein the portable consumer device is a wireless phone.

10. A computer readable medium comprising:

code for receiving a consumer identifier and an offer during a transaction;

code for receiving a validated offer from an entity which provides the offer, wherein the offer is validated when rules associated with the offer are satisfied, the offer being validated based on the consumer identifier, wherein the entiry is a payment processing organization or an issuer; and

code for receiving a selection of the valid offer to complete the transaction.

11. The computer readable medium of claim 10, further comprising code for receiving a product identifier, wherein the product identifier is associated with a product that a consumer has purchased using the portable consumer device, wherein the offer relates to the product.

12. An access device comprising the computer readable medium of claim 10.

13. A server computer comprising the computer readable medium of claim 10.

14. A method comprising:

receiving an offer and a consumer identifier for a consumer during a transaction;

receiving a validated offer, wherein the offer is validated by an entity which provides the offer when rules associated with the offer are satisfied, the offer being validated based on the consumer identifier; and

receiving a selection of the validated offer to complete the transaction.

15. The method of claim 14, wherein receiving the offer, receiving the validated offer, and receiving the selection are performed by a point of sale terminal, wherein the point of sale terminal or a computer in communication with the point of sale terminal is configured to communicate with at least two of a merchant, an issuer, and a payment processing organization to determine if offers provided by the merchant, the issuer, and the payment processing organization are valid.

16. The method of claim 15 wherein the offer relates to a product identifier of a product to be purchased by the consumer.

17. A computer readable medium comprising:

code for receiving an offer and a consumer identifier for a consumer during a transaction;

code for receiving a validated offer, wherein the offer is validated by an entity which provides the offer when rules associated with the offer are satisfied, the offer being validated based on the consumer identifier; and

code for receiving a selection of the validated offer to complete the transaction.

18. An access device comprising the computer readable medium of claim 17.

19. A system comprising:

an access device;

a server computer in communication with the access device,

wherein the access device or the server computer is configured to:

receive a consumer identifier and an offer during a transaction conducted with the access device and the server computer;

receive a validated offer from an entity which provides the offer, wherein the offer is validated when rules associated with the offer are satisfied, the offer being validated based on the consumer identifier, wherein the entity is a payment processing organization or an issuer; and

receive a selection of the valid offer to complete the transaction.

20. The system of claim 19 wherein the transaction is a payment transaction.

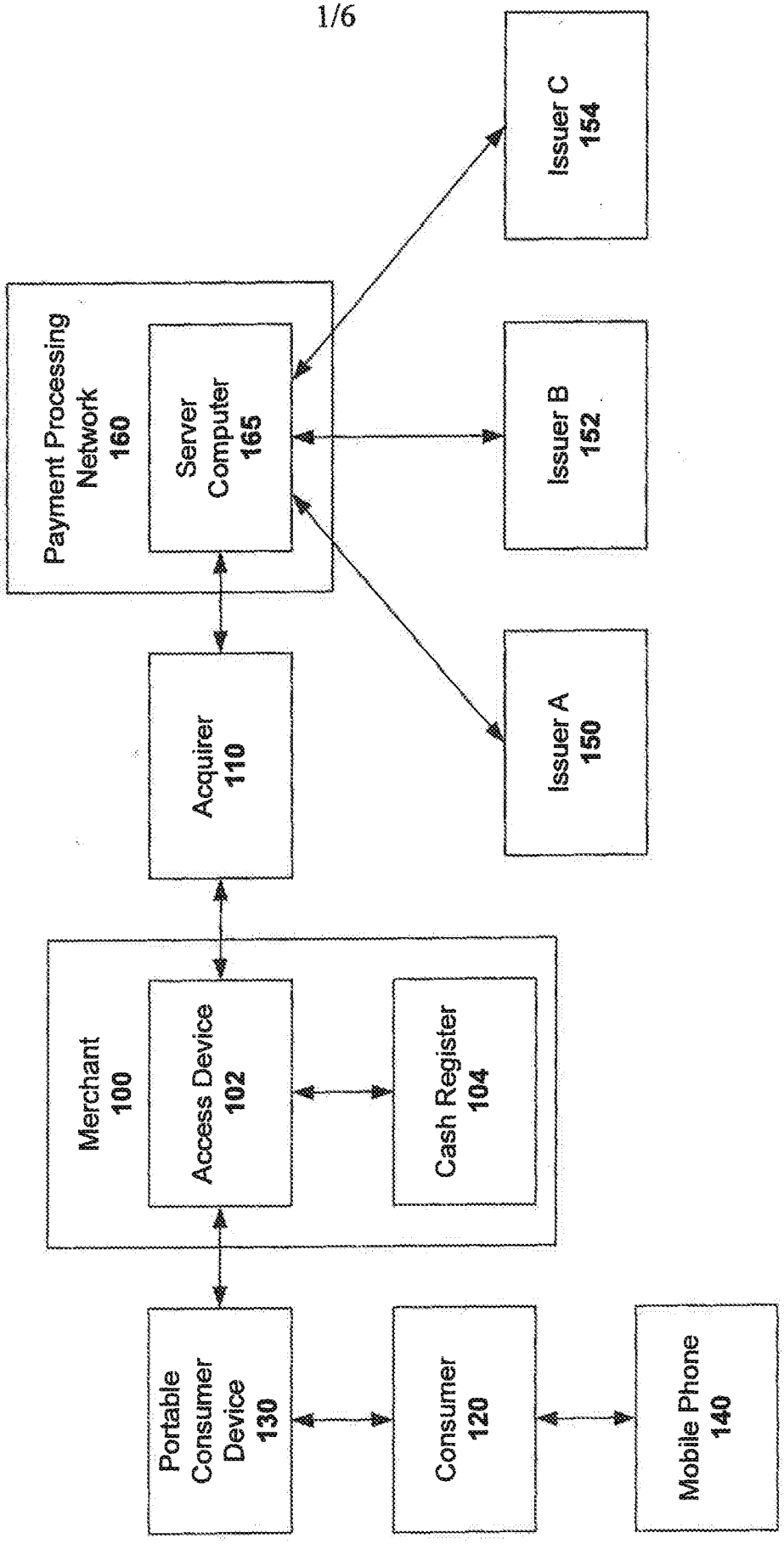

Payment Processing Network 160
Server Computer 165
Issuer C 154
Issuer B 152
Issuer A 150
Acquirer 110
Merchant 100
Access Device 102
Cash Register 104
Portable Consumer Device 130
Consumer 120
Mobile Phone 140

FIG. 1

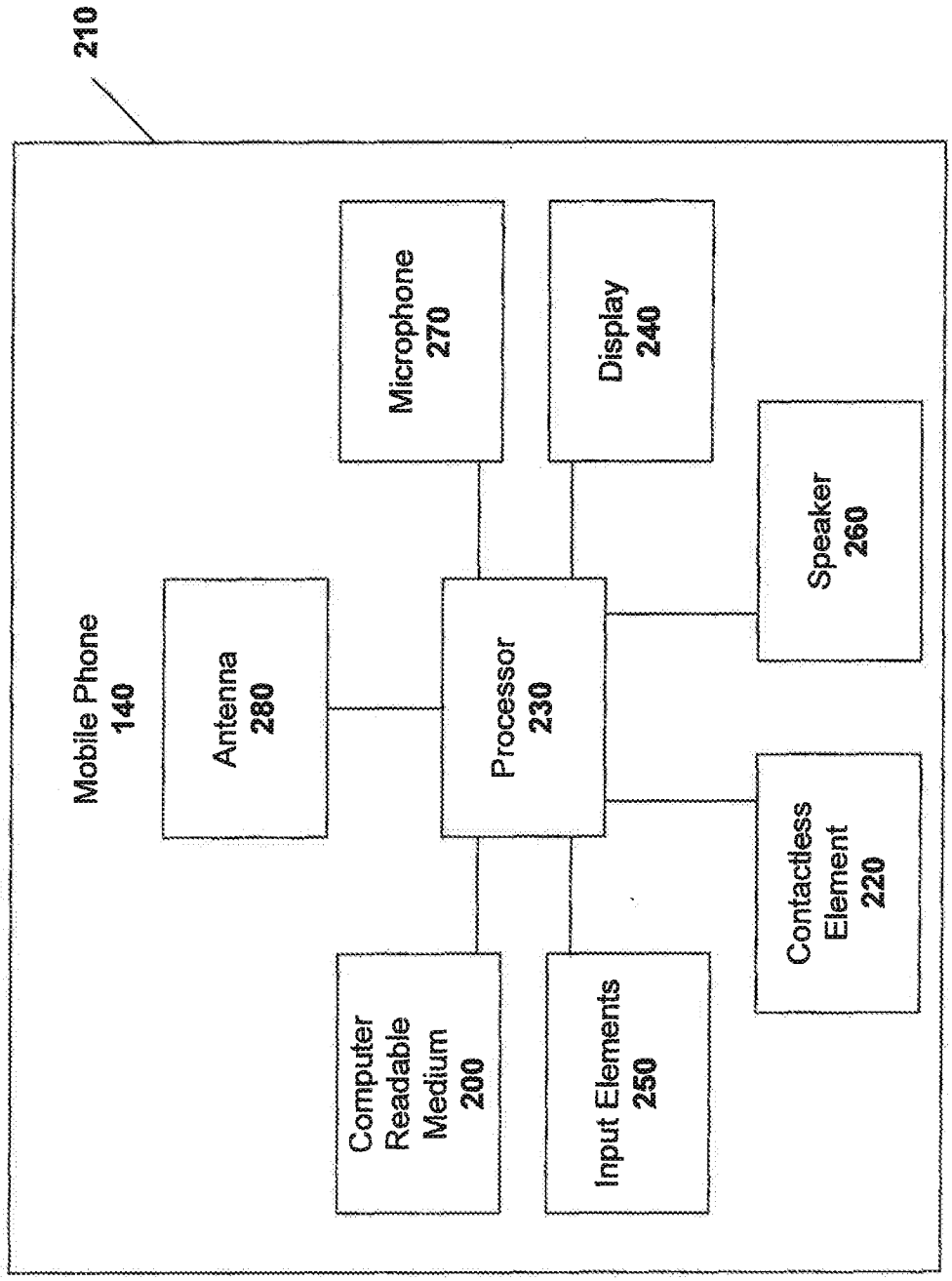

210
Mobile Phone
140
Antenna
280
Processor
230
Microphone
270
Display
240
Speaker
260
Contactless
Element
220
Computer
Readable
Medium
200
Input Elements
250

FIG. 2

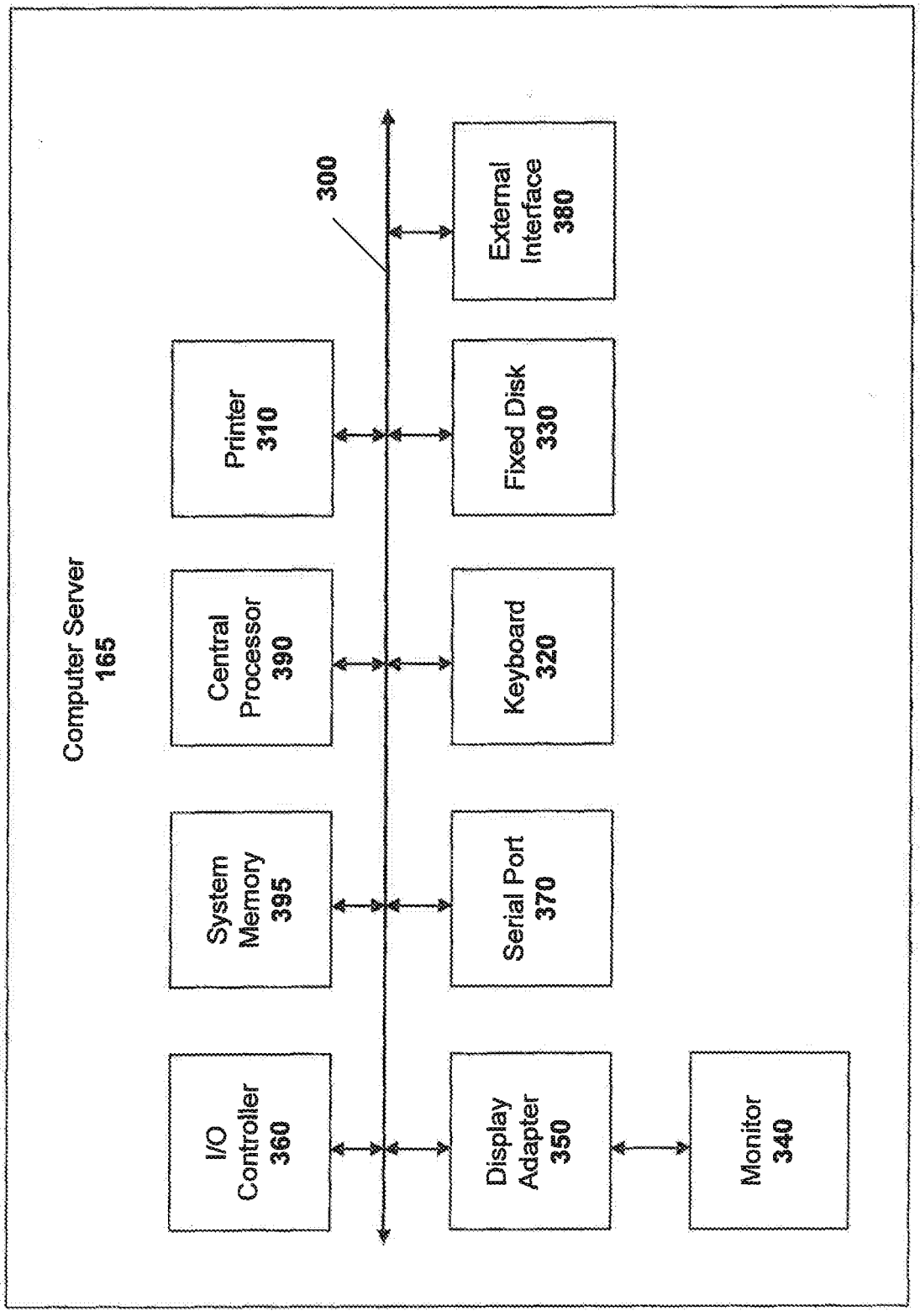

Computer Server
165
300
Printer
310
Central
Processor
390
System
Memory
395
I/O
Controller
360
Display
Adapter
350
Monitor
340
Serial Port
370
Keyboard
320
Fixed Disk
330
External
Interface
380

FIG. 3

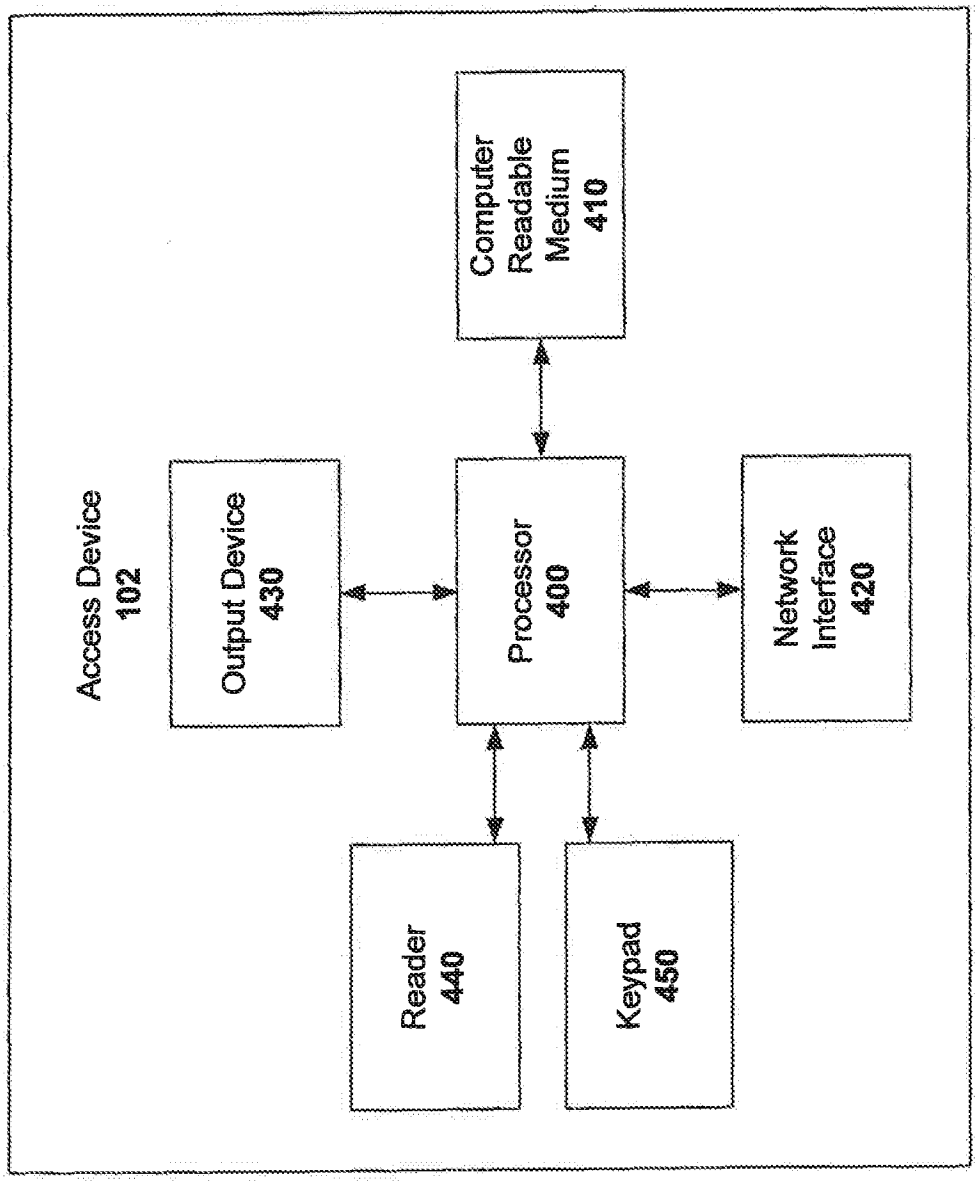

Access Device
102
Output Device
430
Computer
Readable
Medium
410
Processor
400
Network
Interface
420
Reader
440
Keypad
450

FIG. 4

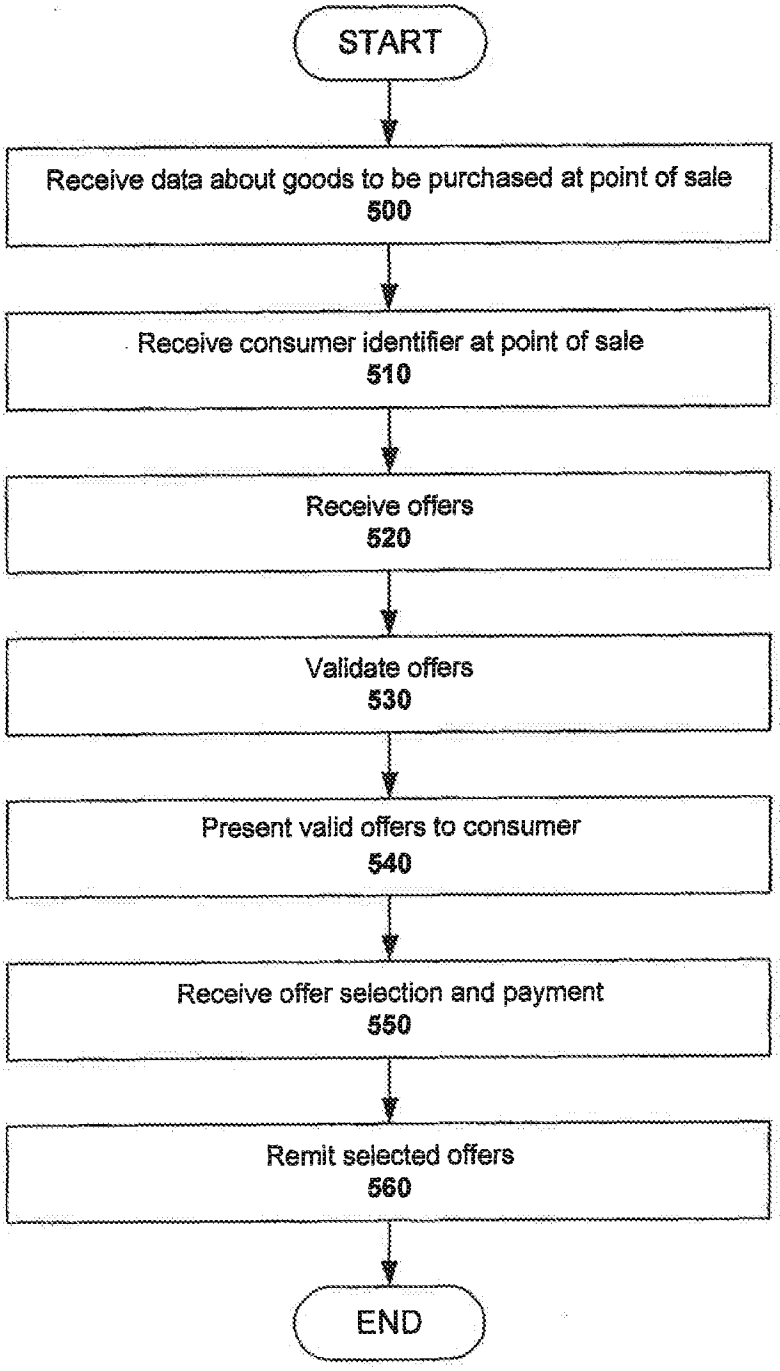

START
Receive data about goods to be purchased at point of sale
500
Receive consumer identifier at point of sale
510
Receive offers
520
Validate offers
530
Present valid offers to consumer
540
Receive offer selection and payment
550
Remit selected offers
560
END

FIG. 5

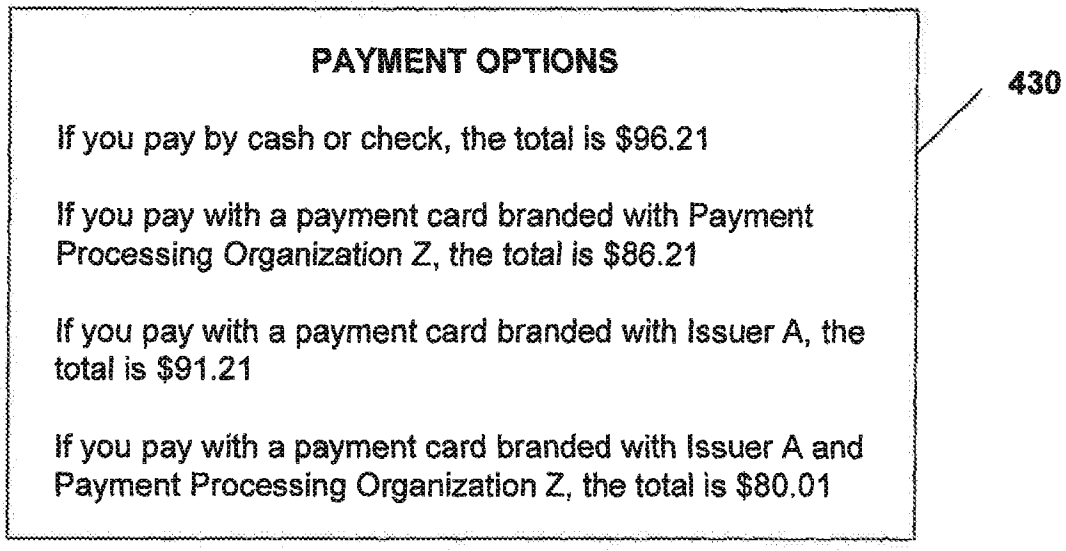

PAYMENT OPTIONS
If you pay by cash or check, the total is $96.21
If you pay with a payment card branded with Payment Processing Organization Z, the total is $86.21
If you pay with a payment card branded with Issuer A, the total is $91.21
If you pay with a payment card branded with Issuer A and Payment Processing Organization Z, the total is $80.01
430

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2007/088815

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 40/00(2006.01)
USPC - 705/41
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - G06F 17/60 (2008.04)
USPC - 705/41

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/0169719 A1 (DIVELY et al) 14 November 2002 (14.11.2002) entire document	1-20
A	US 2003/208406 A1 (OKAMOTO et al) 06 November 2003 (06.11.2003) entire document	1-20
A	US 6,594,376 B2 (HOFFMAN et al) 15 July 2003 (15.07.2003) entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 May 2008	10 JUN 2008
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (April 2005)

Petitioner Exhibit 1002-0626

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 July 2008 (10.07.2008)

PCT

(10) International Publication Number
WO 2008/083105 A2

(51) International Patent Classification:
G06Q 30/00 (2006.01) *G01S 5/00* (2006.01)

(21) International Application Number:
PCT/US2007/088659

(22) International Filing Date:
21 December 2007 (21.12.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/871,898 26 December 2006 (26.12.2006) US
11/960,162 19 December 2007 (19.12.2007) US

(71) Applicants *(for all designated States except US)*: **VISA U.S.A. INC.** [US/US]; P.O. Box 8999, M3-2B, San Francisco, California 94128 (US). **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; 900 Metro Center Boulevard, Foster City, California 94404 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **CARLSON, Mark** [US/US]; 153 Miramontes Avenue, Half Moon Bay, California 94109 (US). **CIUREA, Peter** [US/US]; 6352 Greenridge Court, Martinez, California 94553 (US).

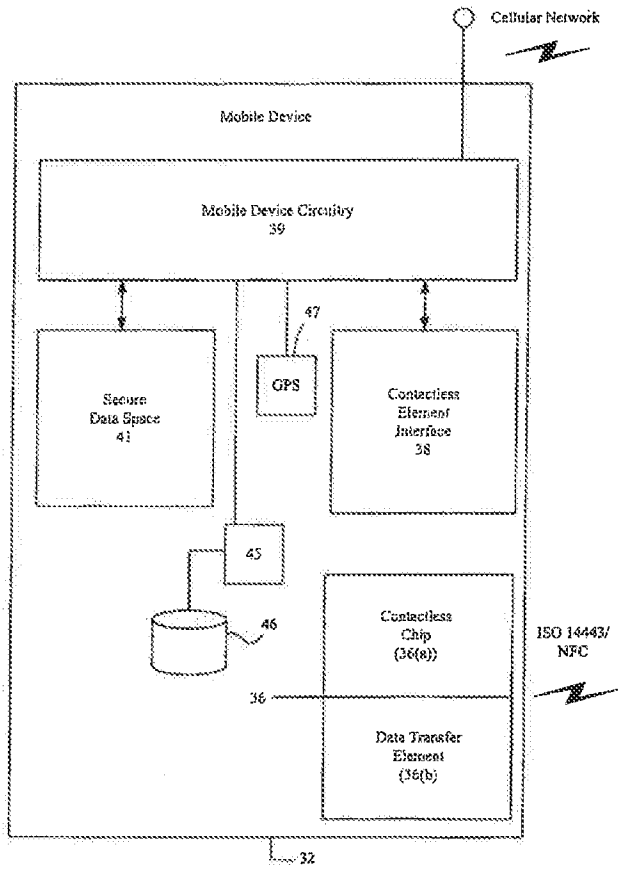
(74) Agents: **TOBIN, Kent J.** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, Eighth Floor, San Francisco, California 94111-3834 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Continued on next page]

(54) Title: MOBILE COUPON METHOD AND PORTABLE CONSUMER DEVICE FOR UTILIZING SAME



(57) Abstract: Embodiments of the present invention relate to systems and methods involving mobile coupons. In one embodiment, an indication of a prior purchase transaction over a payment processing network, serves as a trigger to generate and disseminate a mobile coupon for a subsequent transaction. By generating and promulgating the coupon within a limited time of the first transaction, the recipient is disposed to be receptive based upon his or her current shopping status and also possibly geographic location. According to another embodiment, information from a mobile coupon may be presented from the consumer to a merchant in a contactless manner, utilizing an antenna of a portable device operated by a consumer. Coupon information may be communicated to the merchant with the payment information, or prior to or subsequent to transmission of the payment information to the merchant.

WO 2008/083105 A2

Petitioner Exhibit 1002-0627

European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

MOBILE COUPON METHOD AND PORTABLE CONSUMER DEVICE FOR UTILIZING SAME

CROSS-REFERENCE TO RELATED APPLICATION

[0001] The instant nonprovisional patent application claims priority to U.S. Provisional Patent Application No. 60/871,898, filed December 26, 2006 and incorporated by reference in its entirety herein for all purposes.

BACKGROUND

[0002] Coupons are a useful marketing tool to enhance brand loyalty and introduce new products. By allowing customization of the effective duration and value of an offer, a coupon provides a flexible incentive for a consumer to purchase a particular product or line of products.

[0003] Conventionally, coupons have been available in printed form from sources such as newspapers. Increased adoption of electronic sources of information such as the world-wide-web, however, has led to the increase in popularity of electronic coupons.

[0004] In addition, most consumers now own and operate a cell phone or other portable electronic device. This renders such consumers accessible to the distribution of electronic coupons as they do their shopping, and moreover allows such distributed electronic coupons to be redeemed directly at the store location.

[0005] Accordingly, there is a need in the art for methods and systems allowing for the distribution and use of electronic coupons by mobile electronic devices.

BRIEF SUMMARY

[0006] Embodiments of the present invention relate to systems and methods involving mobile coupons. In one embodiment, indication of a prior purchase transaction over a payment processing network, may serve as a trigger to generate and disseminate a mobile coupon for a subsequent transaction. By generating and promulgating the coupon within a limited time of the first transaction, the recipient is disposed to be receptive based upon his or her current shopping status and also possibly geographic location. According to another embodiment, information from a

Petitioner Exhibit 1002-0629

mobile coupon may be presented to a merchant in a contactless manner, utilizing an antenna of a portable device operated by a consumer. Such mobile coupon information may be communicated to the merchant in a contactless manner with payment information, or may be communicated prior to or subsequent to transmission of payment information to the merchant.

[0007] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] FIG. 1 shows a simplified block diagram of a payment processing system.

[0009] FIG. 1A shows a block diagram of a portable consumer device for use with the payment processing system of FIG. 1.

[0010] FIG. 2 shows a simplified block diagram of an embodiment of a system for implementing a mobile coupon program in accordance with an embodiment of the present invention.

[0011] FIG. 3 shows a simplified flow diagram of a process for enrolling in a mobile coupon program according to an embodiment of the present invention.

[0012] FIG. 4 shows a screen from a POS terminal.

[0013] FIGS. 5(a)-5(c) show different screenshots on a phone. The screenshots include coupons.

[0014] Figure 6 is a schematic illustration of a computer system for use in accordance with embodiments of the present invention.

[0015] Figure 6A is an illustration of basic subsystems the computer system of Figure 6.

[0016] Figure 7 shows a simplified flow of a process of utilizing an embodiment of an electronic coupon according to the present invention.

DETAILED DESCRIPTION

[0017] I. Payment Processing Systems

[0018] Embodiments of the invention are directed to the use of portable consumer devices, and methods and systems employing them. Preferred portable consumer

Petitioner Exhibit 1002-0630

devices are mobile phones. The mobile phones can be used in payment processing systems like those shown in FIG. 1.

[0019] FIG. 1 shows a system 20 that can be used in an embodiment of the invention. The system 20 includes a merchant 22 and an acquirer 24 associated with the merchant 22. In a typical payment transaction, a consumer 30 may purchase goods or services at the merchant 22 using a portable consumer device 32. The acquirer 24 can communicate with an issuer 28 via a payment processing system 26.

[0020] The acquirer 24 is typically a bank that has a merchant account. The issuer 28 may also be a bank, but could also be business entity such as a retail store. Some entities are both acquirers and issuers, and embodiments of the invention include such entities. The issuer 28 may operate a server computer 21, which may have a computer readable medium comprising code for performing the functions that the issuer 28 performs. A database 23 comprising account number information and other information may be operatively coupled to the server computer 21.

[0021] The consumer 30 may be an individual, or an organization such as a business that is capable of purchasing goods or services.

[0022] The portable consumer device 32 may be in any suitable form. For example, suitable portable consumer devices can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). They may include smart cards, ordinary credit or debit cards (with a magnetic strip and without a microprocessor), keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. Other examples of portable consumer devices include cellular phones, personal digital assistants (PDAs), pagers, payment cards, security cards, access cards, smart media, transponders, and the like. The portable consumer devices can also be debit devices (*e.g.*, a debit card), credit devices (*e.g.*, a credit card), or stored value devices (*e.g.*, a stored value card).

[0023] The portable consumer device 32 may comprise a computer readable medium 32(a) and a body 32(b). The computer readable medium 32(a) may be on the body 32(b). The body 32(b) may in the form a plastic substrate, housing, or other structure. The computer readable medium 32(a) may be a memory that stores data and may be in any suitable form. Exemplary computer readable media 32(a)

Petitioner Exhibit 1002-0631

may be in any suitable form including a magnetic stripe, a memory chip, etc. If the portable consumer device 32 is in the form of a card, it may have an embossed region 32(a) which is embossed with a PAN (primary account number).

[0024] Figure 1A shows an enlarged view of the portable (mobile) device. Device 32 further includes a contactless element 36, typically implemented in the form of a semiconductor chip 36(a) (or other data storage element) with an associated wireless data transfer (e.g., data transmission) element 36(b), such as an antenna. Contactless element 36 is associated with (e.g., embedded within) mobile device 32 and data such as a coupon or control instructions transmitted via cellular network may be applied to contactless element 36 by means of contactless element interface 38. Contactless element interface 38 functions to permit the exchange of data and/or control instructions between the mobile device circuitry 39 (and hence the cellular network) and contactless element 36.

[0025] Mobile device 32 may also include a secure data space 41, which may be used by the device to store operating parameters and/or other data utilized in operation of the device. The secure data space 41 may be in the form of a chip that is separate and apart from the chip in the contactless element 36, or alternatively, could be a section of memory in the chip that forms part of the contactless element 36. Note that the chip in the contactless element 36 may include data storage capability in the form of a memory that may be accessed via interface 38 to permit the implementation of read, write, and erase functions, for example.

[0026] In accordance with still other embodiments, the mobile device may further include a processor 45 and computer readable storage medium 46 for storing code and configured to direct the processor to perform various tasks. For example, the computer readable storage medium may comprise a magnetic disk drive or a flash memory chip.

[0027] As discussed below, the computer readable storage medium may contain code that is configured to cause a processor of the portable consumer device to receive and recognize a message including a coupon and code that is delivered to the mobile device. The computer readable storage medium may also include code that is configured to decrypt an encrypted message including the code that is received by the mobile device.

[0028] Contactless element 36 is capable of transferring and receiving data using a near field communications capability (or near field communications medium) typically in accordance with a standardized protocol or data transfer mechanism (identified as ISO 14443/NFC in the figure). Near field communications capability is a short-range communications capability, such as RFID, Bluetooth™, infra-red, or other data transfer capability that can be used to exchange data between the mobile device 32 and a local apparatus, for example located a point-of-sale of a merchant or another location at which coupons are expected to be redeemed. Thus, mobile device 32 is capable of communicating and transferring data and/or control instructions via both cellular network and near field communications capability.

[0029] In accordance with certain embodiments, the mobile device further includes a Global Positioning System (GPS) element 47. GPS element 47 is configured to allow determination of the location of the user at any time. In particular, GPS element 47 relies upon signals from a plurality of orbiting satellites in order to allow the user's location to be determined. Location information obtained from the GPS element 47 may in turn be communicated through the antenna to allow monitoring of the user's position.

[0030] Returning to Figure 1, the payment processing network 26 may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network may include VisaNet™. Payment processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services.

[0031] The payment processing network 26 may include a server computer. A server computer is typically a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The payment processing network 26 may use any suitable wired or wireless network, including the Internet.

[0032] The merchant 22 may also have, or may receive communications from, an access device 34 that can interact with the portable consumer device 32. In embodiment of a system of FIG. 1, the access device 34 is located at the merchant 22. However, it could be located at any other suitable location in other embodiments of the invention.

[0033] The access devices according to embodiments of the invention can be in any suitable form. Examples of access devices include point of sale (POS) devices, cellular phones, PDAs, personal computers (PCs), tablet PCs, handheld specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, and the like.

[0034] If the access device 34 is a point of sale terminal, any suitable point of sale terminal may include a reader 34(a), a processor 34(b) and a computer readable medium 34(c). The reader 34(b) may include any suitable contact or contactless mode of operation. For example, exemplary card readers can include RF (radio frequency) antennas, magnetic stripe readers, etc. to interact with the portable consumer device 32.

[0035] In a typical purchase transaction, the consumer 30 purchases a good or service at the merchant 22 using a portable consumer device 32 such as a credit card. The consumer's portable consumer device 32 can interact with an access device 34 such as a POS (point of sale) terminal at the merchant 22. For example, the consumer 30 may take a credit card and may swipe it through an appropriate slot in the POS terminal.

[0036] Alternatively, the POS terminal may be a contactless reader, and the portable consumer device 32 may be a contactless device such as a contactless card. In certain embodiments, the portable consumer device may be a mobile device such as shown in FIG. 1A above. As described in detail below, the antenna of the mobile device may be utilized to communicate not only payment information to the POS, but also may also communicate information (such as a code) from a mobile coupon to a POS device.

[0037] An authorization request message is then forwarded to the acquirer 24. After receiving the authorization request message, the authorization request

Petitioner Exhibit 1002-0634

message is then sent to the payment processing network 26. The payment processing network 26 then forwards the authorization request message to the issuer 28 of the portable consumer device 32.

[0038] After the issuer 28 receives the authorization request message, the issuer 28 sends an authorization response message back to the payment processing network 26 to indicate whether or not the current transaction is authorized (or not authorized). The transaction processing network 26 then forwards the authorization response message back to the acquirer 24. The acquirer 24 then sends the response message back to the merchant 22.

[0039] After the merchant 22 receives the authorization response message, the access device 34 at the merchant 22 may then provide the authorization response message for the consumer 30. The response message may be displayed by the access device 34, or may be printed out on a receipt.

[0040] At the end of the day, a normal clearing and settlement process can be conducted by the transaction processing network 26. A clearing process is a process of exchanging financial details between and acquirer and an issuer to facilitate posting to a consumer's account and reconciliation of the consumer's settlement position.

[0041] Some of the embodiments described below may use a payment processing system like the one described above, or any suitable combination of components in the payment processing system.

[0042] II. Mobile Coupon Method and System

[0043] Particular embodiments in accordance with the present invention relate to methods and apparatuses which allow distribution and/or redemption of electronic coupons at a mobile personal device. Various embodiments of such a system are described in the following figures.

[0044] Figure 2 shows an overall view of an embodiment of a system in accordance with the present invention for administering a mobile coupon program. A first entity 200 (i.e. Visa) is responsible for operating a payment processing network. Under the control of entity 200 are a number of different operational elements.

[0045] For example, mobile campaign server 202 functions as the interface between entity 200 and the outside world, here represented by the internet "cloud" 204. Mobile campaign server 202 can include at least three components.

[0046] Specifically, mobile enrollment server 206 provides a browser interface for potential users to enroll in the mobile coupon program using an enrollment webpage 208. Mobile enrollment server 206 is configured to receive from potential users certain pieces of information allowing their participation in the program. For example, in an enrollment form supplied electronically to server 206, the prospective participant can provide information such as the telephone number of their portable device, a security password, and preferences regarding the types of mobile coupons that they wish to receive.

[0047] Figure 3 provides a simplified flow chart of the steps for enrolling in a mobile coupon program. In step 302 of enrollment flow 300, a consumer navigates to the website of the enrollment server utilizing his or her browser.

[0048] In the next step 304, the consumer creates a mobile coupon account by inputting identification and validation information. Examples of such identification information include the user's name, the telephone number of the user's mobile electronic device, financial account numbers, and optional aliases. At this stage, the consumer also verifies that they have read appropriate disclaimers and affirmatively indicate that they seek to opt-into the mobile coupon program.

[0049] In step 306 of enrollment flow 300, information entered by the consumer is verified. Examples of such verification include confirming that the consumer identified is actually in possession of the portable device, that the portable device belongs to the consumer, and that any identified account belongs to the consumer.

[0050] Returning to FIG. 2, mobile enrollment server 206 is in turn in electronic communication with user database 210. Database 210 includes data relating to the user of the mobile coupon system, including the specific information provided during enrollment. Access to the contents of database 210 is shared with gateway server 212.

[0051] Gateway server 212 serves as the interface with outside entities responsible for implementing the mobile coupon program. For example, telecommunications

companies ("telecoms") 214 provide the infrastructure necessary to communicate the coupon to the user's mobile device wherever they happen to be. The telecom entities must provide sufficient capacity to handle a sufficiently high volume of coupon messages outgoing to recipients.

[0052] Where such volume of messages is expected to be small (for example at the inception of the mobile coupon program), another type of company called an aggregator will secure sufficient bandwidth for all of the expected messages from the telecom, and then aggregate the messages from different sources.

[0053] In an exemplary embodiment, a coupon is sent to a user's phone or other portable device. The coupon may be sent in any one of a number of different forms, including but not limited to an short messaging service (SMS) message, a SMS link, a multimedia messaging service (MMS) message, or e-mail message.

[0054] The coupon may be communicated utilizing any one of several types of communications systems. For example, the coupon may be communicated to the cell phone utilizing SMS. Such an embodiment offers a number of possible advantages, including broad access as SMS is available on almost every cell phone. Possible disadvantages to mobile coupon distribution utilizing SMS is a weak mechanism for confirming receipt of the coupon by the designated recipient, and also a high transaction cost as charges are typically incurred for each SMS message transmitted.

[0055] In accordance with alternative embodiments, the mobile coupon could be distributed by a Global System for Mobile Communications (GSM) system. Such GSM communication are cheap and secure, and would support confirmation of receipt of the coupon by a designated user.

[0056] Further alternatively, the coupons could be distributed utilizing a Near Field Communications (NFC) system. Such an embodiment would require the portable consumer device to be equipped with an NFC chip and programmed with a software application. The source of the near field signal providing the electronic coupon could be local kiosks, for example as present in a shopping mall. An alternative source of electronic coupons available utilizing such near field communication is the point of sale itself. Other sources are possible.

[0057] The coupon may be communicated to the portable consumer device in encrypted form. Such encryption would prevent interception and unauthorized use of a coupon by other than the intended recipient. A processor present in the portable consumer device could in turn decrypt the message upon its receipt.

[0058] FIG. 4 shows a screen 400 from a POS terminal. The screen 400 shows buttons 402 that a cashier might select in order to initiate a pre-arranged discount utilizing an electronic coupon. For example, button 402a allows the cashier to implement a 30% discount for employees etc. Button 402b allows the cashier to manually enter a number for numeric look-up (NLU) from an electronic coupon displayed on a user's portable electronic device.

[0059] FIGS. 5A-5C are examples of three screenshots showing graphical coupons in different forms. These screenshots are configured to be able to be displayed on the small screen of a mobile phone, personal digital assistant (PDA), or other mobile device.

[0060] FIG. 5A shows a screenshot 500 which includes both a bar code 502 (which is an example of a machine readable code) and a seven digit number 504. The bar code 502 can be scanned with a scanner. One type of scanner which may be used to read a bar code on the screen of a cell phone is a charge coupled device (CCD) scanner. However, a laser-type scanner may not be able to read the bar code displayed due to reflection from the screen.

[0061] In order to process the electronic coupon shown in FIG. 5A, the user accesses and displays the coupon on the screen of his or her portable device. The cashier then accesses the discount screen shown in FIG. 4, and either scans the bar code in directly or enters the seven-digit number utilizing a numeric key pad.

[0062] FIG. 5B illustrates a screenshot 520 showing a different embodiment of a mobile electronic coupon in accordance with the present invention, which includes a visual display 522 and a personalized message 523. This visual display may be related to the nature of the coupon, representing for example the purchase of flowers. Alternatively, the display may simply illustrate the nature of the coupon, for example the display of flowers generically representing a gift.

[0063] Instead of a barcode, a six digit number "024248" is shown by the electronic coupon 520. In processing of coupon 520 by a cashier, this six digit number can be entered into a POS terminal to give the consumer a discount on a purchase. In accordance with one embodiment, the number can be entered by having the cashier type in the individual digits of the code on a numeric keypad. In accordance with an alternative embodiment, the number can be entered by having the cashier activate a predetermined key, or combination thereof, which allows recognition of the coupon and the discount.

[0064] The embodiment of Figure 5B may offer certain advantages over a coupon employing a bar code as shown in Figure 5A. One advantage is ease of operation, as there is no requirement for optical recognition/reading of a code from the screen of the phone. Another possible advantage is reduced cost of implementation, as a bar code scanner device is not required to be purchased or rented by the merchant. In addition, software and hardware upgrades relating to electronic scanning would not be required by this alternative embodiment.

[0065] Lastly, FIG. 5C shows a screenshot 550 showing a "30% off" coupon. This electronic coupon includes a visual display 552 but lacks either a bar code or an identifying number.

[0066] To use this coupon, the user shows the display to the cashier and the cashier selects a button on a POS terminal display (see FIG. 4) to provide the discount to the consumer. According to still further embodiments of the present invention, coupon information such as a code may be communicated to a portable device in a proprietary format.

[0067] Figure 7 shows a simplified flow of a process of utilizing a mobile coupon according to an embodiment of the present invention. In a first step 702 of process flow 700, a purchaser presents items to a cashier. In step 704, the cashier hits the purchase key and enters the items. In step 706, the coupon asks the purchaser whether or not she intends to use coupons. In step 708, the purchaser responds that she intends to use a coupon.

[0068] In step 710 of process flow 700, the cashier hits the coupons key to alert the register to the use of coupons. In step 712, the cashier hits the accept coupon button on the back of the VISA terminal.

Petitioner Exhibit 1002-0639

[0069] In step 714, the VISA terminal displays a message requesting the purchaser to wave the phone to enter a coupon. In step 716, the purchaser waves the phone and the terminal receives the scanned code. In step 718 the processor in communication with the terminal looks up the scanned code. In step 720, the processor returns to the terminal, customer and branding information. In step 722, the terminal displays a branding message customized to the particular purchaser. Finally, in step 724, the terminal sends to the register a numeric look up representing the bar code.

[0070] A variation according to embodiments of the present invention may utilize near field communication of the coupon or a code therein, to the cashier. In this variation, a multi-digit numerical code (i.e. six digits) can be transmitted to the POS terminal via a reader using a contactless device such as the mobile device of FIG. 1A including an antenna. The coupon may be communicated in such a contactless manner using a short range communication method, such as a near field communications (NFC) capability. Examples of such NFC technologies include ISO standard 14443, RFID, Bluetooth™ and Infra-red communications methods. In accordance with such embodiments, the six digit code may or may not be shown on the display of the phone. Embodiments in accordance with the present invention are not limited to communicating coupon code information. In accordance with alternative embodiments, coupon information communicated from a mobile device to a POS terminal may include other information, for example a product code limiting applicability of the mobile coupon to a particular product, or an expiration date/time of the mobile coupon.

[0071] In certain embodiments, payment information (such as a credit card number, debit card number, home zip code of the card holder, or a three digit card verification value code) may be communicated from a mobile device in a contactless manner to the POS terminal. In such embodiments, the coupon information from the mobile device may also be communicated to the POS terminal in a contactless manner. In some embodiments, such communication of mobile coupon information may take place as part of the same message communicating payment information to the POS terminal. Alternatively, the coupon information may be communicated prior to, or following, contactless communication of the payment information to the POS terminal.

Petitioner Exhibit 1002-0640

[0072] The consumer may receive a text message, a phone call, or e-mail indicating that the consumer has received a coupon. The consumer may then use his or her phone to transmit a code corresponding to the coupon, to a contactless reader coupled to a POS terminal. The near field communication can utilize, for example, infrared or an RF communication mode such as Bluetooth. The system shown in FIG. 1 can be used in conjunction with such an embodiment.

[0073] Returning to Figure 2, apart from the mobile campaign server, a number of other elements are also under the control of entity 200. Notification module 250 is responsible for notifying participants in the program of particular events, for example limited time promotions or even the possibility of fraudulent transactions.

[0074] Mobile targeting module 260 is responsible for generating coupons targeted to a user. According to certain embodiments, the coupons can be targeted based upon a location based services (LBS) approach, utilizing prior purchasing activity by a consumer as detected over a payment processing network.

[0075] Specifically, where a payment transaction is conducted over a payment processing network, certain information is communicated that can be used for targeting of a mobile coupon. One piece of information that is potentially useful for targeting is the timing of the prior payment transaction.

[0076] In particular, the very existence of the prior purchase transaction reveals the consumer to be actively engaged in shopping rather than other activities (i.e. sleeping or working). Based upon this timing information, the consumer is known to likely be receptive to a mobile coupon for a subsequent transaction. Accordingly, embodiments of the present invention may thus generate and disseminate a mobile coupon to the consumer within a predetermined, limited time period from receiving an indication from the payment processing network that a prior payment transaction has occurred. Examples of time periods for dissemination of mobile coupons include, but are not limited to, one minute or less, five minutes, ten minutes, fifteen minutes, one-half hour, forty-five minutes, one hour, one and one half hours, two hours, three hours, four hours, and five hours or longer from the time that a prior purchasing activity is detected from the payment processing network. Such an approach allows for dissemination of a timely, non-intrusive mobile coupons to the consumer.

Petitioner Exhibit 1002-0641

[0077] In certain embodiments, the duration of effectiveness of such a mobile coupon can also be limited by time. Such an embodiment would provide an incentive for the recipient to monitor his or her portable device for receipt of a mobile coupon, and use that coupon within the limited period that it is effective. Moreover, in certain embodiments, upon expiration the mobile coupon could be configured to automatically disappear from the consumer's portable device. This would reduce intrusiveness of the mobile coupon, as the consumer is not obligated to delete a backlog of expired coupons from his or her portable device.

[0078] Embodiments of the present invention are not limited to generating and promulgating mobile coupons based upon temporal information gleaned from a prior purchase transaction over a payment processing network. In accordance with alternative embodiments, the mobile coupons can be targeted based upon a geographic location of the user as determined from the payment processing network.

[0079] According to one embodiment, the location of the consumer can be determined from purchasing activity of the user based upon a Location Based Services (LBS) approach. For example, when the user swipes a card at a POS, an authorization message is returned from the payment network which includes a Merchant Identification Number (MID). The user's location at that time of sale can be determined from the MID number.

[0080] According to other embodiments, information regarding the nature of the prior purchase conducted over the payment processing network can be referenced to generate the coupon. Thus, a prior purchase of one product (for example a vacuum cleaner), could lead to generation of a second product (bags for the vacuum cleaner). This coupon generation could be irrespective of the time or physical location of a prior purchasing transaction. Still further alternatively, an LBS approach could be based upon the seller of the second product having an affinity agreement with the seller of the previous product purchased.

[0081] Moreover, a mobile coupon may be generated based upon more than one piece of information gleaned from a prior purchasing transaction conducted over a payment processing network. Specifically, the time, geographic location, and/or nature of the prior purchase transaction could be combined to generate the targeted coupon.

Petitioner Exhibit 1002-0642

[0082] According to still other embodiments, information from a prior purchase transaction available from a payment processing network, may be combined with other information to generate a targeted coupon. For example, information regarding the location of the consumer can be determined from sources other than the payment processing network.

[0083] According to one approach, the location of a consumer can be determined by analyzing the location of the current base station through which the portable user device is transmitting and receiving information. Such current base station information is available from the telecommunications provider with which the consumer is affiliated, and in other applications is utilized to allow the user to contact the closest medical services provider in the case of a medical emergency. Thus, in certain embodiments, geographic information from this source could be combined with information (time, nature of prior purchases) available from the payment processing network, to generate a targeted coupon.

[0084] According to another approach, the location of a consumer can be determined by the use of Global Positioning System (GPS) technology. In this approach, the location of the portable device of the consumer is monitored utilizing a plurality of orbiting satellites. Thus, in other embodiments, geographic information from this source could be combined with information (time, nature of prior purchase) available from the payment processing network, to generate a targeted coupon.

[0085] Utilizing any of these approaches, or others, alone or in combination, the mobile targeting module 260 may send out a targeted mobile coupon to a consumer. For example, the mobile electronic coupon can be targeted in whole or in part based upon the recipient belonging to a particular group, such as an employee of a business or a member of a club.

[0086] Reward module 270 (such as "Visa Extras") is responsible for coordinating and administering an incentive or reward program that is tied to use of the payment network Thus a targeted mobile coupon may be generated and then electronically distributed to a portable consumer device as part of an incentive program. For example, the accrual of a certain volume of purchases utilizing a Visa card, may render the program participant eligible for a particularly valuable type of electronic coupon not typically available to other participants in the mobile coupon program.

This targeted electronic coupon is then communicated to the consumer's mobile device for redemption.

[0087] Other elements indicated under the control of entity 200 in FIG. 2, may relate to the function of the payment network to execute purchase and payment transactions. Partners and banks 280 are outside of the control of entity 200 but interact therewith as part of the processing of payment transactions.

[0088] It should be understood that the present invention as described above can be implemented in the form of control logic using computer software in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement the present invention using hardware and a combination of hardware and software.

[0089] The various components of the mobile coupon system described above may be implemented with a computer system having various features. FIG. 6 shows an example of a generic computer system 610 including display device 620, display screen 630, cabinet 640, keyboard 650, and mouse 670. Mouse 670 and keyboard 650 are representative "user input devices." Mouse 670 includes buttons 680 for selection of buttons on a graphical user interface device. Other examples of user input devices are a touch screen, light pen, track ball, data glove, microphone, and so forth. FIG. 6 is representative of but one type of system for embodying the present invention. It will be readily apparent to one of ordinary skill in the art that many system types and configurations are suitable for use in conjunction with the present invention. In a preferred embodiment, computer system 610 includes a Pentium class based computer, running Windows NT operating system by Microsoft Corporation. However, the apparatus is easily adapted to other operating systems and architectures by those of ordinary skill in the art without departing from the scope of the present invention.

[0090] As noted, mouse 670 can have one or more buttons such as buttons 680. Cabinet 640 houses familiar computer components such as disk drives, a processor, storage device, etc. Storage devices include, but are not limited to, disk drives, magnetic tape, solid state memory, bubble memory, etc. Cabinet 640 can include additional hardware such as input/output (I/O) interface cards for connecting

computer system 610 to external devices external storage, other computers or additional peripherals, further described below.

[0091] FIG. 6A is an illustration of basic subsystems in computer system 610 of FIG. 6. This diagram is merely an illustration and should not limit the scope of the claims herein. One of ordinary skill in the art will recognize other variations, modifications, and alternatives. In certain embodiments, the subsystems are interconnected via a system bus 675. Additional subsystems such as a printer 674, keyboard 678, fixed disk 679, monitor 676, which is coupled to display adapter 682, and others are shown. Peripherals and input/output (I/O) devices, which couple to I/O controller 671, can be connected to the computer system by any number of means known in the art, such as serial port 677. For example, serial port 677 can be used to connect the computer system to a modem 681, which in turn connects to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via system bus allows central processor 673 to communicate with each subsystem and to control the execution of instructions from system memory 672 or the fixed disk 679, as well as the exchange of information between subsystems. Other arrangements of subsystems and interconnections are readily achievable by those of ordinary skill in the art. System memory, and the fixed disk are examples of tangible media for storage of computer programs, other types of tangible media include floppy disks, removable hard disks, optical storage media such as CD-ROMS and bar codes, and semiconductor memories such as flash memory, read-only-memories (ROM), and battery backed memory.

[0092] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0093] The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0094] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0095] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving through a payment processing network, an indication of a purchase transaction by a consumer;

generating a mobile coupon based upon information from the purchase transaction; and

disseminating the mobile coupon to the consumer.

2. The method of claim 1 wherein the mobile coupon is generated based upon a time of the purchase transaction, and the mobile coupon is disseminated to the consumer within a predetermined amount of time from the time of the purchase transaction.

3. The method of claim 2 wherein the mobile coupon is effective for a limited time from the first time.

4. The method of claim 1 wherein the coupon is generated based upon a geographic location of the consumer.

5. The method of claim 4 wherein the geographic location of the consumer is determined from the purchase transaction.

6. The method of claim 4 wherein the geographic location of the consumer is determined from a location of the portable device.

7. The method of claim 6 wherein the geographic location of the consumer is determined from a global positioning system (GPS) element of the portable device.

8. The method of claim 1 wherein the information comprises at least one of a time of the purchase transaction, a geographic location of the purchase transaction, or a product purchased in the purchase transaction.

9. A method comprising:

receiving a coupon comprising a code at a portable consumer device comprising an antenna operated by a consumer;

using the antenna to provide payment information for a purchase transaction to a merchant; and

using the antenna to also provide the code to the merchant.

10. The method of claim 9 wherein the antenna is an RF antenna and the portable consumer device is a mobile phone.

11. The method of claim 9 wherein the payment information comprises a credit card number, a debit card number, a home zip code of the consumer, or a three digit card verification value code.

12. The method of claim 9 wherein the code is provided to the merchant utilizing a near field communication (NFC) channel.

13. The method of claim 9 wherein the portable consumer device includes a global positioning system (GPS), the method further comprising the portable consumer device sending to a remote location a signal indicating its geographic location.

14. A portable consumer device comprising:

a contactless element;

a wireless data transfer element associated with the contactless element;

a processor; and

a computer readable storage medium configured to store a coupon including a code, the contactless element configured to transmit the code to a merchant upon receipt of a command from a user.

15. The portable consumer device of claim 14 wherein the computer readable storage medium is configured to store instructions for the processor to decrypt an encrypted coupon message received by the wireless data transfer element.

16. The portable consumer device of claim 14 wherein the computer readable storage medium is configured to store instructions for the processor to receive and recognize an incoming message including the coupon and the code.

17. The portable consumer device of claim 16 wherein the coupon is received as a short messaging service (SMS) message, a near field communication (NFC) message, or as a global system for mobile communications (GSM) message.

18. The portable consumer device of claim 14 further comprising a global positioning system (GPS) element.

19. The portable consumer device of claim 18 wherein the computer readable storage medium is configured to store instructions for the processor to communicate a geographic location generated by the GPS element to an entity generating the coupon.

20. The portable consumer device of claim 14 further comprising a screen, wherein the computer readable storage medium is configured to store instructions for the processor to display at least a portion of the coupon on the screen.

21. The portable consumer device of claim 14 wherein the wireless data transfer element comprises an infra-red (IR) transmitter or a radio frequency (RF) transmitter.

22. A method comprising:

receiving a coupon comprising a code at a mobile phone operated by a consumer;

displaying the code on a screen of the mobile phone; and

showing the screen including the code to a merchant, thereby allowing the merchant to thereafter provide a discount to the consumer.

23. The method of claim 22 wherein displaying the code comprises displaying a numeric code.

24. The method of claim 22 further comprising providing a visual display with the code on the screen.

25. The method of claim 22 wherein receiving the coupon comprises receiving a short messaging service (SMS) message, a near field communication (NFC) message, or a global system for mobile communications (GSM) message.

26. The method of claim 22 further comprising decrypting the incoming message including the coupon.

27. The method of claim 22 wherein the coupon is generated based upon a of the consumer based upon location-based service (LBS) approach or a global positioning system (GPS) approach.

28. A method comprising:

receiving a coupon comprising a code at a portable consumer device comprising an antenna operated by a consumer; and

providing the code to a merchant using an antenna.

29. The method of claim 28 wherein the antenna is an RF antenna and the portable consumer device is a mobile phone.

30. The method of claim 28 wherein the portable consumer device receives the coupon with the antenna.

31. The method of claim 28 wherein the code is provided to the merchant utilizing a near field communication (NFC) channel.

32. The method of claim 28 wherein the portable consumer device includes a global positioning system (GPS), the method further comprising the portable consumer device sending to a remote location a signal indicating its geographic location.

33. The method of claim 28 wherein the coupon is applicable to a merchant proximate to the geographic location of the portable consumer device.

34. The method of claim 33 wherein the coupon is generated based upon a location of the consumer based upon location-based service (LBS) approach or a global positioning system (GPS) approach.

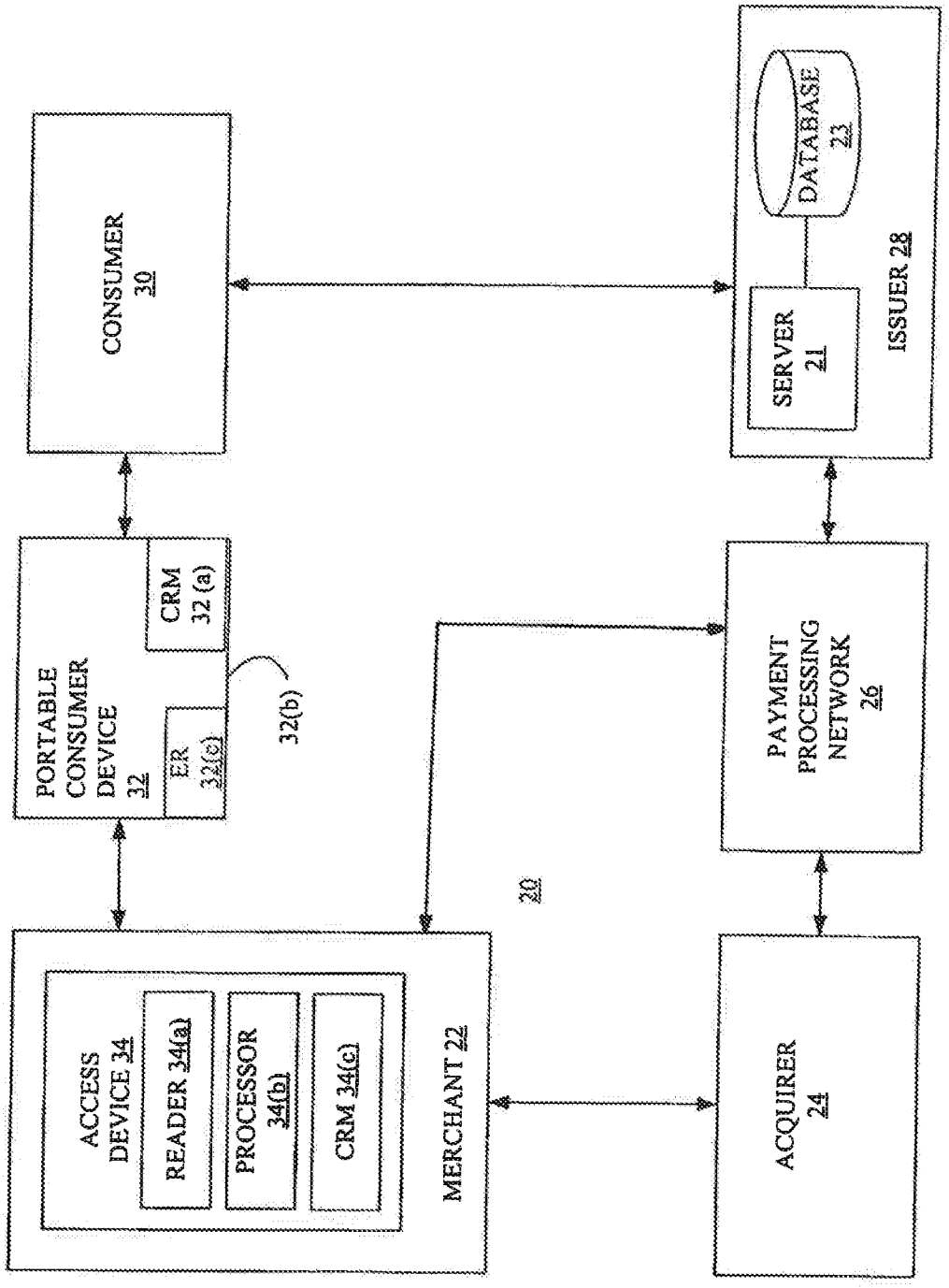

CONSUMER
30
PORTABLE
CONSUMER
DEVICE
32
CRM
32 (a)
ER
32(c)
32(b)
ACCESS
DEVICE 34
READER 34(a)
PROCESSOR
34(b)
CRM 34(c)
MERCHANT 22
20
ACQUIRER
24
PAYMENT
PROCESSING
NETWORK
26
SERVER
21
DATABASE
23
ISSUER 28

FIG. 1

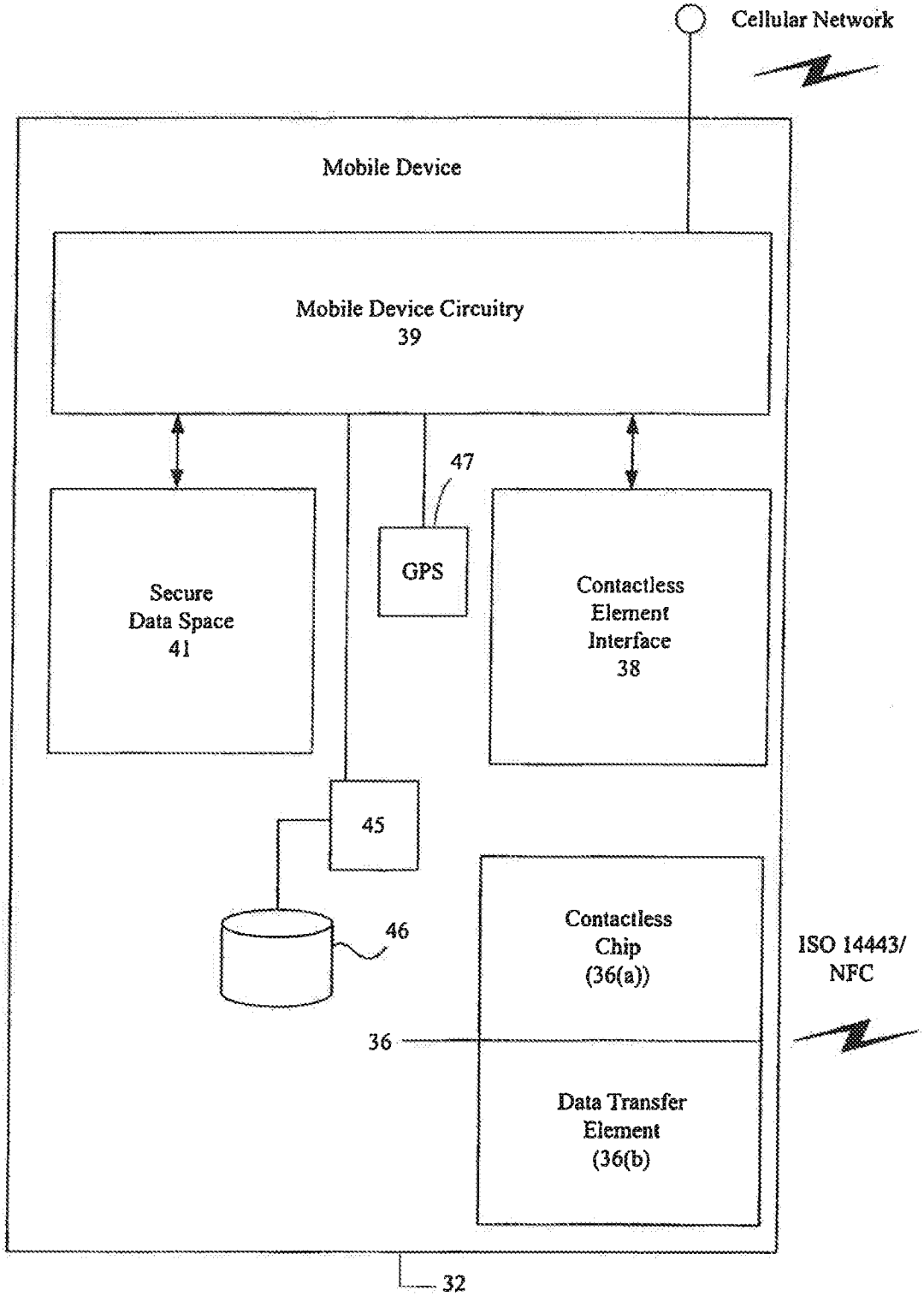

Cellular Network
Mobile Device
Mobile Device Circuitry
39
47
GPS
Secure
Data Space
41
Contactless
Element
Interface
38
45
46
Contactless
Chip
(36(a))
ISO 14443/
NFC
36
Data Transfer
Element
(36(b)
32

FIG. 1A

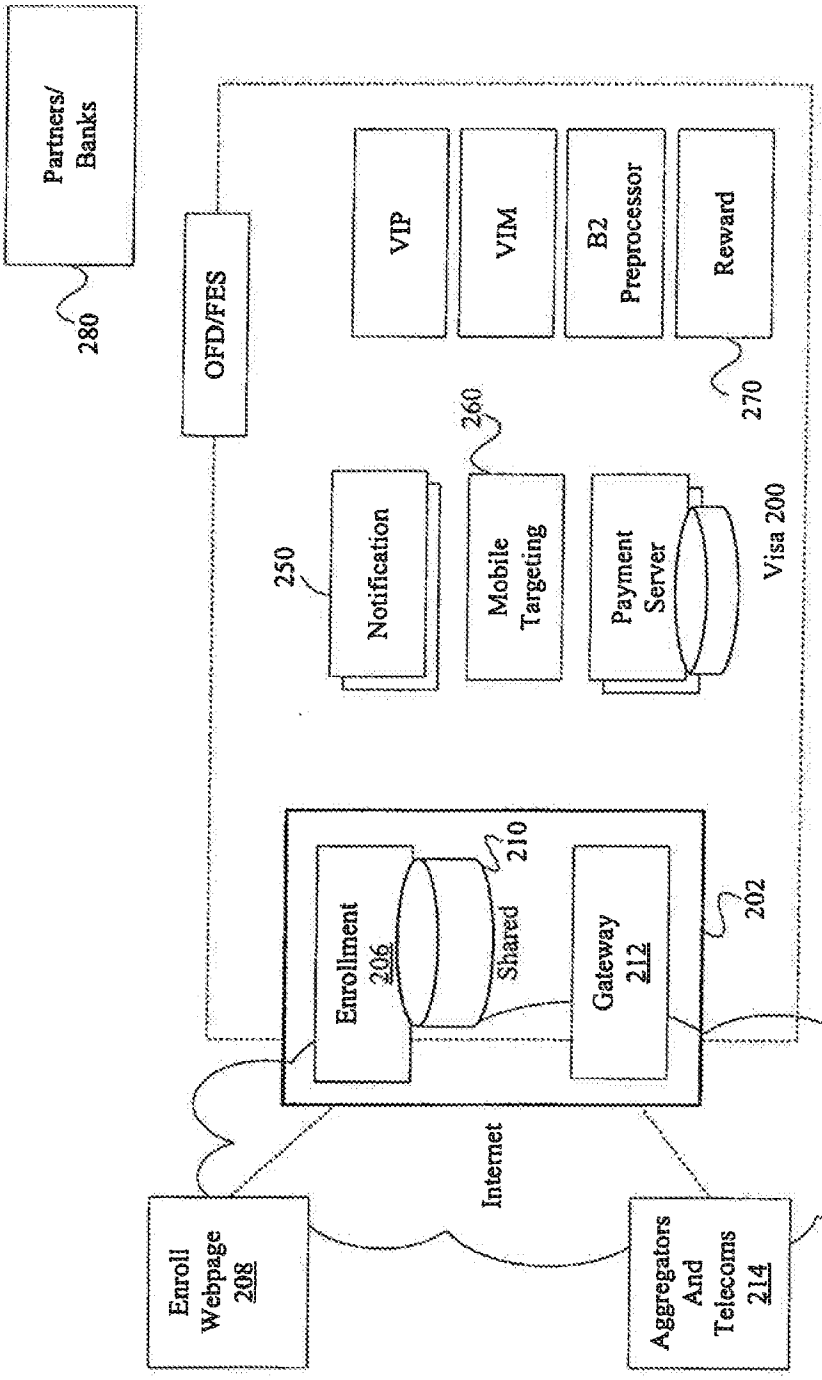

Partners/
Banks
280
OFD/FES
VIP
VIM
B2
Preprocessor
Reward
270
260
250
Notification
Mobile
Targeting
Payment
Server
Visa 200
Enrollment
206
210
Shared
Gateway
212
202
Internet
Enroll
Webpage
208
Aggregators
And
Telecoms
214

FIG. 2

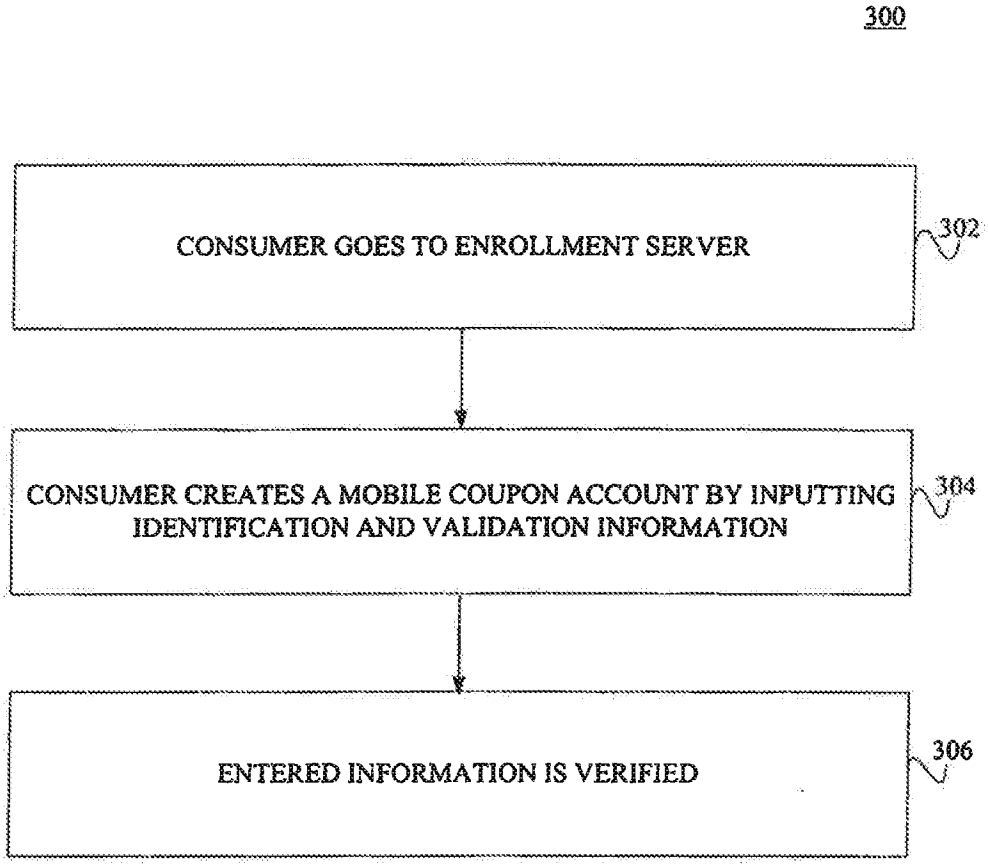

300
CONSUMER GOES TO ENROLLMENT SERVER
302
CONSUMER CREATES A MOBILE COUPON ACCOUNT BY INPUTTING IDENTIFICATION AND VALIDATION INFORMATION
304
ENTERED INFORMATION IS VERIFIED
306

FIG. 3

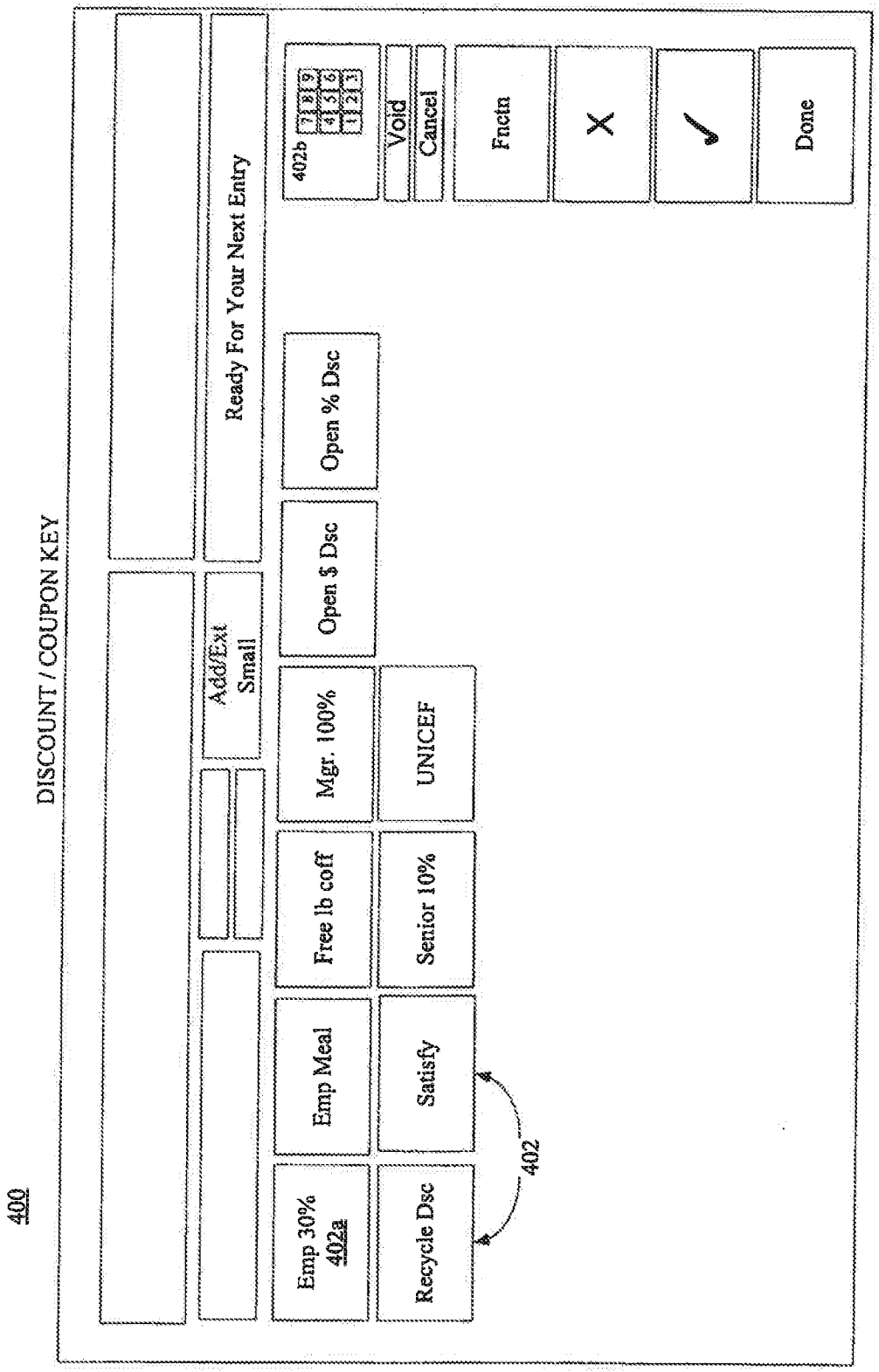

400
DISCOUNT / COUPON KEY
Ready For Your Next Entry
Add/Ext
Small
Emp 30%
402a
Emp Meal
Satisfy
Recycle Dsc
Free lb coff
Senior 10%
Mgr. 100%
UNICEF
Open $ Dsc
Open % Dsc
402b
7 8 9
4 5 6
1 2 3
Void
Cancel
Fnctn
X
✓
Done
402

FIG. 4

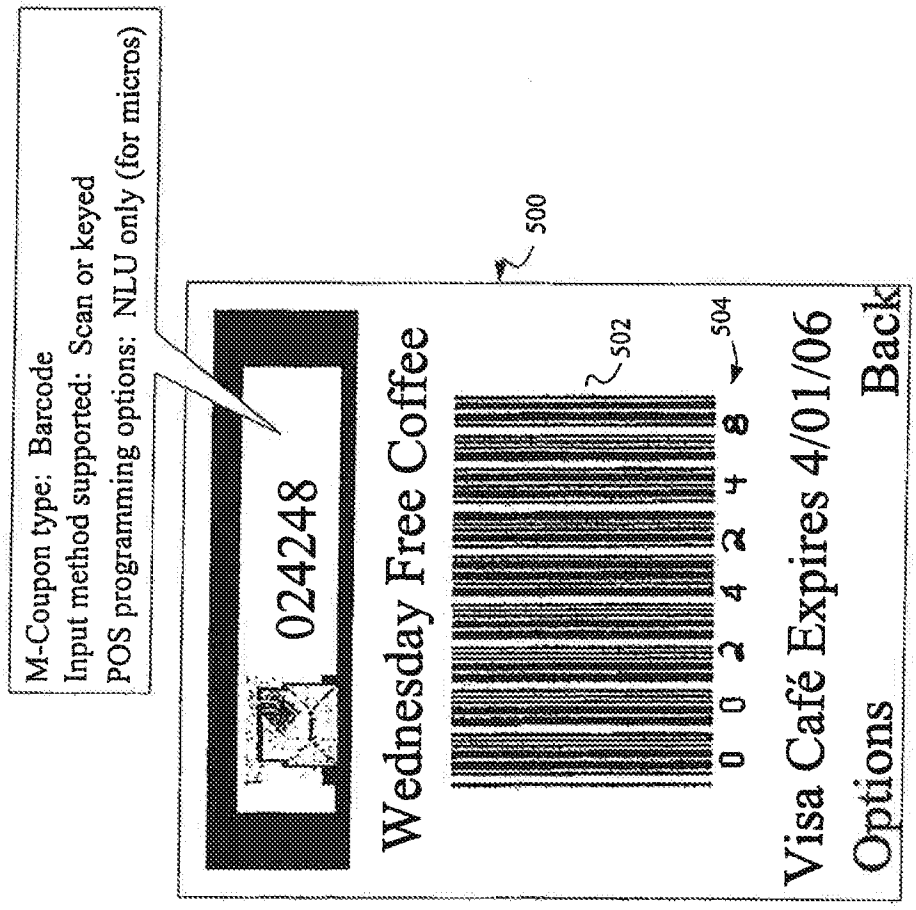

M-Coupon type: Barcode
Input method supported: Scan or keyed
POS programming options: NLU only (for micros)
024248
Wednesday Free Coffee
500
502
504
0 0 2 4 2 4 8
Visa Café Expires 4/01/06
Options
Back

FIG. 5A

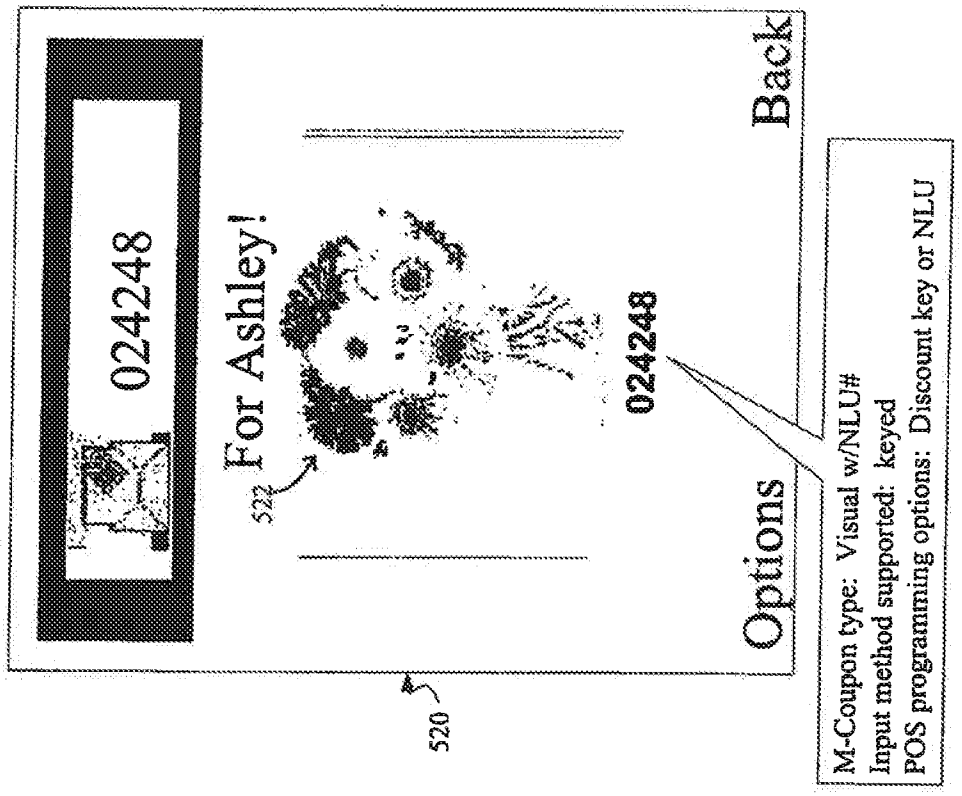

024248
For Ashley!
522
Back
Options
024248
520
M-Coupon type: Visual w/NLU#
Input method supported: keyed
POS programming options: Discount key or NLU

FIG. 5B

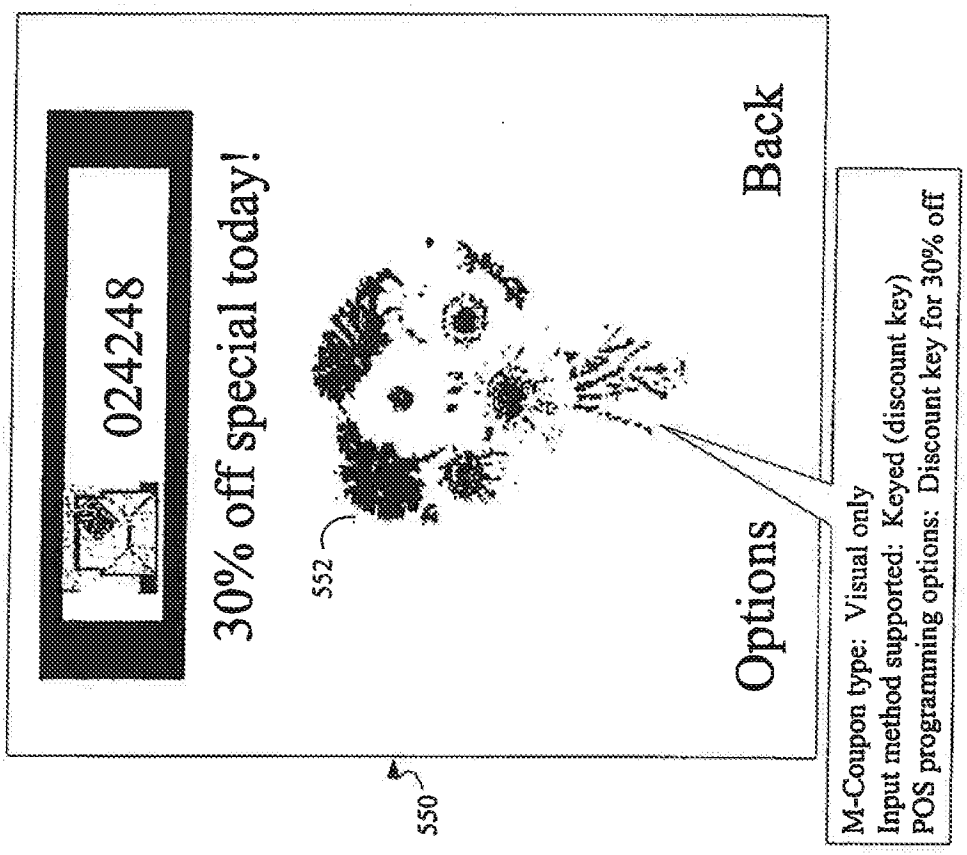

024248
30% off special today!
552
Options
Back
550
M-Coupon type: Visual only
Input method supported: Keyed (discount key)
POS programming options: Discount key for 30% off

FIG. 5C

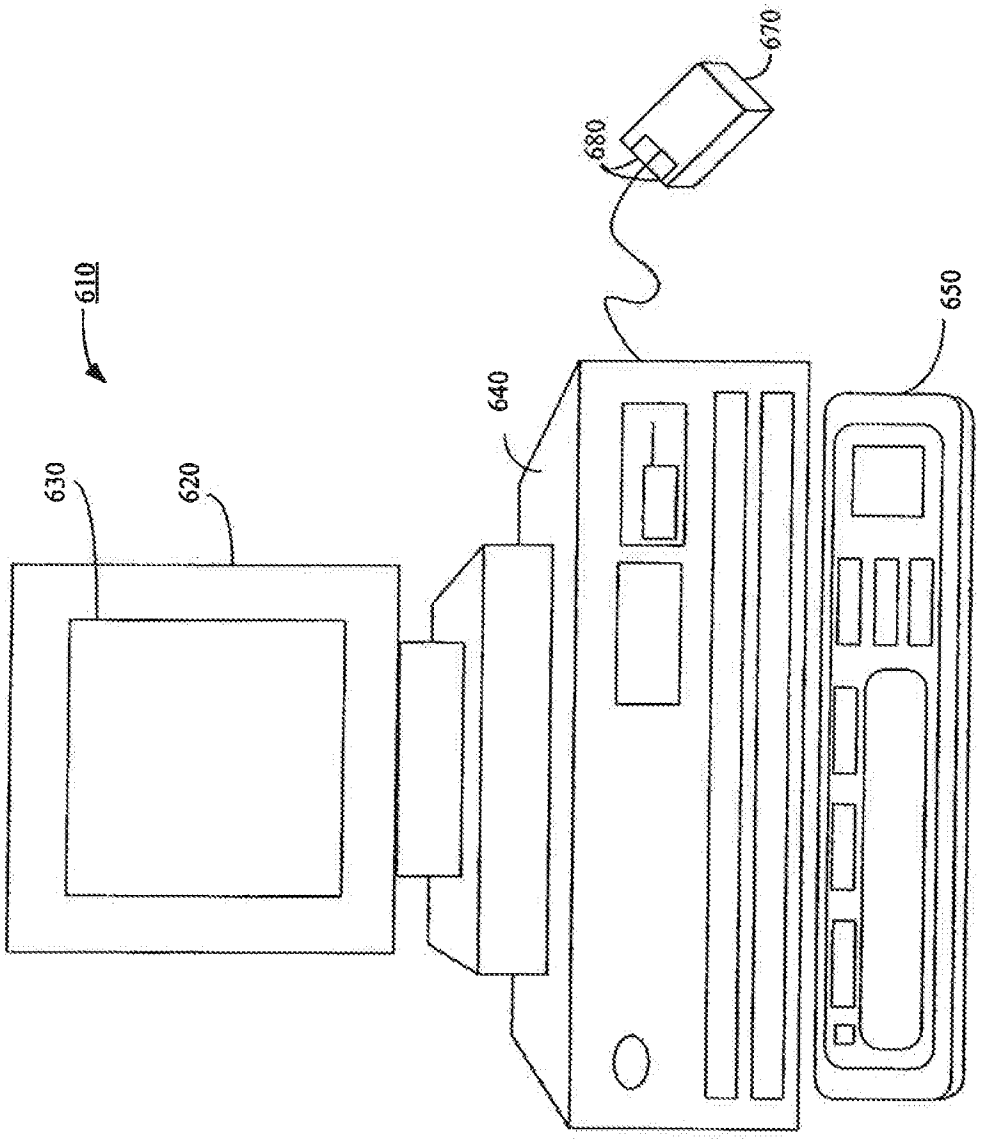


FIG. 6

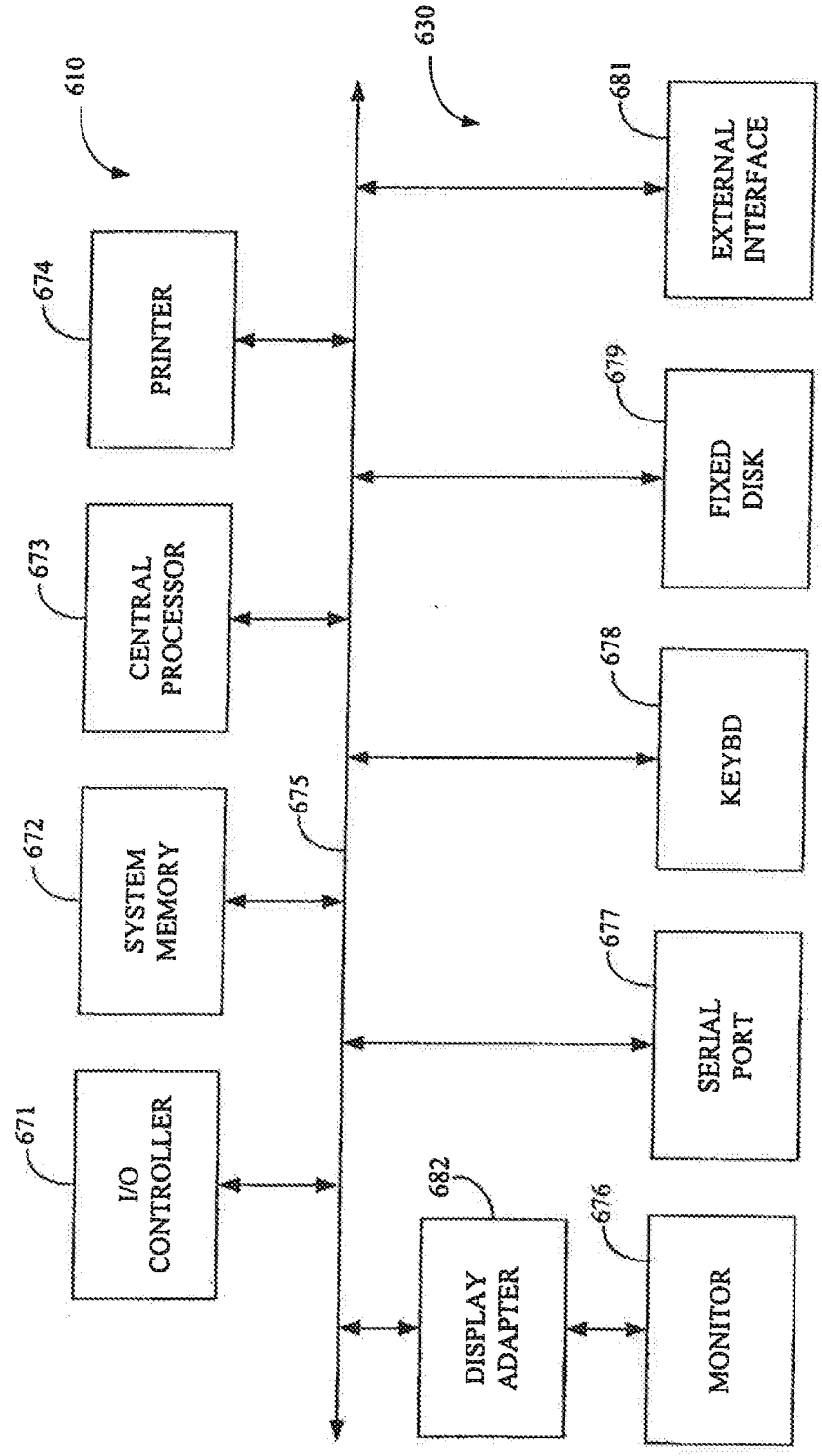

610
630
681
EXTERNAL INTERFACE
674
PRINTER
679
FIXED DISK
673
CENTRAL PROCESSOR
678
KEYBD
672
SYSTEM MEMORY
675
677
SERIAL PORT
671
I/O CONTROLLER
682
DISPLAY ADAPTER
676
MONITOR

FIG. 6A

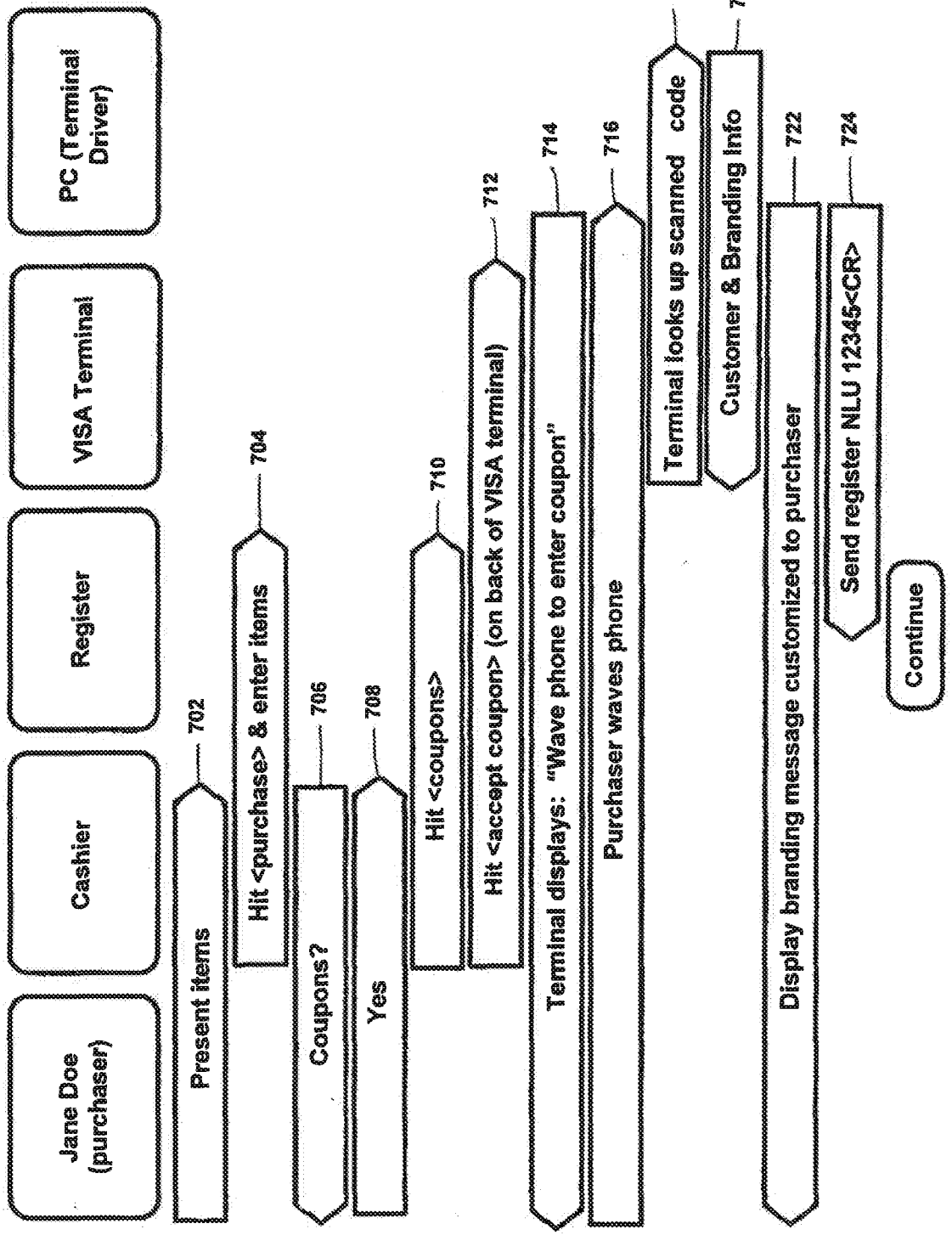


FIG. 7

Petitioner Exhibit 1002-0661

SUBSTITUTE SHEET (RULE 26)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 July 2008 (10.07.2008)

PCT

(10) International Publication Number
WO 2008/083115 A1

(51) International Patent Classification:
G06Q 30/00 (2006.01)

(21) International Application Number:
PCT/US2007/088687

(22) International Filing Date:
21 December 2007 (21.12.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/871,898	26 December 2006 (26.12.2006)	US
11/960,173	19 December 2007 (19.12.2007)	US

(71) Applicants *(for all designated States except US)*: **VISA USA INC.** [US/US]; P.O. Box 8999, M3-2B, San Francisco, California 94128 (US). **VISA INTERNATIONAL SERVICE CORPORATION** [US/US]; 900 Metro Center Boulevard, Foster City, California 94404 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CARLSON, Mark, Steven** [US/US]; 153 Miramontes Avenue, Half Moon Bay, California 94019 (US). **CIUREA, Peter** [US/US]; 6352 Greenridge Court, Martinez, California 94553 (US).

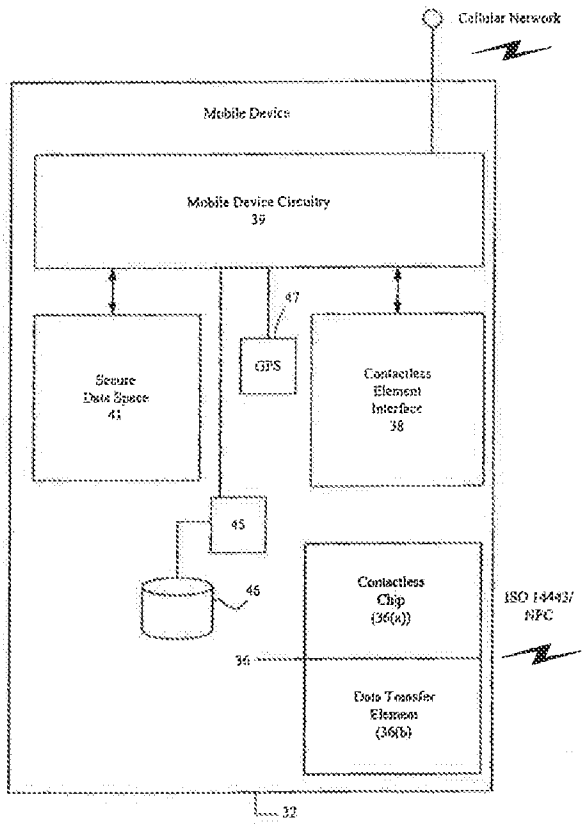
(74) Agents: **TOBIN, Kent, J.** et al.; Townsend And Townsend And Crew Llp, Two Embarcadero Center, 8th Floor, San Francisco, California 94111-3834 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Continued on next page]

(54) Title: MOBILE COUPON METHOD AND SYSTEM



(57) Abstract: A system and a method for using a portable consumer device such as a mobile phone are disclosed. In one embodiment, a method according to the present invention comprises referencing data regarding an individual consumer stored as part of a payment processing network to generate an electronic coupon targeted to the individual consumer. The electronic coupon is transmitted to a mobile device of the individual consumer over a communications network, and purchase transaction utilizing the electronic coupon is processed over the payment processing network. In certain embodiments, the electronic coupon may be generated based upon temporal and/or geographic information of a prior purchase transaction conducted using the payment processing network.

WO 2008/083115 A1

Petitioner Exhibit 1002-0662

ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

Petitioner Exhibit 1002-0663

MOBILE COUPON METHOD AND SYSTEM

CROSS-REFERENCE TO RELATED APPLICATION

[0001] The instant nonprovisional patent application claims priority to U.S. Provisional Patent Application No. 60/871,898, filed December 26, 2006 and incorporated by reference in its entirety herein for all purposes.

BACKGROUND

[0002] Coupons are a useful marketing tool to enhance brand loyalty and introduce new products. By allowing customization of the effective duration and value of an offer, a coupon provides a flexible incentive for a consumer to purchase a particular product or line of products.

[0003] Conventionally, coupons have been available in printed form from sources such as newspapers. Increased adoption of electronic sources of information such as the world-wide-web, however, has led to the increase in popularity of electronic coupons.

[0004] In addition, most consumers now own and operate a cell phone or other portable electronic device. This renders such consumers accessible to the distribution of electronic coupons as they do their shopping, and moreover allows such distributed electronic coupons to be redeemed directly at the store location.

[0005] Accordingly, there is a need in the art for methods and systems allowing for the distribution and use of electronic coupons by mobile electronic devices.

BRIEF SUMMARY

[0006] A system and a method for using a portable consumer device such as a mobile phone are disclosed. In one embodiment, a method according to the present invention comprises referencing data regarding an individual consumer stored as part of a payment processing network to generate an electronic coupon targeted to the individual consumer. The electronic coupon is transmitted to a mobile device of the individual consumer over a communications network, and purchase transaction utilizing the electronic coupon is processed over the payment processing network. In

Petitioner Exhibit 1002-0664

certain embodiments, the electronic coupon may be generated based upon temporal and/or geographic information of a prior purchase transaction conducted using the payment processing network.

[0007] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] FIG. 1 shows a simplified block diagram of a payment processing system.

[0009] FIG. 1A shows a block diagram of a portable consumer device for use with the payment processing system of FIG. 1.

[0010] FIG. 2 shows a simplified block diagram of an embodiment of a system for implementing a mobile coupon program in accordance with an embodiment of the present invention.

[0011] FIG. 3 shows a simplified flow diagram of a process for enrolling in a mobile coupon program according to an embodiment of the present invention.

[0012] FIG. 4 shows a screen from a POS terminal.

[0013] FIGS. 5(a)-5(c) show different screenshots on a phone. The screenshots include coupons.

[0014] Figure 6 is a schematic illustration of a computer system for use in accordance with embodiments of the present invention.

[0015] Figure 6A is an illustration of basic subsystems the computer system of Figure 6.

[0016] Figure 7 shows a simplified flow of a process of utilizing an embodiment of an electronic coupon according to the present invention.

DETAILED DESCRIPTION

[0017] I. Payment Processing Systems

[0018] Embodiments of the invention are directed to the use of portable consumer devices, and methods and systems employing them. Preferred portable consumer devices are mobile phones. The mobile phones can be used in payment processing systems like those shown in FIG. 1.

Petitioner Exhibit 1002-0665

[0019] FIG. 1 shows a system 20 that can be used in an embodiment of the invention. The system 20 includes a merchant 22 and an acquirer 24 associated with the merchant 22. In a typical payment transaction, a consumer 30 may purchase goods or services at the merchant 22 using a portable consumer device 32. The acquirer 24 can communicate with an issuer 28 via a payment processing system 26.

[0020] The acquirer 24 is typically a bank that has a merchant account. The issuer 28 may also be a bank, but could also be business entity such as a retail store. Some entities are both acquirers and issuers, and embodiments of the invention include such entities. The issuer 28 may operate a server computer 21, which may have a computer readable medium comprising code for performing the functions that the issuer 28 performs. A database 23 comprising account number information and other information may be operatively coupled to the server computer 21.

[0021] The consumer 30 may be an individual, or an organization such as a business that is capable of purchasing goods or services.

[0022] The portable consumer device 32 may be in any suitable form. For example, suitable portable consumer devices can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). They may include smart cards, ordinary credit or debit cards (with a magnetic strip and without a microprocessor), keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. Other examples of portable consumer devices include cellular phones, personal digital assistants (PDAs), pagers, payment cards, security cards, access cards, smart media, transponders, and the like. The portable consumer devices can also be debit devices (*e.g.*, a debit card), credit devices (*e.g.*, a credit card), or stored value devices (*e.g.*, a stored value card).

[0023] The portable consumer device 32 may comprise a computer readable medium 32(a) and a body 32(b). The computer readable medium 32(a) may be on the body 32(b). The body 32(b) may in the form a plastic substrate, housing, or other structure. The computer readable medium 32(a) may be a memory that stores data and may be in any suitable form. Exemplary computer readable media 32(a) may be in any suitable form including a magnetic stripe, a memory chip, etc. If the

Petitioner Exhibit 1002-0666

portable consumer device 32 is in the form of a card, it may have an embossed region 32(a) which is embossed with a PAN (primary account number).

[0024] Figure 1A shows an enlarged view of the portable (mobile) device. Device 32 further includes a contactless element 36, typically implemented in the form of a semiconductor chip 36(a) (or other data storage element) with an associated wireless data transfer (e.g., data transmission) element 36(b), such as an antenna. Contactless element 36 is associated with (e.g., embedded within) mobile device 32 and data such as a coupon or control instructions transmitted via cellular network may be applied to contactless element 36 by means of contactless element interface 38. Contactless element interface 38 functions to permit the exchange of data and/or control instructions between the mobile device circuitry 39 (and hence the cellular network) and contactless element 36.

[0025] Mobile device 32 may also include a secure data space 41, which may be used by the device to store operating parameters and/or other data utilized in operation of the device. The secure data space 41 may be in the form of a chip that is separate and apart from the chip in the contactless element 36, or alternatively, could be a section of memory in the chip that forms part of the contactless element 36. Note that the chip in the contactless element 36 may include data storage capability in the form of a memory that may be accessed via interface 38 to permit the implementation of read, write, and erase functions, for example.

[0026] In accordance with still other embodiments, the mobile device may further include a processor 45 and computer readable storage medium 46 for storing code and configured to direct the processor to perform various tasks. For example, the computer readable storage medium may comprise a magnetic disk drive or a flash memory chip.

[0027] As discussed below, the computer readable storage medium may contain code that is configured to cause a processor of the portable consumer device to receive and recognize a message including a coupon and code that is delivered to the mobile device. The computer readable storage medium may also include code that is configured to decrypt an encrypted message including the code that is received by the mobile device.

Petitioner Exhibit 1002-0667

[0028] Contactless element 36 is capable of transferring and receiving data using a near field communications capability (or near field communications medium) typically in accordance with a standardized protocol or data transfer mechanism (identified as ISO 14443/NFC in the figure). Near field communications capability is a short-range communications capability, such as RFID, Bluetooth™, infra-red, or other data transfer capability that can be used to exchange data between the mobile device 32 and a local apparatus, for example located a point-of-sale of a merchant or another location at which coupons are expected to be redeemed. Thus, mobile device 32 is capable of communicating and transferring data and/or control instructions via both cellular network and near field communications capability.

[0029] In accordance with certain embodiments, the mobile device further includes a Global Positioning System (GPS) element 47. GPS element 47 is configured to allow determination of the location of the user at any time. In particular, GPS element 47 relies upon signals from a plurality of orbiting satellites in order to allow the user's location to be determined. Location information obtained from the GPS element 47 may in turn be communicated through the antenna to allow monitoring of the user's position.

[0030] Returning to Figure 1, the payment processing network 26 may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network may include VisaNet™. Payment processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services.

[0031] The payment processing network 26 may include a server computer. A server computer is typically a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The payment processing network 26 may use any suitable wired or wireless network, including the Internet.

Petitioner Exhibit 1002-0668

[0032] The merchant 22 may also have, or may receive communications from, an access device 34 that can interact with the portable consumer device 32. In embodiment of a system of FIG. 1, the access device 34 is located at the merchant 22. However, it could be located at any other suitable location in other embodiments of the invention.

[0033] The access devices according to embodiments of the invention can be in any suitable form. Examples of access devices include point of sale (POS) devices, cellular phones, PDAs, personal computers (PCs), tablet PCs, handheld specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, and the like.

[0034] If the access device 34 is a point of sale terminal, any suitable point of sale terminal may include a reader 34(a), a processor 34(b) and a computer readable medium 34(c). The reader 34(b) may include any suitable contact or contactless mode of operation. For example, exemplary card readers can include RF (radio frequency) antennas, magnetic stripe readers, etc. to interact with the portable consumer device 32.

[0035] In a typical purchase transaction, the consumer 30 purchases a good or service at the merchant 22 using a portable consumer device 32 such as a credit card. The consumer's portable consumer device 32 can interact with an access device 34 such as a POS (point of sale) terminal at the merchant 22. For example, the consumer 30 may take a credit card and may swipe it through an appropriate slot in the POS terminal.

[0036] Alternatively, the POS terminal may be a contactless reader, and the portable consumer device 32 may be a contactless device such as a contactless card. In certain embodiments, the portable consumer device may be a mobile device such as shown in FIG. 1A above. As described in detail below, the antenna of the mobile device may be utilized to communicate not only payment information to the POS, but also may also communicate information (such as a code) from a mobile coupon to a POS device.

[0037] An authorization request message is then forwarded to the acquirer 24. After receiving the authorization request message, the authorization request

Petitioner Exhibit 1002-0669

message is then sent to the payment processing network 26. The payment processing network 26 then forwards the authorization request message to the issuer 28 of the portable consumer device 32.

[0038] After the issuer 28 receives the authorization request message, the issuer 28 sends an authorization response message back to the payment processing network 26 to indicate whether or not the current transaction is authorized (or not authorized). The transaction processing network 26 then forwards the authorization response message back to the acquirer 24. The acquirer 24 then sends the response message back to the merchant 22.

[0039] After the merchant 22 receives the authorization response message, the access device 34 at the merchant 22 may then provide the authorization response message for the consumer 30. The response message may be displayed by the access device 34, or may be printed out on a receipt.

[0040] At the end of the day, a normal clearing and settlement process can be conducted by the transaction processing network 26. A clearing process is a process of exchanging financial details between and acquirer and an issuer to facilitate posting to a consumer's account and reconciliation of the consumer's settlement position.

[0041] Some of the embodiments described below may use a payment processing system like the one described above, or any suitable combination of components in the payment processing system.

[0042] II. Mobile Coupon Method and System

[0043] Particular embodiments in accordance with the present invention relate to methods and apparatuses which allow distribution and/or redemption of electronic coupons at a mobile personal device. Various embodiments of such a system are described in the following figures.

[0044] Figure 2 shows an overall view of an embodiment of a system in accordance with the present invention for administering a mobile coupon program. A first entity 200 (i.e. Visa) is responsible for operating a payment processing network. Under the control of entity 200 are a number of different operational elements.

Petitioner Exhibit 1002-0670

[0045] For example, mobile campaign server 202 functions as the interface between entity 200 and the outside world, here represented by the internet "cloud" 204. Mobile campaign server 202 can include at least three components.

[0046] Specifically, mobile enrollment server 206 provides a browser interface for potential users to enroll in the mobile coupon program using an enrollment webpage 208. Mobile enrollment server 206 is configured to receive from potential users certain pieces of information allowing their participation in the program. For example, in an enrollment form supplied electronically to server 206, the prospective participant can provide information such as the telephone number of their portable device, a security password, and preferences regarding the types of mobile coupons that they wish to receive.

[0047] Figure 3 provides a simplified flow chart of the steps for enrolling in a mobile coupon program. In step 302 of enrollment flow 300, a consumer navigates to the website of the enrollment server utilizing his or her browser.

[0048] In the next step 304, the consumer creates a mobile coupon account by inputting identification and validation information. Examples of such identification information include the user's name, the telephone number of the user's mobile electronic device, financial account numbers, and optional aliases. At this stage, the consumer also verifies that they have read appropriate disclaimers and affirmatively indicate that they seek to opt-into the mobile coupon program.

[0049] In step 306 of enrollment flow 300, information entered by the consumer is verified. Examples of such verification include confirming that the consumer identified is actually in possession of the portable device, that the portable device belongs to the consumer, and that any identified account belongs to the consumer.

[0050] Returning to FIG. 2, mobile enrollment server 206 is in turn in electronic communication with user database 210. Database 210 includes data relating to the user of the mobile coupon system, including the specific information provided during enrollment. Access to the contents of database 210 is shared with gateway server 212.

[0051] Gateway server 212 serves as the interface with outside entities responsible for implementing the mobile coupon program. For example, telecommunications

Petitioner Exhibit 1002-0671

companies ("telecoms") 214 provide the infrastructure necessary to communicate the coupon to the user's mobile device wherever they happen to be. The telecom entities must provide sufficient capacity to handle a sufficiently high volume of coupon messages outgoing to recipients.

[0052] Where such volume of messages is expected to be small (for example at the inception of the mobile coupon program), another type of company called an aggregator will secure sufficient bandwidth for all of the expected messages from the telecom, and then aggregate the messages from different sources.

[0053] In an exemplary embodiment, a coupon is sent to a user's phone or other portable device. The coupon may be sent in any one of a number of different forms, including but not limited to an short messaging service (SMS) message, a SMS link, a multimedia messaging service (MMS) message, or e-mail message.

[0054] The coupon may be communicated utilizing any one of several types of communications systems. For example, the coupon may be communicated to the cell phone utilizing SMS. Such an embodiment offers a number of possible advantages, including broad access as SMS is available on almost every cell phone. Possible disadvantages to mobile coupon distribution utilizing SMS is a weak mechanism for confirming receipt of the coupon by the designated recipient, and also a high transaction cost as charges are typically incurred for each SMS message transmitted.

[0055] In accordance with alternative embodiments, the mobile coupon could be distributed by a Global System for Mobile Communications (GSM) system. Such GSM communication are cheap and secure, and would support confirmation of receipt of the coupon by a designated user.

[0056] Further alternatively, the coupons could be distributed utilizing a Near Field Communications (NFC) system. Such an embodiment would require the portable consumer device to be equipped with an NFC chip and programmed with a software application. The source of the near field signal providing the electronic coupon could be local kiosks, for example as present in a shopping mall. An alternative source of electronic coupons available utilizing such near field communication is the point of sale itself. Other sources are possible.

Petitioner Exhibit 1002-0672

[0057] The coupon may be communicated to the portable consumer device in encrypted form. Such encryption would prevent interception and unauthorized use of a coupon by other than the intended recipient. A processor present in the portable consumer device could in turn decrypt the message upon its receipt.

[0058] FIG. 4 shows a screen 400 from a POS terminal. The screen 400 shows buttons 402 that a cashier might select in order to initiate a pre-arranged discount utilizing an electronic coupon. For example, button 402a allows the cashier to implement a 30% discount for employees etc. Button 402b allows the cashier to manually enter a number for numeric look-up (NLU) from an electronic coupon displayed on a user's portable electronic device.

[0059] FIGS. 5A-5C are examples of three screenshots showing graphical coupons in different forms. These screenshots are configured to be able to be displayed on the small screen of a mobile phone, personal digital assistant (PDA), or other mobile device.

[0060] FIG. 5A shows a screenshot 500 which includes both a bar code 502 (which is an example of a machine readable code) and a seven digit number 504. The bar code 502 can be scanned with a scanner. One type of scanner which may be used to read a bar code on the screen of a cell phone is a charge coupled device (CCD) scanner. However, a laser-type scanner may not be able to read the bar code displayed due to reflection from the screen.

[0061] In order to process the electronic coupon shown in FIG. 5A, the user accesses and displays the coupon on the screen of his or her portable device. The cashier then accesses the discount screen shown in FIG. 4, and either scans the bar code in directly or enters the seven-digit number utilizing a numeric key pad.

[0062] FIG. 5B illustrates a screenshot 520 showing a different embodiment of a mobile electronic coupon in accordance with the present invention, which includes a visual display 522 and a personalized message 523. This visual display may be related to the nature of the coupon, representing for example the purchase of flowers. Alternatively, the display may simply illustrate the nature of the coupon, for example the display of flowers generically representing a gift.

Petitioner Exhibit 1002-0673

[0063] Instead of a barcode, a six digit number "024248" is shown by the electronic coupon 520. In processing of coupon 520 by a cashier, this six digit number can be entered into a POS terminal to give the consumer a discount on a purchase. In accordance with one embodiment, the number can be entered by having the cashier type in the individual digits of the code on a numeric keypad. In accordance with an alternative embodiment, the number can be entered by having the cashier activate a predetermined key, or combination thereof, which allows recognition of the coupon and the discount.

[0064] The embodiment of Figure 5B may offer certain advantages over a coupon employing a bar code as shown in Figure 5A. One advantage is ease of operation, as there is no requirement for optical recognition/reading of a code from the screen of the phone. Another possible advantage is reduced cost of implementation, as a bar code scanner device is not required to be purchased or rented by the merchant. In addition, software and hardware upgrades relating to electronic scanning would not be required by this alternative embodiment.

[0065] Lastly, FIG. 5C shows a screenshot 550 showing a "30% off" coupon. This electronic coupon includes a visual display 552 but lacks either a bar code or an identifying number.

[0066] To use this coupon, the user shows the display to the cashier and the cashier selects a button on a POS terminal display (see FIG. 4) to provide the discount to the consumer. According to still further embodiments of the present invention, coupon information such as a code may be communicated to a portable device in a proprietary format.

[0067] Figure 7 shows a simplified flow of a process of utilizing a mobile coupon according to an embodiment of the present invention. In a first step 702 of process flow 700, a purchaser presents items to a cashier. In step 704, the cashier hits the purchase key and enters the items. In step 706, the coupon asks the purchaser whether or not she intends to use coupons. In step 708, the purchaser responds that she intends to use a coupon.

[0068] In step 710 of process flow 700, the cashier hits the coupons key to alert the register to the use of coupons. In step 712, the cashier hits the accept coupon button on the back of the VISA terminal.

Petitioner Exhibit 1002-0674

[0069] In step 714, the VISA terminal displays a message requesting the purchaser to wave the phone to enter a coupon. In step 716, the purchaser waves the phone and the terminal receives the scanned code. In step 718 the processor in communication with the terminal looks up the scanned code. In step 720, the processor returns to the terminal, customer and branding information. In step 722, the terminal displays a branding message customized to the particular purchaser. Finally, in step 724, the terminal sends to the register a numeric look up representing the bar code.

[0070] A variation according to embodiments of the present invention may utilize near field communication of the coupon or a code therein, to the cashier. In this variation, a multi-digit numerical code (i.e. six digits) can be transmitted to the POS terminal via a reader using a contactless device such as the mobile device of FIG. 1A including an antenna. The coupon may be communicated in such a contactless manner using a short range communication method, such as a near field communications (NFC) capability. Examples of such NFC technologies include ISO standard 14443, RFID, Bluetooth™ and Infra-red communications methods. In accordance with such embodiments, the six digit code may or may not be shown on the display of the phone. Embodiments in accordance with the present invention are not limited to communicating coupon code information. In accordance with alternative embodiments, coupon information communicated from a mobile device to a POS terminal may include other information, for example a product code limiting applicability of the mobile coupon to a particular product, or an expiration date/time of the mobile coupon.

[0071] In certain embodiments, payment information (such as a credit card number, debit card number, home zip code of the card holder, or a three digit card verification value code) may be communicated from a mobile device in a contactless manner to the POS terminal. In such embodiments, the coupon information from the mobile device may also be communicated to the POS terminal in a contactless manner. In some embodiments, such communication of mobile coupon information may take place as part of the same message communicating payment information to the POS terminal. Alternatively, the coupon information may be communicated prior to, or following, contactless communication of the payment information to the POS terminal.

Petitioner Exhibit 1002-0675

[0072] The consumer may receive a text message, a phone call, or e-mail indicating that the consumer has received a coupon. The consumer may then use his or her phone to transmit a code corresponding to the coupon, to a contactless reader coupled to a POS terminal. The near field communication can utilize, for example, infrared or an RF communication mode such as Bluetooth. The system shown in FIG. 1 can be used in conjunction with such an embodiment.

[0073] Returning to Figure 2, apart from the mobile campaign server, a number of other elements are also under the control of entity 200. Notification module 250 is responsible for notifying participants in the program of particular events, for example limited time promotions or even the possibility of fraudulent transactions.

[0074] Mobile targeting module 260 is responsible for generating coupons targeted to a user. According to certain embodiments, the coupons can be targeted based upon a location based services (LBS) approach, utilizing prior purchasing activity by a consumer as detected over a payment processing network.

[0075] Specifically, where a payment transaction is conducted over a payment processing network, certain information is communicated that can be used for targeting of a mobile coupon. One piece of information that is potentially useful for targeting is the timing of the prior payment transaction.

[0076] In particular, the very existence of the prior purchase transaction reveals the consumer to be actively engaged in shopping rather than other activities (i.e. sleeping or working). Based upon this timing information, the consumer is known to likely be receptive to a mobile coupon for a subsequent transaction. Accordingly, embodiments of the present invention may thus generate and disseminate a mobile coupon to the consumer within a predetermined, limited time period from receiving an indication from the payment processing network that a prior payment transaction has occurred. Examples of time periods for dissemination of mobile coupons include, but are not limited to, one minute or less, five minutes, ten minutes, fifteen minutes, one-half hour, forty-five minutes, one hour, one and one half hours, two hours, three hours, four hours, and five hours or longer from the time that a prior purchasing activity is detected from the payment processing network. Such an approach allows for dissemination of a timely, non-intrusive mobile coupons to the consumer.

Petitioner Exhibit 1002-0676

[0077] In certain embodiments, the duration of effectiveness of such a mobile coupon can also be limited by time. Such an embodiment would provide an incentive for the recipient to monitor his or her portable device for receipt of a mobile coupon, and use that coupon within the limited period that it is effective. Moreover, in certain embodiments, upon expiration the mobile coupon could be configured to automatically disappear from the consumer's portable device. This would reduce intrusiveness of the mobile coupon, as the consumer is not obligated to delete a backlog of expired coupons from his or her portable device.

[0078] Embodiments of the present invention are not limited to generating and promulgating mobile coupons based upon temporal information gleaned from a prior purchase transaction over a payment processing network. In accordance with alternative embodiments, the mobile coupons can be targeted based upon a geographic location of the user as determined from the payment processing network.

[0079] According to one embodiment, the location of the consumer can be determined from purchasing activity of the user based upon a Location Based Services (LBS) approach. For example, when the user swipes a card at a POS, an authorization message is returned from the payment network which includes a Merchant Identification Number (MID). The user's location at that time of sale can be determined from the MID number.

[0080] According to other embodiments, information regarding the nature of the prior purchase conducted over the payment processing network can be referenced to generate the coupon. Thus, a prior purchase of one product (for example a vacuum cleaner), could lead to generation of a second product (bags for the vacuum cleaner). This coupon generation could be irrespective of the time or physical location of a prior purchasing transaction. Still further alternatively, an LBS approach could be based upon the seller of the second product having an affinity agreement with the seller of the previous product purchased.

[0081] Moreover, a mobile coupon may be generated based upon more than one piece of information gleaned from a prior purchasing transaction conducted over a payment processing network. Specifically, the time, geographic location, and/or nature of the prior purchase transaction could be combined to generate the targeted coupon.

Petitioner Exhibit 1002-0677

[0082] According to still other embodiments, information from a prior purchase transaction available from a payment processing network, may be combined with other information to generate a targeted coupon. For example, information regarding the location of the consumer can be determined from sources other than the payment processing network.

[0083] According to one approach, the location of a consumer can be determined by analyzing the location of the current base station through which the portable user device is transmitting and receiving information. Such current base station information is available from the telecommunications provider with which the consumer is affiliated, and in other applications is utilized to allow the user to contact the closest medical services provider in the case of a medical emergency. Thus, in certain embodiments, geographic information from this source could be combined with information (time, nature of prior purchases) available from the payment processing network, to generate a targeted coupon.

[0084] According to another approach, the location of a consumer can be determined by the use of Global Positioning System (GPS) technology. In this approach, the location of the portable device of the consumer is monitored utilizing a plurality of orbiting satellites. Thus, in other embodiments, geographic information from this source could be combined with information (time, nature of prior purchase) available from the payment processing network, to generate a targeted coupon.

[0085] Utilizing any of these approaches, or others, alone or in combination, the mobile targeting module 260 may send out a targeted mobile coupon to a consumer. For example, the mobile electronic coupon can be targeted in whole or in part based upon the recipient belonging to a particular group, such as an employee of a business or a member of a club.

[0086] Reward module 270 (such as "Visa Extras") is responsible for coordinating and administering an incentive or reward program that is tied to use of the payment network Thus a targeted mobile coupon may be generated and then electronically distributed to a portable consumer device as part of an incentive program. For example, the accrual of a certain volume of purchases utilizing a Visa card, may render the program participant eligible for a particularly valuable type of electronic coupon not typically available to other participants in the mobile coupon program.

Petitioner Exhibit 1002-0678

This targeted electronic coupon is then communicated to the consumer's mobile device for redemption.

[0087] Other elements indicated under the control of entity 200 in FIG. 2, may relate to the function of the payment network to execute purchase and payment transactions. Partners and banks 280 are outside of the control of entity 200 but interact therewith as part of the processing of payment transactions.

[0088] It should be understood that the present invention as described above can be implemented in the form of control logic using computer software in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement the present invention using hardware and a combination of hardware and software.

[0089] The various components of the mobile coupon system described above may be implemented with a computer system having various features. FIG. 6 shows an example of a generic computer system 610 including display device 620, display screen 630, cabinet 640, keyboard 650, and mouse 670. Mouse 670 and keyboard 650 are representative "user input devices." Mouse 670 includes buttons 680 for selection of buttons on a graphical user interface device. Other examples of user input devices are a touch screen, light pen, track ball, data glove, microphone, and so forth. FIG. 6 is representative of but one type of system for embodying the present invention. It will be readily apparent to one of ordinary skill in the art that many system types and configurations are suitable for use in conjunction with the present invention. In a preferred embodiment, computer system 610 includes a Pentium class based computer, running Windows NT operating system by Microsoft Corporation. However, the apparatus is easily adapted to other operating systems and architectures by those of ordinary skill in the art without departing from the scope of the present invention.

[0090] As noted, mouse 670 can have one or more buttons such as buttons 680. Cabinet 640 houses familiar computer components such as disk drives, a processor, storage device, etc. Storage devices include, but are not limited to, disk drives, magnetic tape, solid state memory, bubble memory, etc. Cabinet 640 can include additional hardware such as input/output (I/O) interface cards for connecting

Petitioner Exhibit 1002-0679

computer system 610 to external devices external storage, other computers or additional peripherals, further described below.

[0091] FIG. 6A is an illustration of basic subsystems in computer system 610 of FIG. 6. This diagram is merely an illustration and should not limit the scope of the claims herein. One of ordinary skill in the art will recognize other variations, modifications, and alternatives. In certain embodiments, the subsystems are interconnected via a system bus 675. Additional subsystems such as a printer 674, keyboard 678, fixed disk 679, monitor 676, which is coupled to display adapter 682, and others are shown. Peripherals and input/output (I/O) devices, which couple to I/O controller 671, can be connected to the computer system by any number of means known in the art, such as serial port 677. For example, serial port 677 can be used to connect the computer system to a modem 681, which in turn connects to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via system bus allows central processor 673 to communicate with each subsystem and to control the execution of instructions from system memory 672 or the fixed disk 679, as well as the exchange of information between subsystems. Other arrangements of subsystems and interconnections are readily achievable by those of ordinary skill in the art. System memory, and the fixed disk are examples of tangible media for storage of computer programs, other types of tangible media include floppy disks, removable hard disks, optical storage media such as CD-ROMS and bar codes, and semiconductor memories such as flash memory, read-only-memories (ROM), and battery backed memory.

[0092] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

Petitioner Exhibit 1002-0680

[0093] The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0094] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0095] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

Petitioner Exhibit 1002-0681

WHAT IS CLAIMED IS:

1. A method comprising:

referencing data regarding an individual consumer stored as part of a payment processing network to generate an electronic coupon targeted to the individual consumer;

transmitting the electronic coupon to a mobile device of the individual consumer over a communications network; and

processing a purchase transaction utilizing the electronic coupon over the payment processing network.

2. The method of claim 1 wherein the electronic coupon is generated based upon a prior transaction conducted over the payment processing network.

3. The method of claim 2 wherein the electronic coupon is generated within a predetermined time from a time of the prior transaction.

4. The method of claim 1 wherein the electronic coupon is targeted based upon a geographic location of the individual consumer.

5. The method of claim 4 wherein the geographic location of the consumer is determined from a location based services (LBS) approach based upon a prior transaction conducted over the payment processing network.

6. The method of claim 5 wherein the geographic location is determined from a merchant identification number in the prior transaction.

7. The method of claim 4 wherein the geographic location of the consumer is determined from a global positioning system (GPS) element in the mobile device.

8. The method of claim 4 wherein the geographic location of the consumer is determined from the mobile device communicating through the communications network.

9. The method of claim 1 wherein the electronic coupon is communicated in encrypted form.

Petitioner Exhibit 1002-0682

10. The method of claim 1 wherein the electronic coupon is communicated including a code able to be electronically transmitted from the mobile device to a point of sale.

11. The method of claim 1 wherein the data regarding the individual consumer is obtained based upon an enrollment form submitted by the individual consumer.

12. The method of claim 1 wherein the data regarding the individual consumer is obtained based upon the individual consumer's use of the payment processing network.

13. A server for a mobile coupon program, the server comprising:

a processor; and

a computer readable storage medium in electronic communication with the processor, the computer readable storage medium having stored thereon, code instructing the processor to,

reference data regarding an individual consumer stored as part of a payment processing network to generate an electronic coupon targeted to the individual consumer, and

transmit the electronic coupon to a mobile device of the individual consumer over a communications network.

14. The server of claim 13 wherein the code instructs generation of the electronic coupon based upon a prior transaction conducted over the payment processing network.

15. The server of claim 14 wherein the code instructs generation of the electronic coupon within a predetermined time of a time of the prior transaction.

16. The server of claim 13 wherein code instructs generation of the electronic coupon based upon a geographic location of the individual consumer.

17. The server of claim 16 wherein the geographic location of the consumer is determined from a location based services (LBS) approach based upon a prior transaction conducted over the payment processing network.

Petitioner Exhibit 1002-0683

18. The server of claim 16 wherein the geographic location of the consumer is determined from a merchant identification number in the prior transaction.

19. The server of claim 16 wherein the geographic location of the consumer is determined from a global positioning system (GPS) element in the mobile device.

20. The server of claim 16 wherein the geographic location of the consumer is determined from the mobile device communicating through the communications network.

21. A method comprising:

a consumer conducting a first purchasing transaction over a payment processing network;

generating an electronic coupon targeted to the consumer based upon the first purchasing transaction;

transmitting the electronic coupon to a mobile device of the consumer; and

processing a second purchasing transaction over the payment processing network, the second purchasing transaction involving use of the electronic coupon to obtain a discount.

22. The method of claim 21 wherein the coupon is generated within a predetermined time of a time of the first purchasing transaction.

23. The method of claim 21 wherein the coupon is generated based upon a geographic location of the first purchasing transaction.

24. The method of claim 21 wherein the first purchasing transaction or the second purchasing transaction allow the consumer to receive an award.

Petitioner Exhibit 1002-0684

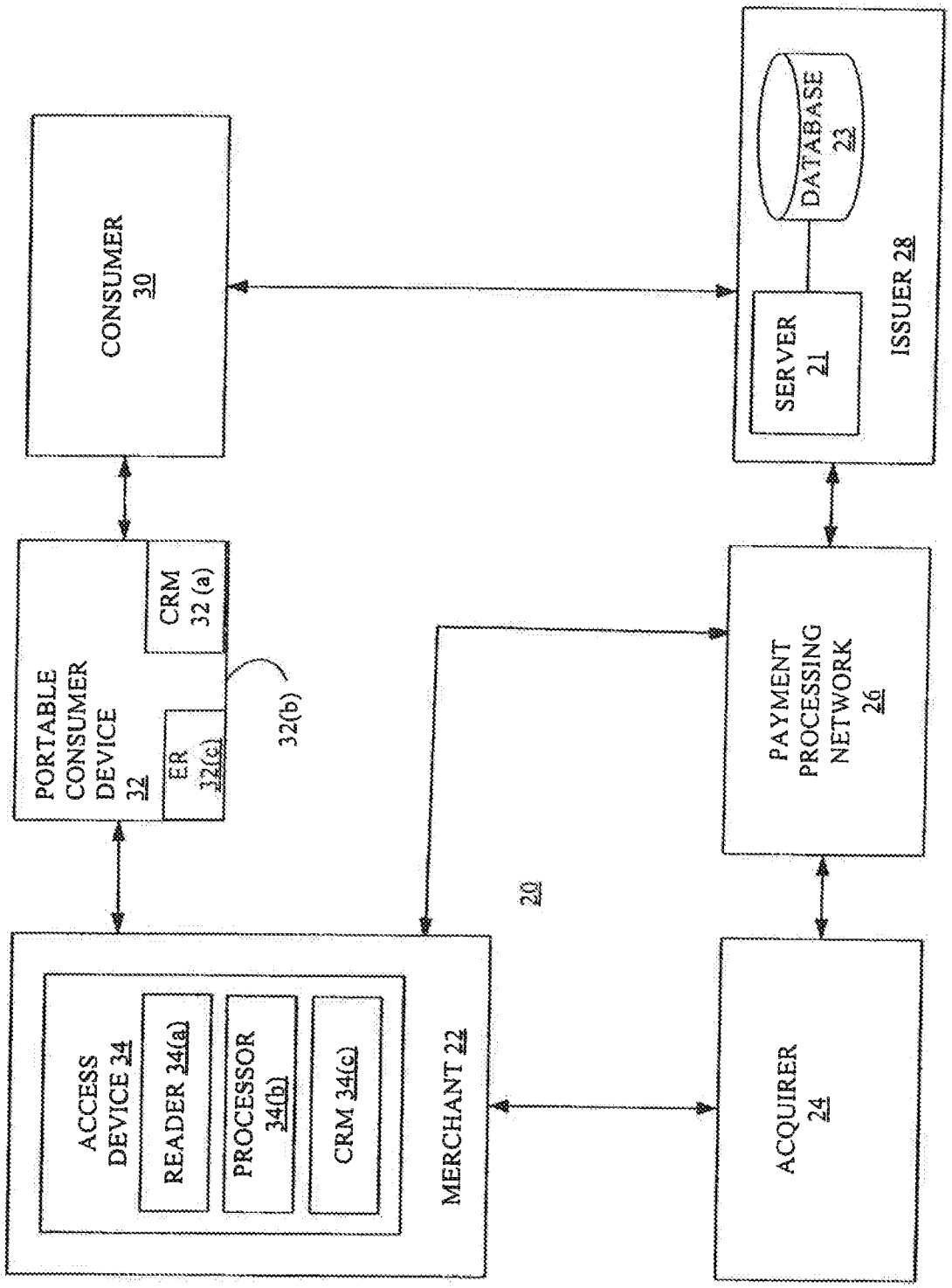

CONSUMER 30
PORTABLE CONSUMER DEVICE 32
CRM 32 (a)
ER 32(c)
32(b)
ACCESS DEVICE 34
READER 34(a)
PROCESSOR 34(b)
CRM 34(c)
MERCHANT 22
20
PAYMENT PROCESSING NETWORK 26
ACQUIRER 24
SERVER 21
DATABASE 23
ISSUER 28

FIG. 1

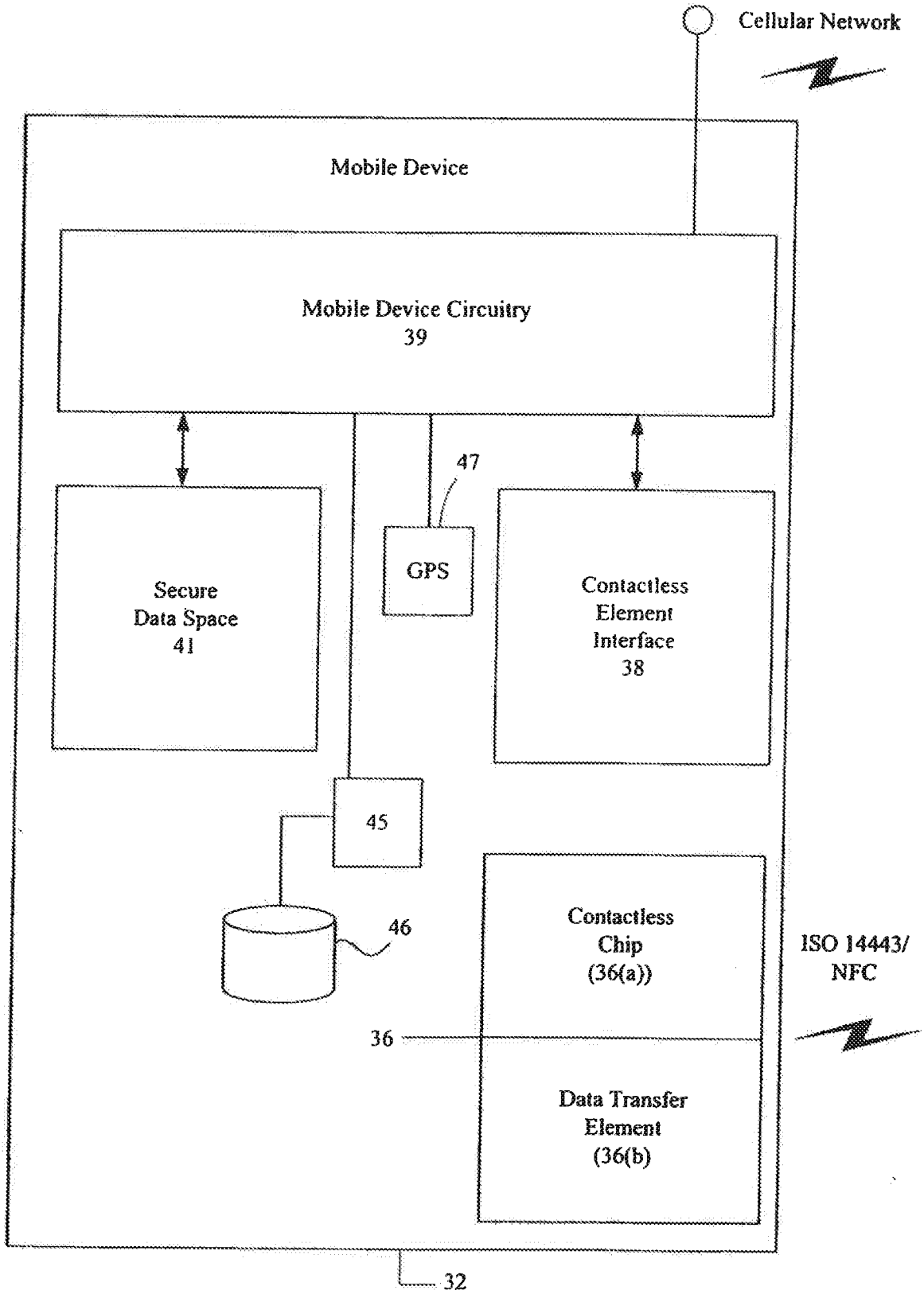

Cellular Network
Mobile Device
Mobile Device Circuitry
39
47
GPS
Secure
Data Space
41
Contactless
Element
Interface
38
45
46
Contactless
Chip
(36(a))
ISO 14443/
NFC
36
Data Transfer
Element
(36(b)
32

FIG. 1A

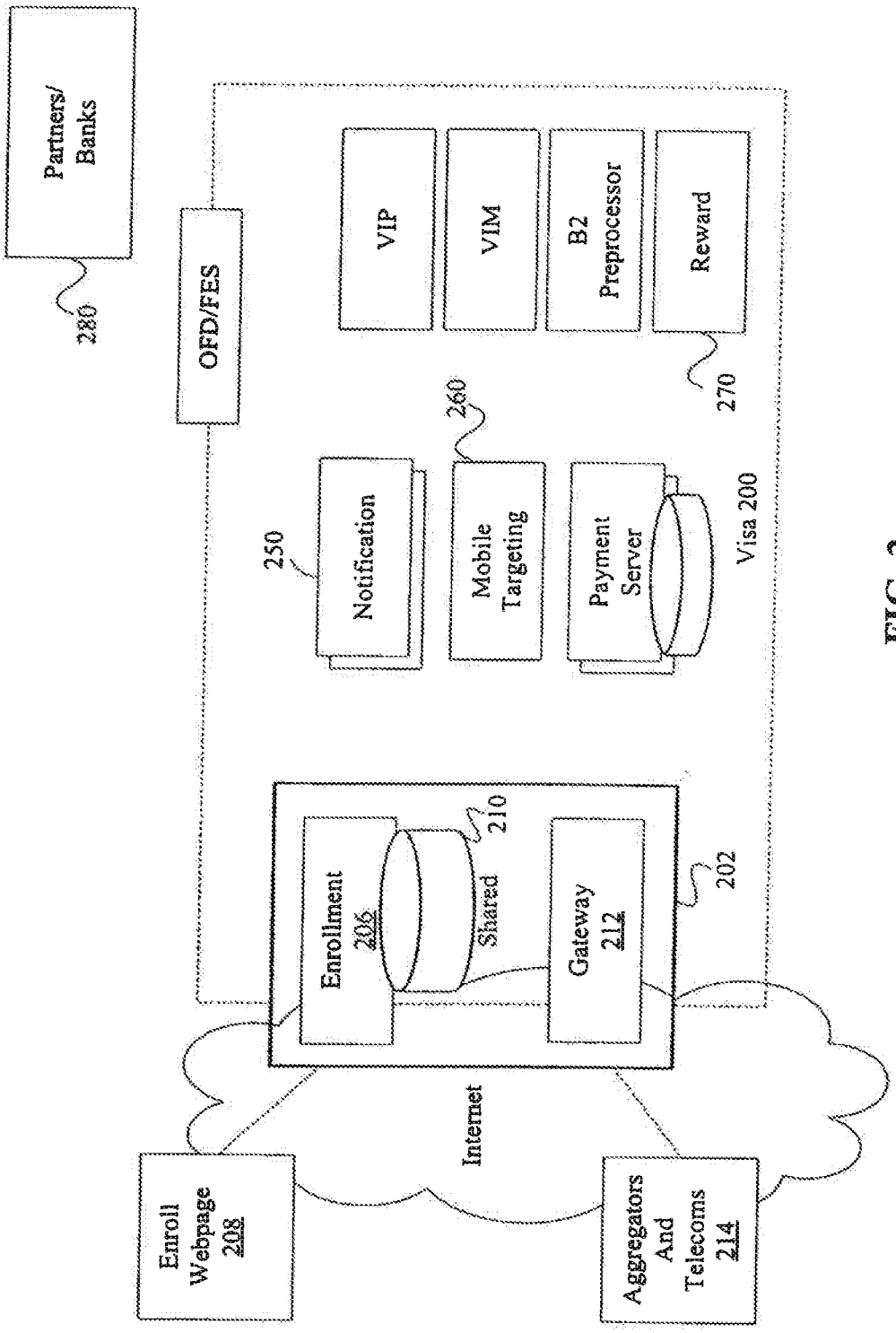

Partners/ Banks
280
OFD/FES
VIP
VIM
B2 Preprocessor
Reward
270
260
250
Notification
Mobile Targeting
Payment Server
Visa 200
Enrollment 206
210
Shared
Gateway 212
202
Internet
Enroll Webpage 208
Aggregators And Telecoms 214

FIG. 2

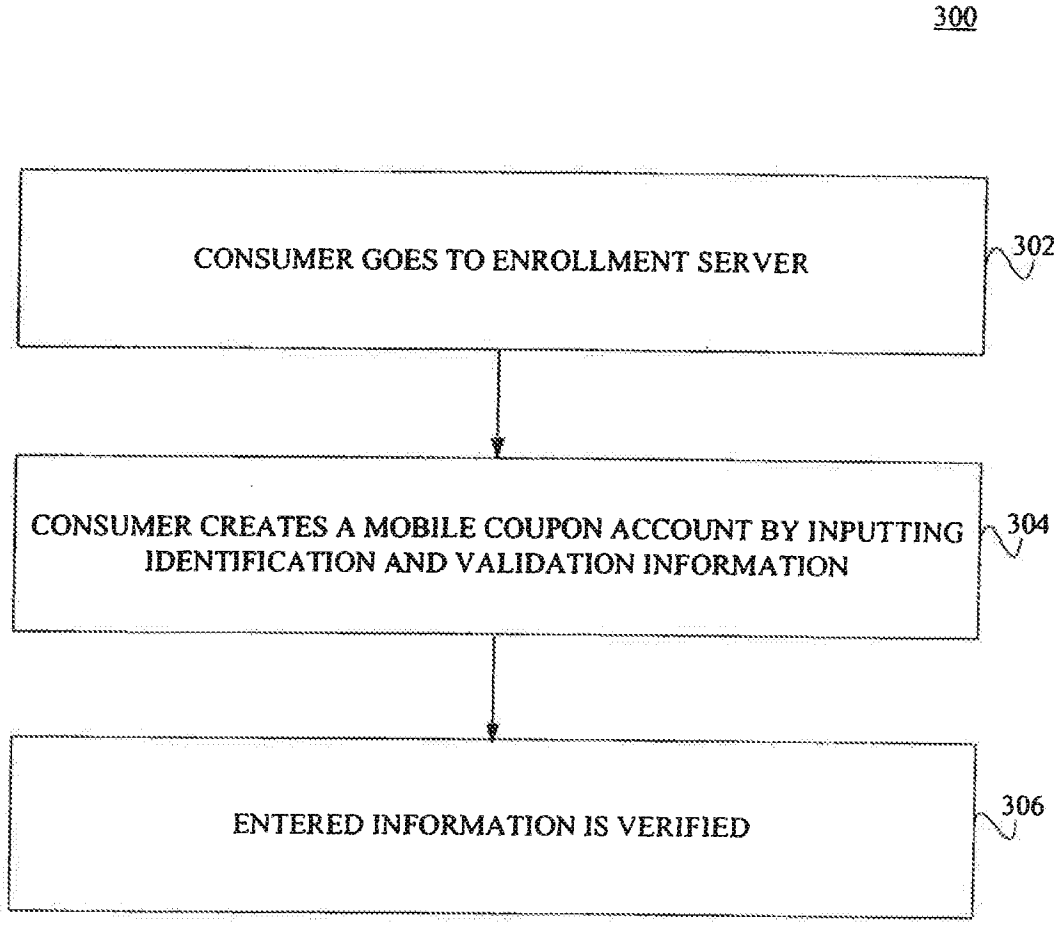


FIG. 3

Petitioner Exhibit 1002-0688

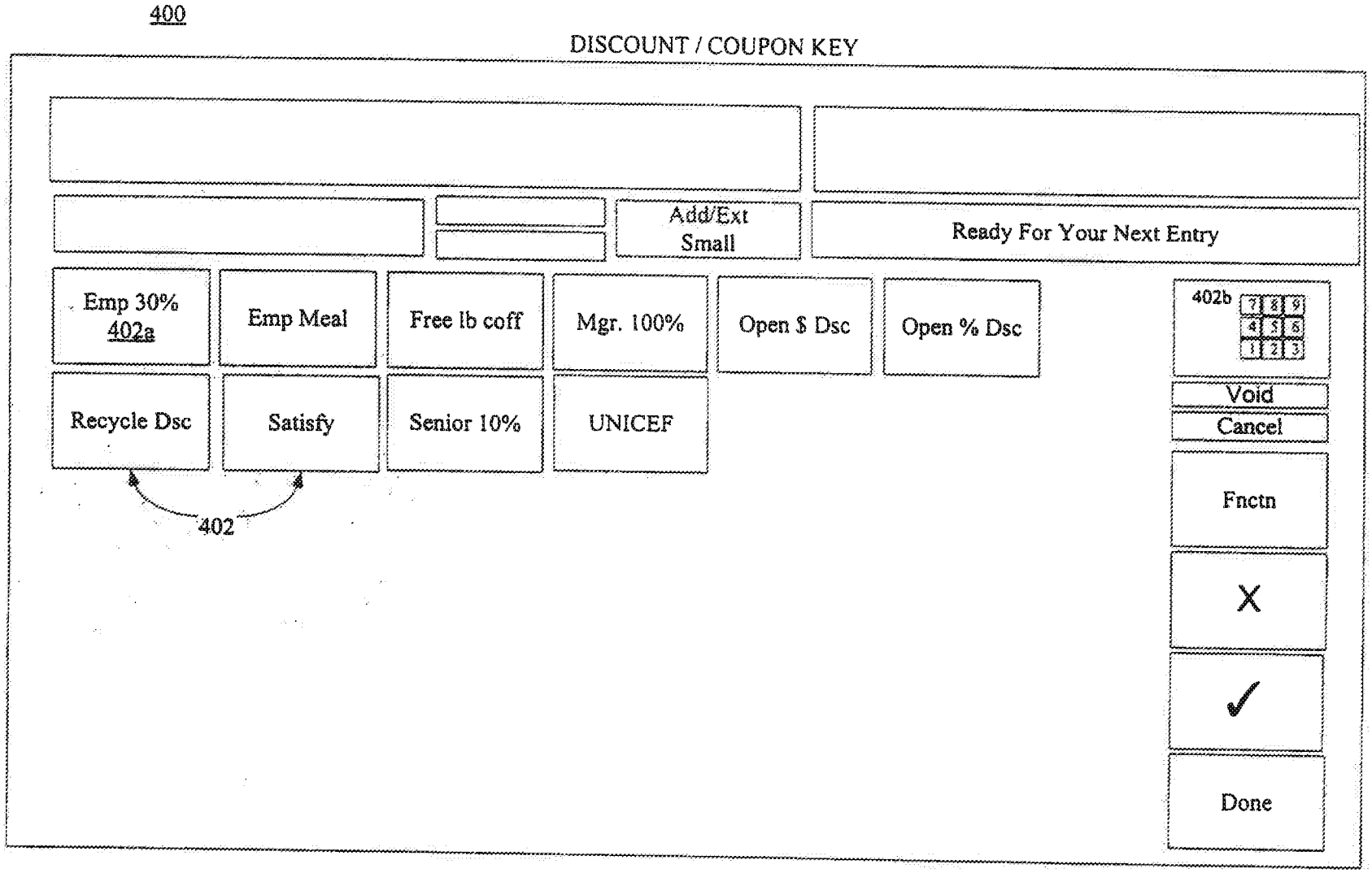


FIG. 4

Petitioner Exhibit 1002-0689

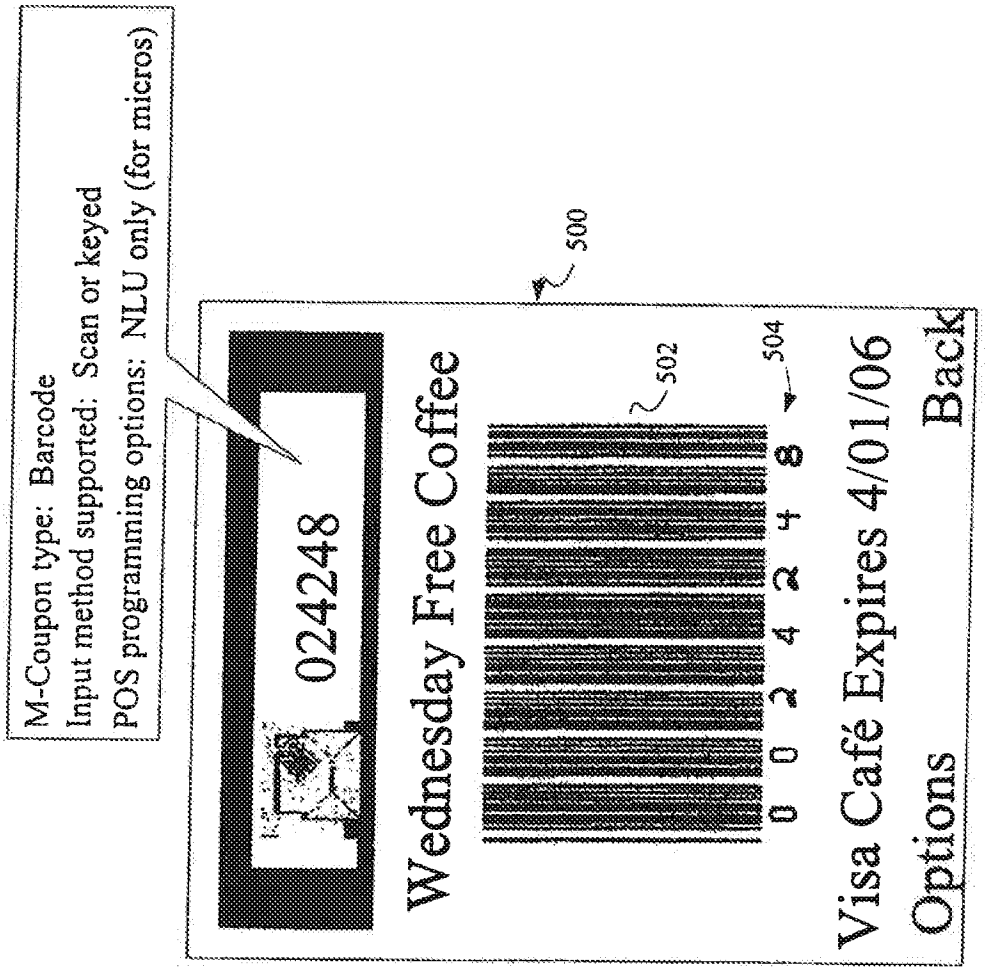

M-Coupon type: Barcode
Input method supported: Scan or keyed
POS programming options: NLU only (for micros)
024248
Wednesday Free Coffee
500
502
504
0 0 2 4 2 4 8
Visa Café Expires 4/01/06
Options
Back

FIG. 5A

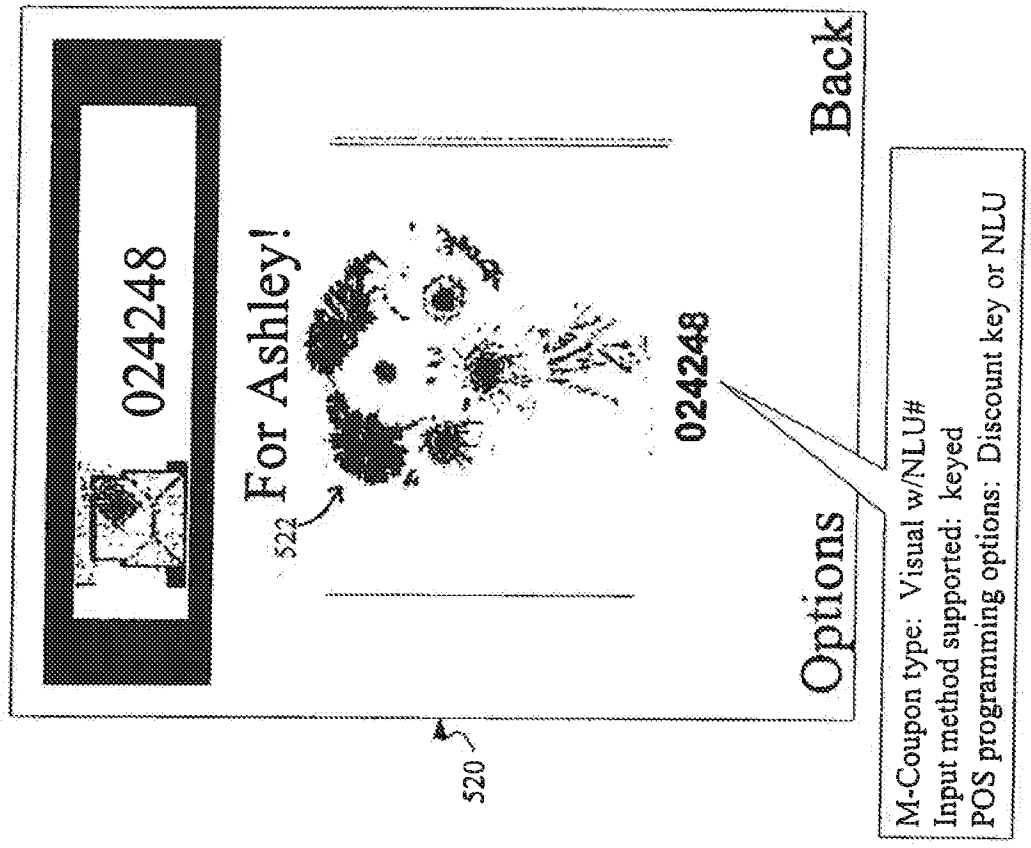

024248
For Ashley!
522
024248
Back
Options
520
M-Coupon type: Visual w/NLU#
Input method supported: keyed
POS programming options: Discount key or NLU

FIG. 5B

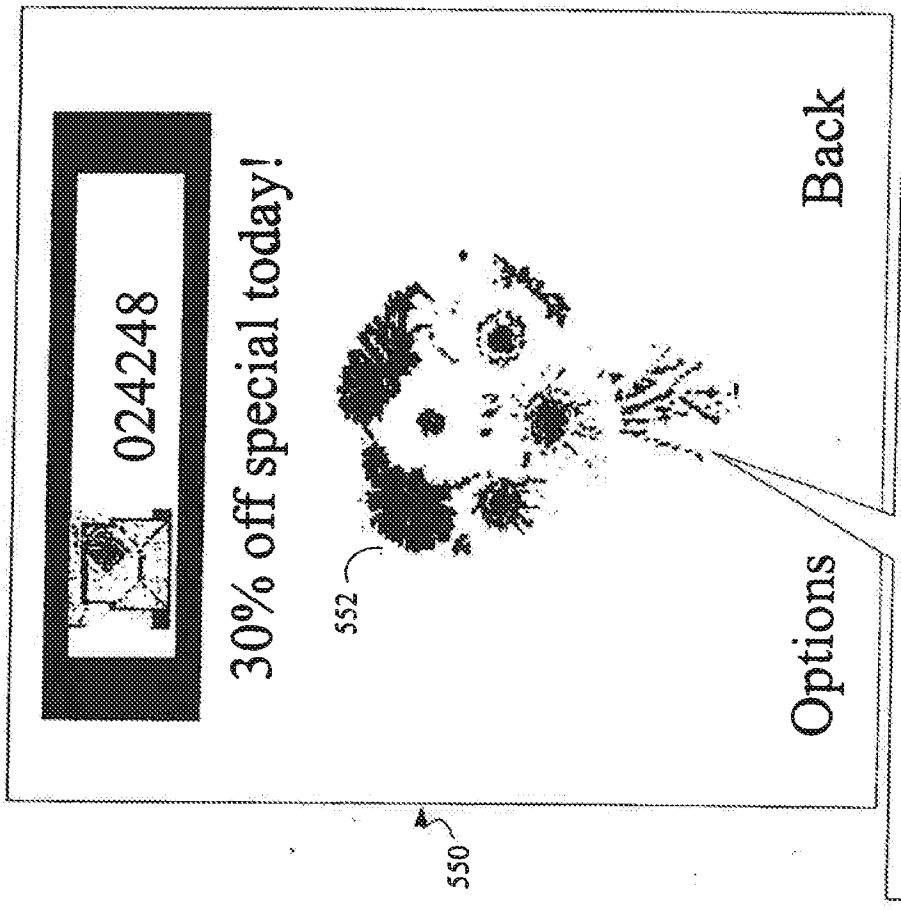


FIG. 5C

Petitioner Exhibit 1002-0692

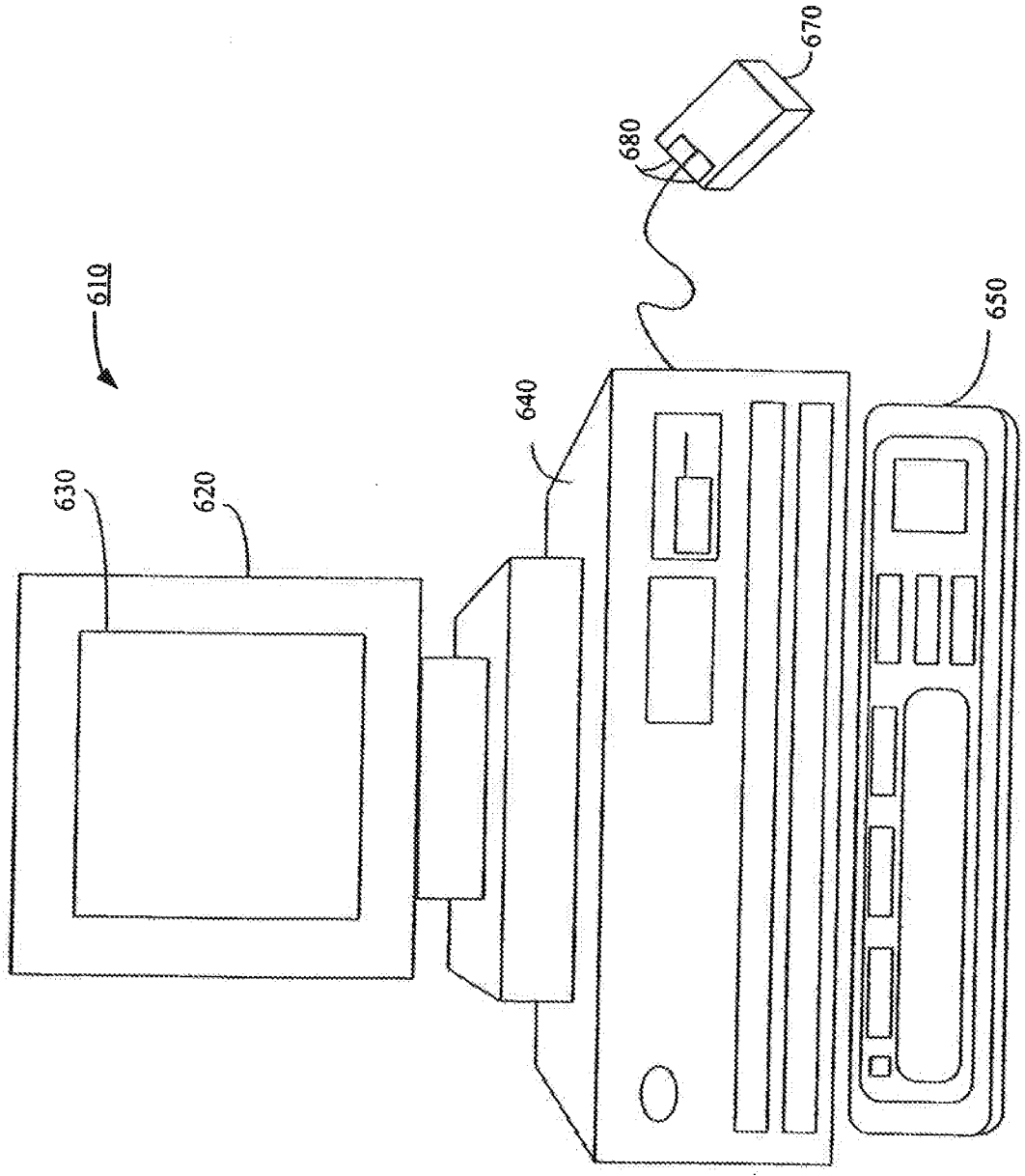


FIG. 6

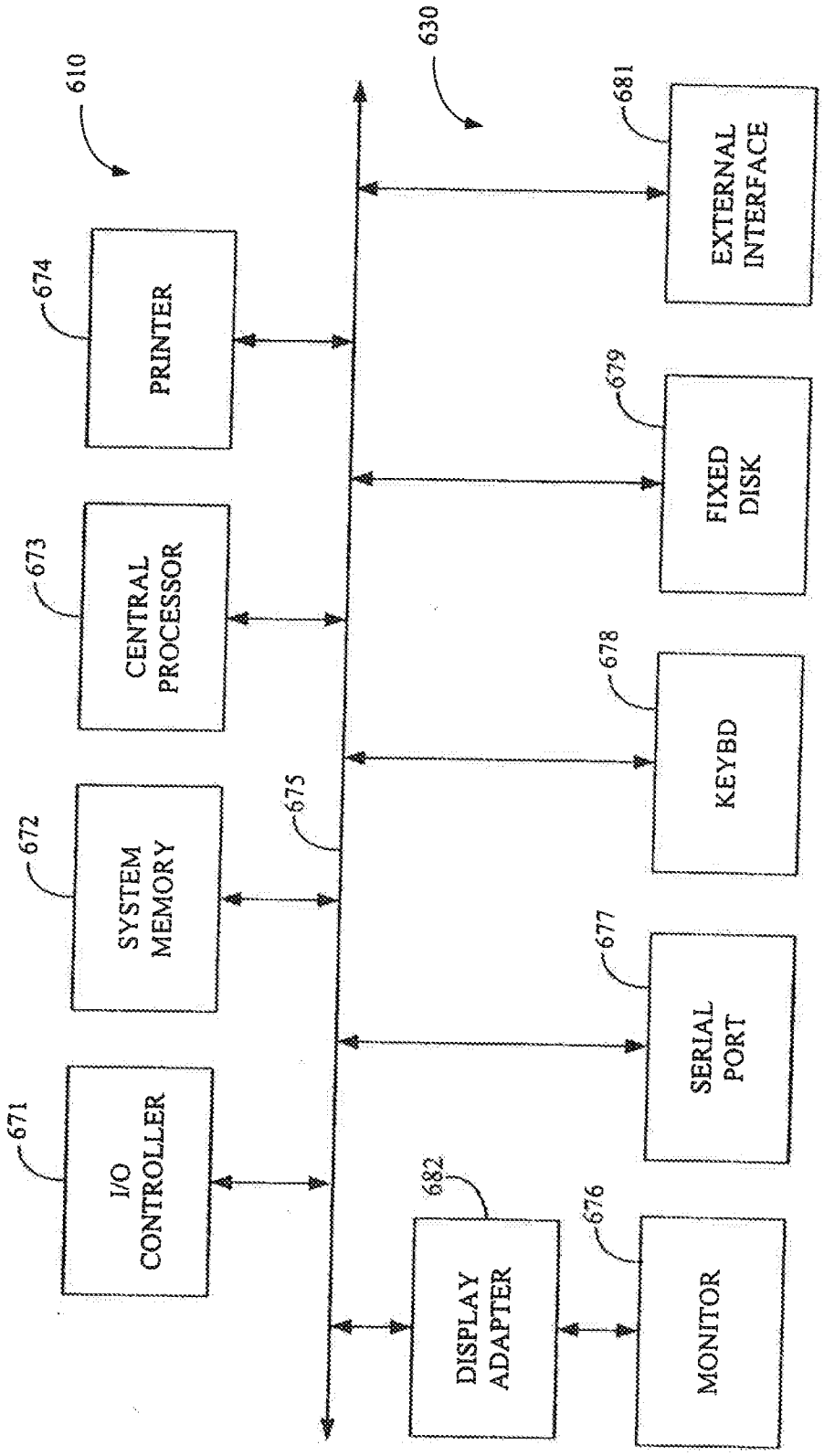

610
630
681
EXTERNAL INTERFACE
674
PRINTER
679
FIXED DISK
673
CENTRAL PROCESSOR
678
KEYBD
672
SYSTEM MEMORY
675
677
SERIAL PORT
671
I/O CONTROLLER
682
DISPLAY ADAPTER
676
MONITOR

FIG. 6A

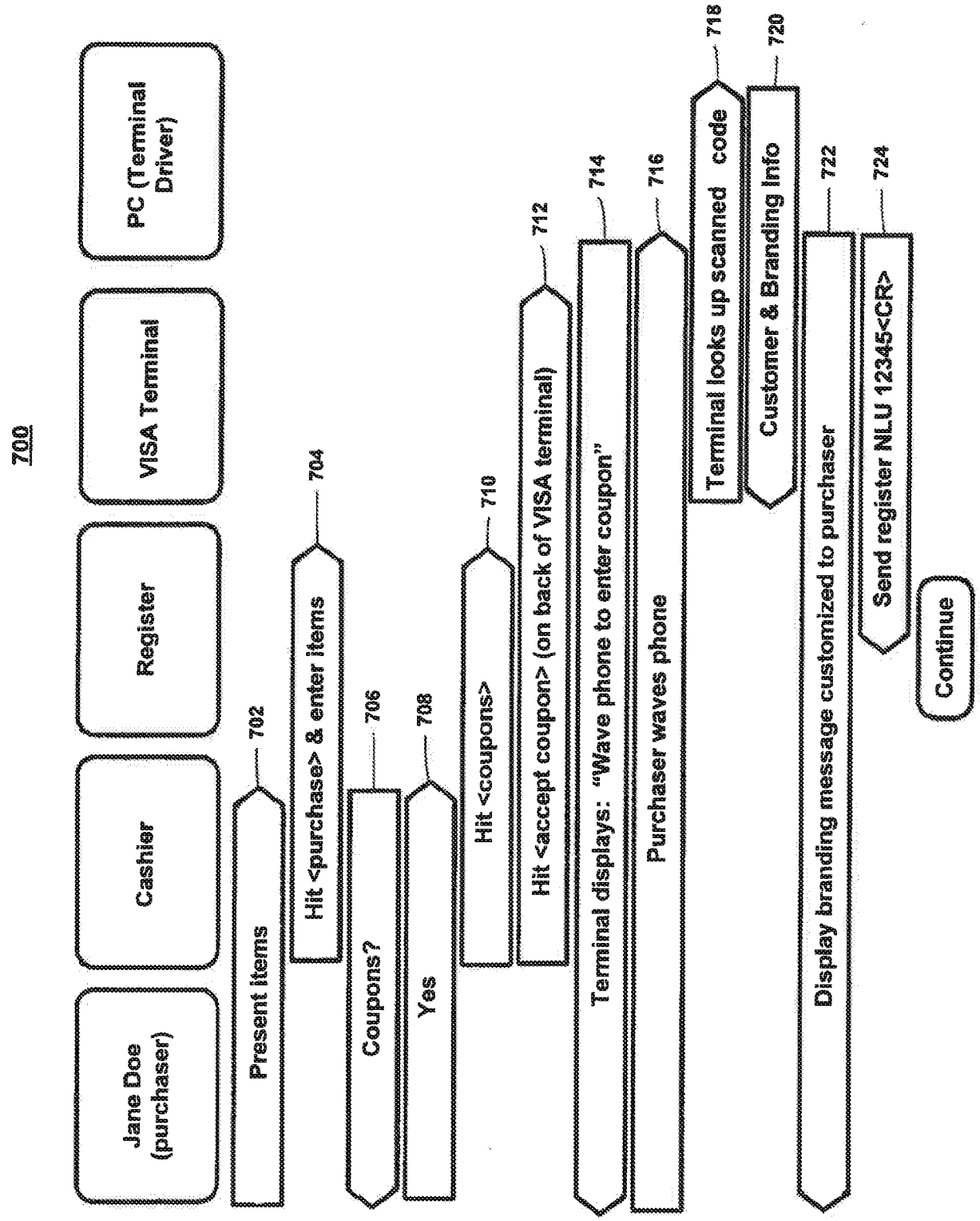


FIG. 7

Petitioner Exhibit 1002-0695

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 07/88687

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 30/00 (2008.04)
USPC - 705/14
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
USPC - 705/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC - 705/1; 705/37; 705/60; 707/104.1; 709/217

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WEST(USPAT, USPUB, EPO, JPO, DERWENT) DialogPRO(Engineering); Google Scholar - payment and processing and network and generate and electronic and coupon and targeted and individual and consumer

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2004/0030607 A1 (Gibson) 12 February 2004 (12.02.2004), para [0011],[0018],[0006].	1-24
Y	US 2003/0004808 A1 (Elhaoussine et al.) 02 January 2003 (02.01.2003), para [0021],[0022],[0035],[0099].	1-24
A	US 2006/0282382 A1 (Balasubramanian et al.) 14 December 2006 (14.12.2006), entire document.	1-24
A	US 2006/0253390 A1 (McCarthy et al.) 09 November 2006 (09.11.2006), entie document.	1-24
A	US 2006/0224449 A1 (Byerley et al.) 05 October 2006 (05.10.2006), entire document.	1-24
A	US 2006/0149529 A1 (Nguyen et al.) 06 July 2006 (06.07.2006), entire document.	1-24

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 March 2008 (29.03.2008)	12 MAY 2008

Name and mailing address of the ISA/US	Authorized officer:
Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (April 2007)

Petitioner Exhibit 1002-0696

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 July 2008 (10.07.2008)

PCT

(10) International Publication Number
WO 2008/083119 A1

(51) International Patent Classification:
G06Q 40/00 (2006.01)

(21) International Application Number:
PCT/US2007/088704

(22) International Filing Date:
21 December 2007 (21.12.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/871,898 26 December 2006 (26.12.2006) US

(71) Applicants *(for all designated States except US)*: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; 900 Metro Center Boulevard, Foster City, California 94404 (US). **VISA U.S.A. INC.** [US/US]; P.O. Box 8999, M3-2B, San Francisco, California 94128 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CARLSON, Mark** [US/US]; 153 Miramonte Avenue, Half Moon Bay, California 94019 (US). **HAMMAD, Ayman** [US/US]; 6048 Corte Montanas, Pleasanton, California 94566 (US). **FAITH, Patrick** [US/US]; 2810 Jones Gate Court, Pleasanton, California 94566 (US).

(74) Agents: **MARTINEZ-LEMKE, Sheila P.** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, 8th Floor, San Francisco, California 94111 (US).

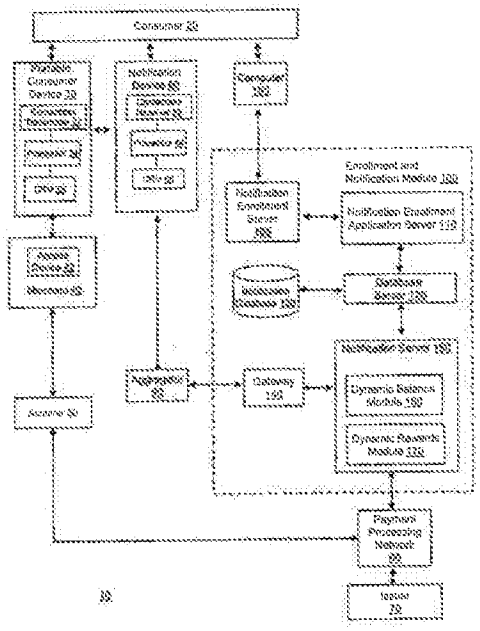
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: REAL-TIME BALANCE UPDATES



(57) Abstract: A method and a system that receive retrieve dynamic data when a notification with dynamic data is triggered. The dynamic data is associated with an account that is associated with a portable consumer device associated with a consumer. The method and system automatically send the notification with the dynamic data to a notification device, wherein the notification with

Petitioner Exhibit 1002-0697

WO 2008/083119 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

Petitioner Exhibit 1002-0698

REAL-TIME BALANCE UPDATES

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This is a non-provisional patent application of and claims the benefit of the filing date of U.S. Provisional Patent Application No. 60/871,898 filed on December 26, 2006. This application is herein incorporated by reference in its entirety for all purposes.

BACKGROUND

[0002] Some prior systems send consumers notices regarding current transactions. For example, an issuer may notify a consumer when their credit card is being used to make a large purchase. These prior systems often rely on contact information in the account information to notify the consumer. If, for example, only the consumer's home address is on file, the notice may not get to the consumer until well after the transaction has been completed.

[0003] Consumers with prepaid cards may want to know the balance left on their prepaid cards before a transaction or as soon as a transaction is completed. For example, a consumer may want to know whether they can afford to purchase a product with the prepaid card before they check out or even before they go to the store. Typically, a consumer contacts the issuer of their prepaid card such as a bank to determine their current balance on the prepaid card. In some cases, however, a prepaid card e.g. gift card may not be associated with an account with an issuer such as those cards purchased at retail stores. The consumer may not easily be able to get their current balance.

[0004] Embodiments of the present disclosure address these and other problems, individually and collectively.

SUMMARY OF THE INVENTION

[0005] Embodiments of the invention relate to automatic notifications, methods of providing and requesting automatic notifications, and systems that provide automatic notifications.

[0006] Embodiments of the invention address the above-noted problems by providing methods and systems of providing notifications with dynamic data to the

Petitioner Exhibit 1002-0699

consumer. Dynamic data refers to information that reflects all transactions on a portable consumer device made through the time a notification is triggered. An example of dynamic data is a real-time updated account balance. Examples of dynamic data include real-time updated account balance and a real-time updated rewards information associated with an account on a portable consumer device. When triggered, a notification with dynamic data is sent to the notification device e.g. cellular phone. The notification can be triggered on a periodic basis or when the consumer uses their portable consumer device to make a transaction. The notification can also be triggered when the consumer requests the dynamic data. For example, consumer could request dynamic data by placing their portable consumer device next to their notification device so that a transmitter in the portable consumer device sends a request to a receiver in the notification device. The consumer could also request the dynamic data by selecting a programmed key on their notification device. Dynamic data is then delivered to the notification device and provided to the consumer if the consumer is enrolled to receive the notification.

[0007] An embodiment of the invention is directed to a method that retrieves when a notification with dynamic data is triggered. The dynamic data is associated with an account associated with a portable consumer device associated with a consumer. The method also automatically sends the notification to the notification device, wherein the notification with dynamic data is provided to the consumer.

[0008] Another embodiment of the invention is directed to a method that triggers a notification with dynamic data using a notification device. The dynamic data is associated with an account on a portable consumer device associated with a consumer. The method also receives the notification on the notification device.

[0009] Another embodiment of the invention is directed to a system that includes a payment processing network for generating and storing dynamic data and a notification server coupled to the payment processing network. The notification server is configured to retrieve the dynamic data from the payment processing network when a notification with dynamic data is triggered. The dynamic data is associated with an account associated with a portable consumer device associated with a consumer. The notification server is also configured to automatically send the

notification with the dynamic data to the notification device, wherein the notification with dynamic data is provided to consumer.

[0010] Another embodiment of the invention is directed to a phone having a processor, a receiver coupled to the processor, an output device coupled to the processor, and a computer readable medium coupled to the processor. The computer readable medium includes code for displaying a notification including dynamic data to the output device after a portable consumer device is used by a consumer.

[0011] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. 1 is a block diagram illustrating a dynamic data notification system, in accordance with an embodiment of the invention.

[0013] FIG. 2 is a flow chart illustrating a method of providing dynamic data notifications, in accordance with an embodiment of the invention.

[0014] FIG. 3 is a schematic drawing of a cellular phone displaying a real-time balance update, in accordance with an embodiment of the invention.

DETAILED DESCRIPTION

[0015] Embodiments of the invention are directed to a method of providing notifications with dynamic data, a method of requesting notifications with dynamic data, and a dynamic data notification system. More specifically, a notification with dynamic data is triggered when the consumer requests the notification or when the consumer uses the portable consumer device. The consumer can also have notifications automatically sent to the notification device on a periodic basis. Once the notification is triggered, dynamic data is retrieved and delivered to the notification device if the consumer is enrolled to receive the notification.

[0016] Certain embodiments of the invention may provide one or more technical advantages to issuers and consumers. One technical advantage to a consumer may be knowing their current balance or rewards available on their card without having to

contact the issuer which could save time and could save the consumer money. Another technical advantage to a consumer may be that the consumer can request the current balance left on their card so that they can determine whether they have sufficient funds or credit to make a purchase or complete a transaction. A technical advantage to an issuer may be that automatic notifications are sent to consumers and issuer does not have to provide notifications by other means.

[0017] Certain embodiments of the invention may include none, some, or all of the above technical advantages. One or more other technical advantages may be readily apparent to one skilled in the art from the figures, descriptions, and claims included herein.

[0018] **FIG. 1** is a block diagram illustrating a dynamic data notification system **10**, in accordance with an embodiment of the invention. Dynamic data notification system **10** includes a consumer **20**, a portable consumer device **30**, a merchant **40**, an acquirer **50**, a payment processing network **60**, an issuer **70**, a notification device **80**, an aggregator **90**, an enrollment and notification module **100**, and a computer **190**. Although one consumer **20**, one portable device **30**, one merchant **40**, one acquirer **50**, one issuer **70**, one notification device **80**, and one computer **190** are shown, there may be any suitable number of any of these entities in dynamic data notification system **10**.

[0019] Dynamic data notification system **10** includes a consumer **20** in operative communication with portable consumer device **30**. Dynamic data notification system **10** also includes a merchant **40** having an access device **42** for interacting with portable consumer device **30** and an acquirer **50** associated with merchant **40**. Acquirer **50** is in communication with issuer **70** through payment processing network **60**.

[0020] Dynamic data notification system **10** also includes a notification device **80** in operative communication with consumer **20** for displaying notifications to consumer **20** and for receiving request or instructions for notifications from consumer **20**. Notification device **80** is also in communication with portable consumer device **30** for receiving a request for a notification from consumer **20**.

[0021] Dynamic data notification system **10** also includes an enrollment and notification module **100** for processing notifications and an aggregator **90** for

collecting and forwarding notifications from enrollment and notification module **100** to notification device **80**. Dynamic data notification system **10** also includes a computer **190** in communication with enrollment notification module **100** and consumer **20**. Consumer can use computer **190** to receive notifications and to enroll in notifications. Dynamic data notification system **10** also includes a payment processing network **60** that is in communication with enrollment and notification module **100**, with acquirer **50**, and with issuer **70**.

[0022] Consumer **20** refers to an individual or organization such as a business that is capable of purchasing goods or services or making any suitable transaction with merchant **40**.

[0023] Portable consumer device **30** refers to any suitable device that allows the transaction to be conducted with merchant **40**. Portable consumer device **30** may be in any suitable form. For example, suitable portable consumer devices **30** can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). They may include smart cards, magnetic stripe cards, keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. Other examples of portable consumer devices **30** include cellular phones, personal digital assistants (PDAs), pagers, payment cards, security cards, access cards, smart media, transponders, and the like. In some cases, portable consumer device **30** may be associated with an account of consumer **20** such as a bank account.

[0024] In the illustrated example, portable consumer device **30** includes a contactless transmitter **32** for sending wireless signals, a processor **34**, and a computer readable medium (CRM) **36**. These elements of portable consumer device **30** are in communication with each other. Processor **34** (e.g., a microprocessor) processes the functions of portable consumer device **30**.

[0025] Contactless transmitter **32** refers to any suitable device for sending wireless signals with information stored in memory (e.g. CRM **36**) on portable consumer device **30** to notification device **80**. Contactless transmitter **32** transmits signals using a near field communications (NFC) capability to send information from portable consumer device **30** to the contactless receiver **82** on notification device **82**. Typically, NFC capability is in accordance with a standardized protocol or data

transfer mechanism (e.g., ISO 14443/NFC). Some examples of NFC capability are radio-frequency identification (RFID), Bluetooth™, infra-red, and other suitable communications capability. In other embodiments, contactless transmitter **32** transmits information via a cellular network by means of an interface (not shown). The interface functions to permit exchange of data between the cellular network (not shown) and contactless transmitter **32**.

[0026] CRM **36** may be on the body of portable consumer device **30**. The body may in the form of a plastic substrate, a housing, or other structure. CRM **36** may be a memory that stores data and may be in any suitable form. Exemplary CRM **36** may be in any suitable form including a magnetic stripe, a memory chip, etc. If portable consumer device **30** is in the form of a card, it may have an embossed region (ER) which is embossed with a PAN (primary account number). CRM **36** may electronically store the PAN as well as other data such as PIN data.

[0027] Merchant **40** refers to any suitable entity or entities that makes a transaction with consumer **20**. Merchant **40** may use any suitable method to make the transaction. For example, merchant **40** may use an e-commerce business to allow the transaction to be conducted by merchant **40** through the Internet. Other examples of merchant **40** include a department store, a gas station, a drug store, a grocery store, or other suitable business.

[0028] Access device **42** may be any suitable device for communicating with merchant **40** and for interacting with portable consumer device **30**. Access device **42** can be in any suitable location such as at the same location as merchant **40**. Access device **42** may be in any suitable form. Some examples of access devices **42** include POS devices, cellular phones, PDAs, personal computers (PCs), tablet PCs, handheld specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, websites, and the like. Access device **42** may use any suitable contact or contactless mode of operation to send or receive data from portable consumer devices **30**.

[0029] If access device **42** is a POS terminal, any suitable POS terminal may be used and may include a reader, a processor, and a computer readable medium. Reader may include any suitable contact or contactless mode of operation. For

example, exemplary card readers can include radio frequency (RF) antennas, optical scanners, bar code reader, magnetic stripe readers, etc. to interact with portable consumer device **30**.

[0030] Acquirer **50** refers to any suitable entity that has an account with merchant **40**. In some embodiments, issuer **70** may also be acquirer **50**.

[0031] Issuer **70** refers to any suitable entity that may open and maintain an account associated with portable consumer device **30** for consumer **20**. Some examples of issuers may be a bank, a business entity such as a retail store, or a governmental entity. In many cases, issuer **70** may also issue portable consumer device **30** associated with the account to consumer **20**.

[0032] Payment processing network **60** refers to a network of suitable entities that have information related an account associated with portable consumer device **30**. This information includes data associated with the account on portable consumer device **30** such as profile information, dynamic data, and other suitable information. Dynamic data refers to any suitable information that is updated to reflect the transactions made using portable consumer device **30**.

[0033] Although not shown in the illustrated embodiment, payment processing network **60** may have or operate a server computer and may include a database. The database may include any hardware, software, firmware, or combination of the preceding for storing and facilitating retrieval of information. Also, the database may use any of a variety of data structures, arrangements, and compilations to store and facilitate retrieval of information. The server computer may be coupled to the database and may include any hardware, software, other logic, or combination of the preceding for servicing the requests from one or more client computers. Server computer may use any of a variety of computing structures, arrangements, and compilations for servicing the requests from one or more client computers. In one embodiment, the server computer may be a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. Server computer services the requests of one or more client computers.

[0034] Payment processing network **60** may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network **60** may include VisaNet™. Networks that include VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services. Payment processing network **60** may use any suitable wired or wireless network, including the Internet.

[0035] Notification device **80** refers to any suitable device for receiving notifications and for providing the notifications to consumer **20**. Notifications refer to communications of dynamic data to consumer **20** on notification device **80**. Notifications may be in any suitable form and may be delivered by any suitable method. Some examples of notifications includes a phone call, a voice message, a voicemail message, a short message service (SMS) message e.g. a text message, an instant messaging (IM) message, or an email message, or a periodically updated display on a device. An exemplary embodiment of a notification is a real-time balance update. The real-time balance update is a communication to notify consumer **20** of the funds available (balance) on portable consumer device **30** after the last transaction is accounted for. Another embodiment of a notification is real-time rewards information update that is a communication to notify consumer **20** of rewards available for redemption after the last transaction.

[0036] Dynamic data refers to any suitable information that reflects all transactions on a portable consumer device **30** made through the time a notification of the dynamic data is triggered. Dynamic data relates to an account associated with a portable consumer device **30** associated with consumer **20**. For example, dynamic data can be account balances such as credit card account balances, stored value account balances, rewards balances, checking account balances, savings account balances, investment account balances, brokerage account balances, and other suitable account balances.

[0037] Notification device **80** may be in any suitable form. For example, suitable notification devices **80** can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). Some examples of notification device **80** include desktop or laptop computers, cellular phones (e.g., as shown in FIG. 3), personal digital assistants (PDAs), pagers, payment cards, security cards, access cards, smart media, transponders, and the like. In some embodiments, notification device **80** and portable consumer device **30** are embodied in the same device.

[0038] Notification device **80** includes a contactless receiver **82** for receiving wireless signals, a processor **84** coupled to the receiver **82**, and a computer readable medium (CRM) **36** coupled to processor **84**. Although not shown, notification device **80** may also include one or more input devices (e.g., keypads) or output devices (e.g., displays, speakers) coupled to processor **84**. Contactless receiver **82** refers to any suitable device for receiving wireless signals. The signals are received by contactless receiver **82** by any suitable method (e.g., using NFC capability). In one example, contactless receiver **82** receives a wireless signal with a request for a notification from contactless transmitter **32** of portable consumer device **30**. In another example, contactless receiver **82** receives a wireless signal with a notification(s) from aggregator **90** via a cellular network. Processor **84** (e.g., a microprocessor) processes the functions of notification device **80**. CRM **86** comprises code for processing requests for notifications, for receiving notifications, and for providing notifications to consumer **20**. An example of code for providing notifications to consumer **20** includes code for displaying notifications including dynamic data to an output device.

[0039] Consumer **20** uses computer **190** to receive notifications and/or enroll in a program to receive notifications. Computer **190** can be a desktop computer, a laptop computer, a cellular or mobile phone, a personal digital assistant (PDA), or other suitable device.

[0040] Enrollment and notification module **100** comprises a notification enrollment server **105**, a notification enrollment application server **110**, a database server **120**, a notification database **130**, a notification server **150** having a dynamic balance module **160** and a dynamic rewards module **170**, and a gateway **140**. Notification

enrollment server **105** in communication with a notification enrollment application server **110** which is in communication with database server **120** for storing and retrieving information to and from notification database **130**. Database server **120** is also in communication with notification server **150**. Notification server **150** is also in communication with gateway **140**, dynamic balance module **160**, and dynamic rewards module **170**. Although enrollment and notification module **100** is shown as being separate from issuer **70**, enrollment and notification module **100** can be at issuer **70** in some embodiments. In these embodiments, issuer **70** processes the notifications sent to notification device **80**.

[0041] Notification enrollment server **105** refers to a device that receives enrollment information from consumer **20** via computer **190** and sends the enrollment information to notification enrollment application server **110**. Notification enrollment application server **110** receives the enrollment information from consumer **20** through notification enrollment server **105** or from issuer **70** and may store the enrollment information in notification database **130**. Notification database **130** may receive and store new or updated enrollment information and other account information.

[0042] Enrollment information includes trigger information that describes the occurrences that must take place to trigger notifications and the types of dynamic data that consumer **20** wants to receive in the notifications. Consumer **20** may define the trigger information when enrolling in a program to receive notifications.

[0043] In some cases, notifications are triggered by actions taken by consumer **20** or another suitable entity. For example, a notification may be triggered by using of portable consumer device **30** at access device **42** by consumer **20** or by merchant **40**. In another example, a notification may be triggered by the sending of a request by consumer **20** for a notification using portable consumer device **30**, notification device **80**, computer **190**, or other suitable device. In yet another example, a notification may be triggered by placing portable consumer device **30** near notification device **80** so that a signal with a request for a notification is transmitted from contactless transmitter **32** on portable consumer device **30** to contactless receiver **82** on notification device **80**. In another example, a notification may be triggered by the completion of a transaction on an account associated with portable

consumer device **30**. In other cases, periodic notifications may be triggered by the termination a time period defined by consumer **20**. Examples of a time period include a week, a day, and an hour. For example, if consumer **20** selects the time period of a day, daily notifications will be sent to notification device **80**. Typically, daily notifications would be sent at approximately the same time every day.

[0044] Notification server **150** includes dynamic balance module **160** for processing notifications with dynamic balances and dynamic rewards module **170** for processing notifications with dynamic rewards information.

[0045] Notification server **150** processes notifications with dynamic data and sends the notifications through gateway **140** to aggregator **90**. If the dynamic data is a dynamic balance, dynamic balance module **160** processes the notification. If the dynamic data is dynamic rewards, dynamic rewards module **170** processes the notification. Gateway **140** is a any suitable device that converts information from the protocol or format used in enrollment and notification module **100** to those used in aggregator **90**. Aggregator **90** refers to any suitable entity or device that receives notifications, collects the notifications, and transmits the notifications to notification device **80** for consumer **20**. In some cases, aggregator **90** may be a wireless telephone company.

[0046] Notification server **150** is triggered to send a notification with dynamic data and processes the notification. Notification server **150** retrieves enrollment information with trigger information from notification database **130** using database server **120**. Notification server **150** confirms that consumer **20** is enrolled to receive the notification triggered based on the trigger information. Notification server **150** retrieves the dynamic data from issuer **70** or other suitable entity and sends the notification with the dynamic data through gateway **140** to aggregator **90**. Aggregator **90** collects notifications according to enrollment information and forwards the notifications to notification device **80**. If the notification triggered is associated with dynamic balance data, dynamic balance module **160** processes the notification. If the notification triggered is associated with dynamic rewards data, dynamic rewards module **170** processes the notification.

[0047] In one example embodiment, consumer **20** enrolls in a program using computer **190** to receive notifications on their notification device **80** (e.g. a cellular

phone) in the form of text or voice messages. Consumer **20** enrolls to receive notifications with the dynamic balance on the account associated with their portable consumer device **30** (e.g. a prepaid or gift card). Consumer **20** specifies that the notification will be sent every time portable consumer device **30** interacts with access device **42**.

[0048] In a typical payment transaction, consumer **20** uses portable consumer device **30** at access device **42** to purchase goods or services from merchant **40**. For example, a consumer may use a gift card with $50 to buy a $25 game cartridge at a toy store using a POS (point of sale) terminal at the toy store. The consumer may swipe the gift card through a slot in the POS terminal and the POS terminal may read data including an account number from the gift card.

[0049] An authorization request message is then forwarded to acquirer **50** and acquirer **50** forwards the message through payment processing network **60** to issuer **70**. Using portable consumer device **30** at access device **42** triggers notification server **150** to send a notification.

[0050] Issuer **70** determines whether or not to authorize the transaction. The transaction may be authorized if there are sufficient funds, and may be declined if there are insufficient funds. An authorization response message is then sent back through payment processing network **60** to acquirer **50** who forwards it to merchant **40**. At the end of the day, a normal clearing and settlement process can be conducted by payment processing network **60**. A clearing process is a process of exchanging financial details between and acquirer and an issuer to facilitate posting to a consumer's account and reconciliation of the consumer's settlement position.

[0051] In this example, the notification triggered is associated with a dynamic balance and dynamic balance module **160** processes the notification. Dynamic balance module **160** is triggered to send a notification when consumer used portable consumer device **30**. For example, dynamic balance module **160** may receive information that the previously described and registered gift card has been used to purchase a $25 game cartridge.

[0052] Dynamic balance module **160** retrieves enrollment information with trigger information from notification database **130** using database server **120**. Dynamic balance module **160** uses the trigger information to confirm that consumer **20** wants

to receive the notification that has been triggered. Dynamic balance module **160** also determines from the trigger information that consumer **20** wants to receive the triggered notification in the form of a text message. Dynamic balance module **160** retrieves the dynamic balance on the account associated with portable consumer device **30**. For example, the module **160** may determine that there is the balance on the gift card is $25. The dynamic balance will reflect the last transaction authorized including the transaction associated with the action of using portable consumer device **30** that triggered the notification. Dynamic balance module **160** sends a text message with the dynamic balance to notification device **80**. For example, the text message may indicate that the gift card now has a balance of $25 after buying the $25 game cartridge. Notification device **80** provides the text message to consumer **10**. For example, the consumer's phone may display the balance of $25 plus the account number associated with the gift card. Consumer **20** may thereafter store this information in the notification device **80** for future use in determining how much money is left on the portable consumer device **30**.

[0053] Modifications, additions, or omissions may be made to dynamic data notification system **10** without departing from the scope of the disclosure. The components of dynamic data notification system **10** may be integrated or separated according to particular needs. Moreover, the operations of dynamic data notification system **10** may be performed by more, fewer, or other system modules. Additionally, operations of dynamic data notification system **10** may be performed using any suitable logic comprising software, hardware, other logic, or any suitable combination of the preceding.

[0054] **FIG. 2** is a flow chart illustrating a method of providing dynamic data notifications, in accordance with an embodiment of the invention.

[0055] Consumer **20** enrolls in a program using computer **190** to receive notifications on their portable consumer device **30** (step **200**). Computer **190** sends enrollment information from consumer **20** to notification enrollment server **105**. Notification enrollment server **105** sends the enrollment information to notification enrollment application server **110**. Notification enrollment application server **110** sends the enrollment information to database server **120** to store it in notification database **130**.

[0056] A notification is triggered (step **210**). Notification server **150** detects that the notification has been triggered. Consumer **20** or other suitable entity triggers the notification.

[0057] In one embodiment, consumer **20** or other suitable entity triggers a notification by using portable consumer device **30** at access device **42**. In some cases, a notification is only triggered if the transaction is authorized and completed. When portable consumer device **30** is used, information indicating that a notification has been triggered is sent from access device **42** to acquirer **50** which forwards it to notification server **150** through payment processing network **60**.

[0058] In another embodiment, consumer **20** triggers a notification by requesting it on notification device **80** or computer **190** which forwards the request for a notification to notification server **150**. For example, consumer **20** may request a notification by selecting a programmed button on their cellular phone. The cellular phone sends the request to notification server **150**.

[0059] In another embodiment, consumer **20** triggers a notification by placing portable consumer device **30** next to notification device **80**. A signal with a request for a notification is emitted from contactless transmitter **32** in portable consumer device **30** and received by contactless receiver **82** on notification device **80**. Notification device **80** forwards the request to notification server **150**.

[0060] In yet another embodiment, a notification is triggered automatically on a periodic basis by notification server **150**. Typically, the notification is triggered at the end of the time period although any time during that time period can be used. Consumer **20** selects the time period such as daily, hourly, or weekly. For example, consumer **20** can select daily notifications sent at 12:00 a.m.

[0061] In one example embodiment, consumer **20** enrolls in a program using computer **190** to receive notifications on their notification device **80** e.g. cellular phone in the form of email messages. Consumer **20** enrolls to receive notifications with the dynamic balance on the account on their portable consumer device **30** e.g. a prepaid card. Consumer **20** specifies that the notification will be sent every time portable consumer device **30** interacts with access device **42**.

[0062] Notification server **150** retrieves enrollment information (step **220**) retrieved from notification database **130** using database server **120**. The enrollment information is associated with an account on portable consumer device **30**. In embodiments where consumer **20** requested the notification, notification server **150** may skip retrieving the enrollment information and checking enrollment for the notification (steps **220** and **230**) and go to retrieving dynamic data (step **240**).

[0063] Notification server **150** analyzes trigger information in the enrollment information to determine whether consumer **20** is enrolled to receive the notification that has been triggered (step **230**). If consumer **20** is not enrolled for the notification, the method ends (step **270**) and a notification is not sent to consumer **20**.

[0064] If consumer **20** is enrolled to receive the notification, notification server **150** retrieves the dynamic data (step **240**). Notification server **150** generates a notification with the dynamic data and sends it to aggregator **90** through gateway **140**. Aggregator **90** forwards the notification to notification device **160** for delivery to consumer **20** (step **250**). Notification device **80** provides the notification to consumer **20** (step **260**).

[0065] In one embodiment, the notification may be shown to consumer **20** on a screen on notification device **80**. The display of the notification may be a text message displayed on a screen or other suitable display until consumer **20** turns off the display. In other cases, the notification may be displayed for a predetermined period of time.

[0066] In another embodiment, the notification may be sent to consumer in the form of a voice message or voicemail message to consumer **20**. For example, the notification may be an automated voice announcement that is sent to the notification device **20**.

[0067] After providing the notification, the method ends (step **270**). Modifications, additions, or omissions may be made to the method without departing from the scope of the disclosure. The method may include more, fewer, or other steps. Additionally, steps may be performed in any suitable order without departing from the scope of the disclosure.

[0068] FIG. 3 is a schematic drawing of a cellular phone displaying a real-time balance update, in accordance with an embodiment of the invention. Notification device **80** includes a display **320** for displaying information such as notifications with dynamic data, buttons **330** for inputting information such as requests for notifications, a speaker (not shown) to send aural signals to consumer **20**, and a microphone (not shown) to receive aural signals from consumer **20**.

[0069] Display **320** includes a dynamic data display **322** for displaying the notification of the updated dynamic data consumer **20**. In the illustrated example, dynamic data display **322** is showing the real-time balance update on the account associated with portable consumer device **30**. Dynamic data can be updated at any suitable time. Some examples of when the dynamic data is updated include when consumer requests the dynamic data, when consumer **20** uses portable consumer device **30**, or periodically.

[0070] Buttons **330** include a balance request button **334** for requesting a real-time balance update and a rewards request button **336** for requesting a real-time rewards information update. Display **320** also includes a balance request button indicator **324** indicating that selecting balance request button **334** will request a real-time balance update. Display **320** also includes a rewards request button indicator **326** indicating that selecting rewards request button **336** will request a real-time rewards information update.

[0071] In operation, consumer **20** selects balance request button **334** to display real-time balance update on dynamic data display **322**. The request is forwarded to notification server **150**. Notification server **150** retrieves the real-time balance from issuer **70** or other suitable entity over payment processing network **60**. Notification server **150** sends the real-time balance update to notification device **80** and notification device **80** displays the update to consumer **20**.

[0072] Modifications, additions, or omissions may be made to notification device **80** without departing from the scope of the disclosure. For example, notification device **80** and portable consumer device **30** may be integrated into the same device. Also, the components of notification device **80** may be integrated or separated according to particular needs. Moreover, the operations of notification device **80** may be performed by more, fewer, or other modules. Additionally, operations of notification

device **80** may be performed using any suitable logic comprising software, hardware, other logic, or any suitable combination of the preceding.

[0073] It should be understood that the present disclosure as described above can be implemented in the form of control logic using computer software in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement the present disclosure using hardware and a combination of hardware and software.

[0074] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0075] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0076] The above description is illustrative and is not restrictive. Many variations of the disclosure will become apparent to those skilled in the art upon review of the disclosure. The scope of the disclosure should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0077] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the disclosure.

WHAT IS CLAIMED IS:

1. A method comprising:

when a notification with dynamic data is triggered, retrieving the dynamic data associated with an account associated with a portable consumer device associated with a consumer; and

automatically sending the notification with the dynamic data to a notification device, wherein the notification with the dynamic data is provided to the consumer.

2. A method of Claim 1, wherein the dynamic data is a real-time balance update.

3. A method of Claim 1, wherein the dynamic data is a real-time rewards information update.

4. A method of Claim 1, further comprising:

retrieving enrollment information; and

confirming that consumer is enrolled to receive the notification based on the enrollment information.

5. A method of Claim 1,

wherein the notification is triggered by a transaction being conducted using a portable consumer device associated with the consumer, and

wherein the dynamic data is based on an amount of the transaction being conducted.

6. A method of Claim 1,

wherein the notification is triggered based on a time period predefined by the consumer,

wherein automatically sending the notification to the notification device includes periodically sending the notification to the notification device based on the predefined time period.

7. A method of Claim 1, wherein the notification is triggered by a request for the notification with dynamic data sent from the notification device.

8. A method of Claim 1, wherein the notification is triggered by a signal sent from a contactless transmitter on portable consumer device to a contactless receiver on the notification device.

9. A method of Claim 1, wherein the notification with dynamic data is provided to consumer on a display.

10. A method of Claim 1,

wherein the notification device is a phone, and

wherein the notification sent to the notification device includes at least one of a phone call, voicemail, SMS, IM, or email.

11. A method comprising:

triggering a notification with dynamic data using a notification device, the dynamic data associated with an account associated with a portable consumer device associated with a consumer; and

receiving the notification on the notification device.

12. A system comprising:

a payment processing network for generating and storing dynamic data; and

a notification server coupled to the payment processing network, the notification server configured to:

when a notification with dynamic data is triggered, retrieve the dynamic data from the payment processing network, the dynamic data associated with an account associated with a portable consumer device associated with a consumer;

automatically send the notification with the dynamic data to the notification device, wherein the notification with dynamic data is provided to consumer.

13. The system of Claim 12, wherein the notification server is further configured to:

retrieve enrollment information; and

confirm that consumer is enrolled to receive the notification based on the enrollment information.

14. The system of Claim 12,

wherein the notification is triggered by a transaction being conducted using a portable consumer device associated with the consumer, and

wherein the dynamic data is based on an amount of the transaction being conducted.

15. The system of Claim 12,

wherein the notification is triggered based on a time period predefined by the consumer, and

wherein automatically sending the notification to the notification device includes periodically sending the notification to the notification device based on the predefined time period.

16. The system of Claim 12, wherein the notification is triggered by a request for the notification with dynamic data sent from the notification device.

17. The system of Claim 12, wherein the notification is triggered by a signal sent from a contactless transmitter on portable consumer device to a contactless receiver on the notification device.

18. A phone, comprising:

a processor;

a receiver coupled to the processor;

an output device coupled to the processor; and

a computer readable medium coupled to the processor, the computer readable medium includes code for displaying a notification including dynamic data to the output device after a portable consumer device is used by a consumer.

19. The phone of Claim 18, wherein the dynamic data is a balance associated with the portable consumer device.

20. The phone of Claim 18, wherein the portable consumer device is a prepaid card.

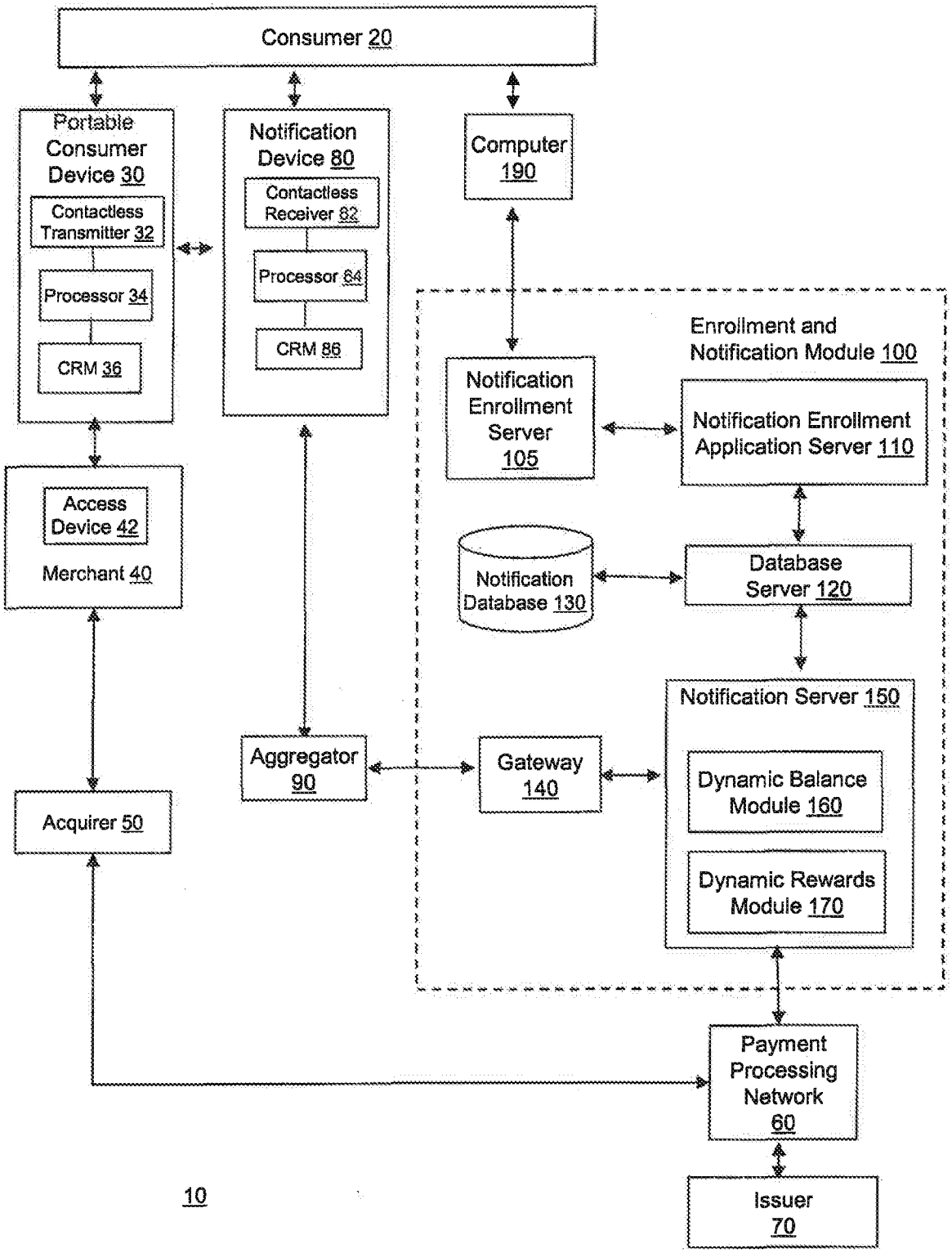

Consumer 20
Portable Consumer Device 30
Contactless Transmitter 32
Processor 34
CRM 36
Notification Device 80
Contactless Receiver 82
Processor 84
CRM 86
Computer 190
Enrollment and Notification Module 100
Notification Enrollment Server 105
Notification Enrollment Application Server 110
Access Device 42
Merchant 40
Notification Database 130
Database Server 120
Notification Server 150
Aggregator 90
Gateway 140
Dynamic Balance Module 160
Dynamic Rewards Module 170
Acquirer 50
Payment Processing Network 60
10
Issuer 70

FIG. 1

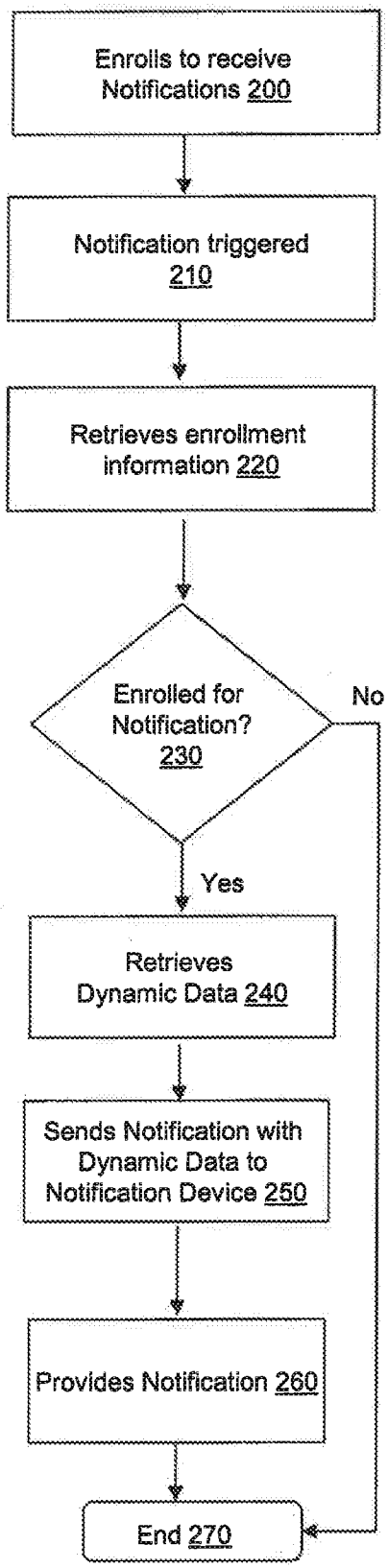

Enrolls to receive Notifications 200
Notification triggered 210
Retrieves enrollment information 220
Enrolled for Notification? 230
No
Yes
Retrieves Dynamic Data 240
Sends Notification with Dynamic Data to Notification Device 250
Provides Notification 260
End 270

FIG. 2

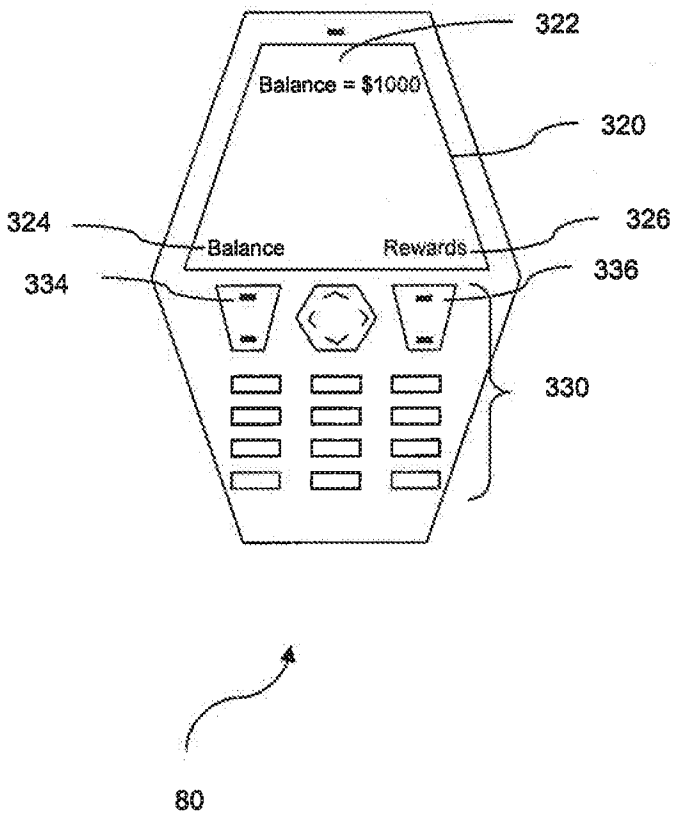


FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 07/88704

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 40/00 (2008.04)
USPC - 705/39
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
USPC: 705/39

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 705/35, 40 (see also text search below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Electronic Databases Searched: pubWEST, USPTO, Google, Answers.com, Google Patents
Search Terms Used: dynamic, data, rewards, information, portable, device, transaction, pay, notification, voicemail, email, SMS, cell phone, telephone, balance, computer, prepaid, card, realtime, transmit, contactless, dynamic, automatic

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 2006/0053056 A1 (ALSPACH-GOSS et al.) 09 March 2006 (09.03.2006) para [0006]-[0007], [0022], [0024]-[0025], [0027]-[0029], [0033], [0036]-[0037], [0050]-[0051], [0056]-[0058], [0069], [0071], [0077], [0091], [0103], [0109]-[0112], [0114], [0123], [0136], [0144], [0148], [0160], [0167], [0170], [0175], [0177] and [0179]	1-3, 5-12 and 14-20 4 and 13
Y	US 2005/0035847 A1 (BONALLE et al.) 17 February 2005 (17.02.2005) para [0057], [0063], [0083], [0085]), [0104] and [0124	4 and 13
A	US 2006/0248007 A1 (HOFER et al.) 02 November 2006 (02.11.2006)	1-20

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 May 2008 (25.05.2008)	11 JUN 2008

Name and mailing address of the ISA/US	Authorized officer:
Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Petitioner Exhibit 1002-0722

Electronic Patent Application Fee Transmittal

Application Number:	17654732
Filing Date:	14-Mar-2022
Title of Invention:	METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS
First Named Inventor/Applicant Name:	Paresh K. Patel
Filer:	Douglas James Crisman/vladimir skliba
Attorney Docket Number:	104402-5065-US

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	130	130
		Total in USD ($)		**130**

Electronic Acknowledgement Receipt

EFS ID:	46452482
Application Number:	17654732
International Application Number:	
Confirmation Number:	5715
Title of Invention:	METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS
First Named Inventor/Applicant Name:	Paresh K. Patel
Customer Number:	24341
Filer:	Douglas James Crisman/vladimir skliba
Filer Authorized By:	Douglas James Crisman
Attorney Docket Number:	104402-5065-US
Receipt Date:	21-AUG-2022
Filing Date:	14-MAR-2022
Time Stamp:	08:29:32
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$130
RAM confirmation Number	E20228K930222641
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Petitioner Exhibit 1002-0725

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		104402_5065_US_IDS.pdf	1427930 de7f7d953c0c61a70f4a0730223d456fc11d4799	yes	15
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Transmittal Letter		1	4	
	Information Disclosure Statement (IDS) Form (SB08)		5	15	
Warnings:					
Information:					
2	Foreign Reference	CN105139196A.pdf	1402400 c7bd0f7820809e11c8def3bd6935aed3b933421f	no	20
Warnings:					
Information:					
3	Foreign Reference	EP1571607A2.pdf	605193 318f239fa7451752c9f0abb596536e8ea0f61808	no	12
Warnings:					
Information:					
4	Foreign Reference	EP2061001A1.pdf	1305794 d81b1d327d20494cf9c844048fdb6a53abbdf1eb	no	18
Warnings:					
Information:					
5	Foreign Reference	JP2002183812A.pdf	714627 7b4d91f57e4e7521f65e53996734e415e64791aa	no	8
Warnings:					
Information:					

Petitioner Exhibit 1002-0726

6	Foreign Reference	JP2003242401A.pdf	2168857 7e887a7fba37919d334565743e51620e6a72538f	no	21
Warnings:					
Information:					
7	Foreign Reference	JP2003323662A.pdf	961837 54ac6c472f2ed7c1faac7fd0e06f82859cd98a2f	no	10
Warnings:					
Information:					
8	Foreign Reference	JP2004252640A.pdf	1079102 478d04d80bf7d397576cf507ef8ee598504bc512	no	15
Warnings:					
Information:					
9	Foreign Reference	JP2005526325A.pdf	1076999 8c32bf720d1938bd4ed7a38ebc6eff1f4cc73295	no	17
Warnings:					
Information:					
10	Foreign Reference	JP2009259226A.pdf	521454 5c15af7481782832e644ea1538e3fb7a7edc3b2b	no	17
Warnings:					
Information:					
11	Foreign Reference	JP2012504273A.pdf	10123009 fff7463ee84805385f54f30d6d9ca1e5d778a377	no	117
Warnings:					
Information:					
12	Foreign Reference	WO2003098561A1.pdf	1252625 5eab6664adb604b78d81104047d19b712a615020	no	32
Warnings:					
Information:					

13	Foreign Reference	WO2007015610A1.pdf	1643789 4bbb497e82f87cc1b4b6b57cca875f189a8e14c4	no	28
Warnings:					
Information:					
14	Foreign Reference	WO2008083022A1.pdf	1264198 bf9486a3da5eb7f63c85280a9a5ed4e8cfa33b58	no	27
Warnings:					
Information:					
15	Foreign Reference	WO2008083025A2.pdf	1450358 573253cba7275038782d8a9ac3260500bcf3c70e	no	30
Warnings:					
Information:					
16	Foreign Reference	WO2008083078A1.pdf	1592721 9742e9f7d0b2a1ec7c34058dda645bf239d07443	no	31
Warnings:					
Information:					
17	Foreign Reference	WO2008083089A1.pdf	1609765 0eac6d4ac3c96df20d3946a9d14a8b4fbfa8ee31	no	31
Warnings:					
Information:					
18	Foreign Reference	WO2008083105A2.pdf	1697058 678d19fb02946c27b67b613f343ee96713f4e536	no	35
Warnings:					
Information:					
19	Foreign Reference	WO2008083115A1.pdf	1666218 0041083c3bf32a4d787e949a23603d483345fe93	no	35
Warnings:					
Information:					

20	Foreign Reference	WO2008083119A1.pdf	1433009 538f7381d3339584c7473b89a00fca097376be00	no	26
Warnings:					
Information:					
21	Fee Worksheet (SB06)	fee-info.pdf	38125 aa83e9ceca1e952cf99070a78a3b61bd8a25902a	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	35035068		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronically filed August 21, 2022

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Paresh K. Patel	Confirmation No.:	5715
Serial No.:	17/654, 732	Art Unit:	3698
Filed:	March 14, 2022	Examiner:	Frantzy Poinvil
For:	Method and System for Presenting Representations of Payment Accepting Unit Events	Attorney Docket No.:	104402-5065-US

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure provisions of 37 C.F.R. §1.56, there is hereby provided certain information which the Examiner may consider material to the examination of the subject U.S. patent application. It is requested that the Examiner make this information of record if it is deemed material to the examination of the application.

1. Enclosures accompanying this Information Disclosure Statement are:

1a. ☒ A list of all patents, publications, applications, or other information submitted for consideration by the office.

1b. A legible copy of:

☒ Each foreign patent;

☒ Each publication or that portion which caused it to be listed on the PTO-1449;

☐ For each cited pending U.S. application, the application specification including the claims, and any drawing of the application, or portion of the application which caused it to be listed on the PTO-1449 including any claims directed to that portion;

☒ all other information or portion which caused it to be listed on the PTO-1449.

1c. ☒ An English language copy of search report(s) from a counterpart foreign application or PCT International Search Report.

1d. ☒ Explanations of relevancy (ATTACHMENT 1(d), hereto) or English language abstracts of the non-English language publications.

Petitioner Exhibit 1002-0730

2. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(b):

☐ Within three months of the filing date of a national application other than a continued prosecution application under §1.53(d);

☐ Within three months of the date of entry of the national stage as set forth in §1.491 in an international application;

☐ Before the mailing of the first Office action on the merits;

☐ Before the mailing of a first Office action after the filing of a request for continued examination under §1.114.

3. ☒ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(c) after the period specified in 37 C.F.R. §1.97(b), but before the mailing date of any of a final action under 37 C.F.R. §1.113, a notice of allowance under 37 C.F.R. §1.311 or an action that otherwise closes prosecution in the application.

(Check either Item 3a, 3b or 3c)

3a. ☐ The Certification Statement in Item 5 below is applicable. Accordingly, no fee is required.

3b. ☐ The $260.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. _____).

3c. ☒ The $130.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 104402-5065-US).

(Items 3b or 3c to be checked if any reference known for more than 3 months)

4. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(d) after the period specified in 37 C.F.R. §1.97(c), but on or before the date of payment of the issue fee.

(Check Item 4a, and 4b or 4c)

4a. ☐ The Certification Statement in Item 5 below is applicable.

4b. ☐ The $260.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. _____).

4c. ☐ The $130.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. _____).

5. ☐ Certification Statement (applicable if Item 3a or Item 4a is checked)

(Check either Item 5a, 5b, 5c or 5d)

Petitioner Exhibit 1002-0731

5a. ☐ In accordance with 37 C.F.R. §1.97(e)(1), it is certified that each item of information contained in this information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Information Disclosure Statement.

5b. ☐ In accordance with 37 C.F.R. §1.97(e)(2), it is certified that no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 C.F.R. §1.56(c) more than three months prior to the filing of this information disclosure statement.

5c. ☐ Each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

5d. ☐ Pursuant to 37 C.F.R. §1.704(d), each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

6. ☒ Copies of each cited U.S. patent and each U.S. patent application publication are not enclosed pursuant to the USPTO OG Notice dated 05 August 2003 waiving the requirement under 37 C.F.R. 1.98(a)(2)(i) for U.S. patent applications filed after June 30, 2003.

7. ☐ This application is a continuing application under 37 C.F.R. §1.53(b) or (d).

(Check appropriate Items 7a, 7b and/or 7c)

7a. ☐ A Petition to Withdraw from issue under 37 C.F.R. §1.313(b)(5) is concurrently filed herewith.

7b. ☐ Copies of publications listed on Form PTO-1449 from prior application Serial No. _____ filed _____, of which this application claims priority under 35 U.S.C. §120, are not being submitted pursuant to 37 C.F.R. §1.98(d).

7c. ☐ Copies of the publications listed on the attached Form PTO-1449 that were not previously cited in prior application Serial No. _____ filed _____, are provided herewith.

Petitioner Exhibit 1002-0732

8. ☐ This is a Supplemental Information Disclosure Statement. (Check Item 8a)

8a. ☐ This Supplemental Information Disclosure Statement under 37 C.F.R. §1.97(f) supplements the Information Disclosure Statement filed on . A bona fide attempt was made to comply with 37 C.F.R. §1.98, but inadvertent omissions were made. These omissions have been corrected herein. Accordingly, additional time is requested so that this Supplemental Information Disclosure Statement can be considered as if properly filed on .

9. ☐ In accordance with 37 C.F.R. §1.98, a concise explanation of what is presently understood to be the relevance of each non-English language publication is:

(Check Item 9a, 9b, or 9c)

9a. ☐ satisfied because all non-English language publications were cited on the enclosed English language copy of the PCT International Search Report or the search report from a counterpart foreign application indicating the degree of relevance found by the foreign office.

9b. ☐ set forth in the application.

9c. ☐ enclosed as an attachment hereto.

10. ☒ The Commissioner is authorized to charge any additional fee required or credit any overpayment for this Information Disclosure Statement and/or Petition to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 104402-5065-US).

11. ☒ No admission is made that the information cited in this Statement is, or is considered to be, material to patentability nor a representation that a search has been made (other than a search report of a foreign counterpart application or PCT International Search Report if submitted herewith). 37 C.F.R. §§1.97(g) and (h).

Respectfully submitted,

Date: August 21, 2022

/Douglas J. Crisman/ 39,951

Douglas J. Crisman (Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP
1400 Page Mill Road
Palo Alto, CA 94304
(650) 843-4000

DB2/ 43915760.1

Petitioner Exhibit 1002-0733

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 June 2009 (04.06.2009)

PCT

(10) International Publication Number
WO 2009/070430 A2

(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/US2008/082830

(22) International Filing Date:
7 November 2008 (07.11.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/030,845	22 February 2008 (22.02.2008)	US
61/050,904	6 May 2008 (06.05.2008)	US
61/060,755	11 June 2008 (11.06.2008)	US
60/986,534	8 November 2007 (08.11.2007)	US
60/992,029	3 December 2007 (03.12.2007)	US

(71) Applicant *(for all designated States except US)*: **SURIDX, INC.** [US/US]; 888 Worcester Street, Suite 260, Wellesley, MA 02482 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **SCHIBUK, Norman** [US/US]; 145 Fox Boulevard, Merrick, NY 11566 (US).

(74) Agents: **SUNSTEIN, Bruce, D.** et al.; Bromberg & Sunstein, LLP, 125 Summer Street, Boston, MA 02110 (US).

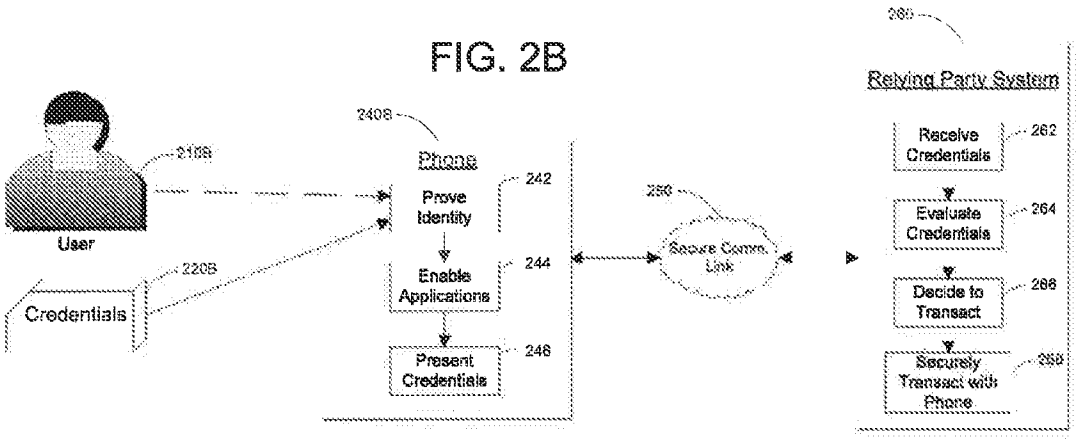
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

(54) Title: APPARATUS AND METHODS FOR PROVIDING SCALABLE, DYNAMIC, INDIVIDUALIZED CREDENTIAL SERVICES USING MOBILE TELEPHONES

FIG. 2B



(57) Abstract: Apparatus and methods perform transactions in a secure environment between an individual and another party, such as a merchant, in various embodiments. The individual possesses a mobile electronic device, such as a smartphone, that can encrypt data according to a public key infrastructure. The individual authenticates the individual's identity to the device, thereby unlocking credentials that may be used in a secure transaction. The individual causes the device to communicate the credentials, in a secure fashion, to an electronic system of a relying party, in order to obtain the relying party's authorization to enter the transaction. The relying party system determines whether to grant the authorization, and communicates the grant and the outcome of the transaction to the device using encryption according to the public key infrastructure.

WO 2009/070430 A2

Petitioner Exhibit 1002-0734

Attorney Docket: 3304/106WO

Apparatus and Methods for Providing Scalable, Dynamic, Individualized Credential Services Using Mobile Telephones

Priority

This application claims the benefit of the United States provisional patent applications having the following serial numbers and filing dates: 60/986,534 filed on November 8, 2007; 60/992,029 filed on December 3, 2007; 61/030,845 filed on February 22, 2008; 61/050,904 filed May 6, 2008; and 61/060,755 filed on June 11, 2008. Each of these applications is incorporated herein by reference in its entirety.

Technical Field

The present invention relates to apparatus and computer-implemented methods for distributed public key infrastructures (PKI). More specifically, the present invention relates to credential services, such as authenticating individuals and distributing data, using a distributed public key infrastructure, and includes in various embodiments the use of mobile telephones and flash memory to these ends.

Background Art

A public key infrastructure (PKI) provides a model through which electronic devices may authenticate themselves to each other and exchange encrypted messages. PKI is described in industry standards, for example International Telecommunication Union, *Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks*, hereby incorporated by reference. This standard is known as "X.509", and may be found on the Internet at http://www.itu.int/rec/T-REC-X.509/en. A PKI allows an individual to validate the public data of another individual, typically a public encryption key. The public key is distributed, via a computer network, in a certificate, and a cryptographic algorithm may be applied to ensure its accuracy. Certificates are described in Internet Engineering Task Force (IETF), *Request for Comments 3280: Internet X.509 Public*

Petitioner Exhibit 1002-0735

Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, hereby incorporated by reference, and which may be found at http://tools.ietf.org/html/rfc3280. Several companies, such as RSA Security, offer public key infrastructure software and services. Using a PKI, messages can be sent from one device to another without possibility of undetected alteration, so PKI systems are important in such diverse applications as electronic commerce, physical access systems, and secure communications.

However, present PKI systems suffer from a number of drawbacks. First, an organization (such as the Department of Defense) or business enterprise (such as IBM Corporation) may have thousands of locations and hundreds of thousands of employees. Quickly responding to authentication requests generally requires duplicating and distributing data to many servers and locations. The process of distributing data, and the resultant data availability at a number of sites, introduces security attack vectors. Second, as a practical matter this data model requires authenticating applications to be connected to a data network, potentially incurring high costs to provide connectivity. Third, enterprises may wish to communicate with each other. Trust may be developed differently within each enterprise, and one internal trust model may be different from the other. A party in one enterprise verifying a trust relationship within the other enterprise must use a foreign trust model, a potentially complex undertaking. Given certain PKI constraints, such as limitations on the length of a trust chain, it may be impossible to verify trust cross organizations under certain conditions. Also, each enterprise may need to query many different servers to obtain complete trust information, resulting in slow response times and high network traffic.

These drawbacks may be summarized by noting that the PKI deployment model currently in use does not efficiently serve the relationships and physical geometries of the participating parties to large numbers of authentication transactions. Current systems assume that an authenticating party can be in any place any time, requiring large amounts of bandwidth and large numbers of servers to move authentication data and validate it. This architecture does not scale, even in reasonably small use cases.

Summary of the Invention

The present invention addresses the aforementioned drawbacks, and a person skilled in the art may appreciate additional advantages. In accordance with embodiments of the

Petitioner Exhibit 1002-0736

invention, authentication data are protected by a distributed PKI. In a distributed PKI, authentication data are stored on an edge device, typically a mobile electronic device such as a cellular telephone or personal digital assistant (PDA). An individual needing authentication carries this edge device to its place of intended use. The individual presents authentication data directly to a relying party system over a short-range data network. Devices participating in a transaction need not access a remote validation service, saving bandwidth usage and response time. Further, authentication computations may be performed by each device participating in a transaction. Although the total number of computations may be large, spreading the workload to the edge devices decreases the computational power required by each device, bringing edge device hardware and software implementation requirements to practical levels. Increasing the number of devices in use proportionately increases the distribution of authentication data and computational power available, allowing the system to scale linearly. By employing data encryption between the edge device and the relying party system, the individual may enter secure transactions. The encryption keys used by each device may be validated using certificates, which themselves may be validated without access to a data network using cross-certificates and cached OCSP responses. The use of encryption prevents replay attacks against certificate data. By limiting the number of systems involved in any transaction to only two, the invention aids the establishment of trust models between individuals in two enterprises without requiring path discovery of foreign trust chains.

In a first embodiment of the invention there is provided a process for authenticating an individual to participate in a transaction with a relying party. The process includes producing a mobile electronic device, the device storing a digitally signed document containing a set of credential data, derived from a corresponding set of credentials, of the individual, and requiring, as a condition to using the stored set of credential data for authentication purposes, entry into the device of authentication data authenticating a would-be user of the device as the individual. The process further includes entering the authentication data into the device to authenticate the individual to the device, so that the individual can use the stored set of credential data, and also includes causing the device to communicate the set of credential data to a system of the relying party, for purposes of authenticating the individual to participate in the transaction.

Petitioner Exhibit 1002-0737

In related embodiments, the transaction includes: a purchase; receiving an extension of credit; obtaining access to money stored in a financial account; obtaining access to a physical location; obtaining access to a web page; obtaining access to a computing resource; obtaining access to data by downloading; receiving an HTTP cookie; or uploading medical data of the individual.

In some embodiments the mobile electronic device includes one of a smartphone and a personal digital assistant. The mobile electronic device may include WORM memory, as that term is defined below. The WORM memory may include a set of encryption data, the set having a private encryption key or private signature key of the individual. The mobile electronic device may have a display and an advertisement associated with an item in the set of encryption data, with the process further comprising displaying the advertisement on the display in connection with use of the device. The advertisement may be stored in the WORM memory.

In various related embodiments, the set of credential data is derived from one or more of: a passport, a birth certificate, a Transportation Worker Identification Credential (TWIC), a Common Access Card (CAC), a smartcard, a driver's license, a pilot's certificate, an identification card, an organization membership card, an insurance card, a credit card, a debit card, a store discount card, a public transportation card, or a library card. In other related embodiments, entering authentication data includes entering data pertaining to one of: a fingerprint, a handprint, a photograph, an iris scan, a retina scan, a password, an authorization code, or a personal identification number. Entering authentication data may include providing two-factor authentication data, for example a password and biometric data. The mobile electronic device may communicate by wireless communication. The system of the relying party may include one of: a vending machine, a parking meter, an electronic toll collection system, a physical access system, and a magnetic stripe reader.

In another related embodiment, a suite of applications is stored on the device, and the set of credential data identifies a subset of the suite of applications to be made available to the individual upon authentication of the would-be user as the individual. The process may be continued by causing the device to run an application loaded thereon, the application being unavailable for use until there has been entry into the device of authentication data authenticating the would-be user of the device as the individual.

Petitioner Exhibit 1002-0738

The process may also be continued in a related embodiment by receiving at the mobile electronic device, from the system of the relying party, a response to the communication of the set of credential data. Receiving the response may include receiving a verification of a credential in the set of credentials, or receiving a notification that the transaction has been completed. Receiving the response may also trigger updating a transaction log maintained on the mobile electronic device, and/or setting of an upload flag to enqueue uploading of data reflecting the transaction. In a related embodiment, the mobile electronic device includes a WORM memory, and the mobile device performs, on the WORM memory, an operation triggered by receiving the response. The operation may be storage of data related to the response, or rendering a portion of the WORM memory unreadable. Independently of receiving a response, causing the device to communicate the set of credential data may trigger storing, in a transaction log maintained on the mobile electronic device, a record having data related to the transaction.

In another embodiment there is provided a process for use by a relying party in authenticating an individual having a mobile electronic device to participate in a transaction with the relying party. As before, the device in this embodiment is storing a digitally signed document containing a set of credential data, derived from a corresponding set of credentials, of the individual and is requiring, as a condition to using the stored set of credential data for authentication purposes, entry into the device of authentication data authenticating a would-be user of the device as the individual. The process of this embodiment includes receiving, in a system in communication with the device, the digitally signed document from the device, wherein receipt of the digitally signed document constitutes verification of entry into the device of the authentication data. The process further includes using the system to evaluate a selected credential in the set of credentials, and storing data, associated with the transaction and the digitally signed document, in the system of the relying party in a transaction log.

In related embodiments, the transaction includes: a purchase; granting an extension of credit; providing access to money stored in a financial account; providing access to a physical location; providing access to a web page; providing access to a computing resource; providing access to data for downloading by the individual; or transmitting an HTTP cookie.

Petitioner Exhibit 1002-0739

In some embodiments the mobile electronic device includes one of a smartphone and a personal digital assistant. The mobile electronic device may include WORM memory, as that term is defined below. The WORM memory may include a set of encryption data, the set having a private encryption key or private signature key of the individual. In a related embodiment, using the system to evaluate the selected credential includes validating a digital signature of the digitally signed document, using a public signature key of the individual that forms a key pair with the private signature key of the individual.

In various related embodiments, the set of credential data is derived from one or more of: a passport, a birth certificate, a Transportation Worker Identification Credential (TWIC), a Common Access Card (CAC), a smartcard, a driver's license, a pilot's certificate, an identification card, an organization membership card, an insurance card, a credit card, a debit card, a store discount card, a public transportation card, or a library card. Furthermore, receiving the digitally signed document may include receiving the document wirelessly. In other related embodiments, using the system to evaluate the selected credential includes: validating a digital signature of the digitally signed document using a public signature key of the individual; comparing a digest derived from the credential data with a stored digest; comparing the time the digitally signed document was received from the device with a timestamp in the document; and/or obtaining a certificate status response from the mobile electronic device. The timestamp may be indicative of the time when credentials on the mobile electronic device were last updated or when the mobile electronic device was last connected to a network in a session meeting pre-specified criteria. Obtaining a certificate status response is accomplished in some embodiments by transmitting a first message including a cryptographic nonce to the mobile electronic device, the first message encrypted with a public encryption key of the individual; and receiving a second message including the nonce and the certificate status response from the mobile electronic device.

In a related embodiment, using the system to evaluate the selected credential includes communicating with a computer system, of a third party, that can validate the accuracy of the credential data or verify that the credential is unexpired. The third party may be an issuer of the selected credential or an agent of the issuer. Communicating may include receiving, from the third party, data indicating that the selected credential has not been revoked. The

Petitioner Exhibit 1002-0740

process may further include obtaining a certificate status response from the third party, or obtaining a certificate revocation list from the third party.

The process may be continued in another embodiment by transmitting, to the mobile electronic device, a message responsive to receipt of the digitally signed document. Transmitting may include transmitting data indicating that the selected credential in the set of credentials is valid and unexpired, or transmitting a notification that the transaction has been completed.

In another embodiment there is provided a mobile electronic device, usable by an individual for authentication of transactions. The device includes a storage module in which are stored a digitally signed document containing a set of credential data, derived from a corresponding set of credentials, of the individual, and authentication data of the individual. The device has a data entry arrangement for entering data into the device. The device further includes a controller, coupled to the storage module and the data entry arrangement, programmed to require, as a condition to using the stored set of credential data for authentication purposes, entry of the authentication data into the device via the data entry arrangement, so as to authenticate a would-be user of the device as the individual. The device also has a communication port for receiving and transmitting the digitally signed document.

In a related embodiment, the set of credentials includes a plurality of credentials of the individual, so that the device can be used to authenticate distinct classes of transactions, each class of transactions being associated with a distinct credential. In other related embodiments, the storage module includes non-volatile memory, WORM memory, or both WORM memory and WMRM memory incorporated in flash memory. In some of these embodiments, the WORM memory includes the digitally signed document or a set of encryption data, the set having a private encryption key of the individual or a private signature key of the individual.

In one embodiment of the device, the storage module includes an application stored therein, and the device also has a user control module restricting use of the application until there has been entry into the device, via the data entry arrangement, of the authentication data, to authenticate the would-be user of the device as the individual.

Petitioner Exhibit 1002-0741

In another embodiment there is provided a process for configuring an electronic device to be usable by an individual for authentication of transactions. The process includes storing a digitally signed document in the electronic device, the digitally signed document including credential data derived from a set of credentials pertaining to the individual. The process also includes storing, in the electronic device, authentication data associated with the individual. In this process, the device includes a user control module that precludes access to the credential data without entry into the device of the authentication data.

The set of credentials may include a physical credential. The physical credential may be selected from the group consisting of: a passport, a birth certificate, a Transportation Worker Identification Credential (TWIC), a Common Access Card (CAC), a smartcard, a driver's license, a pilot's certificate, an identification card, an organization membership card, an insurance card, a credit card, a debit card, a store discount card, a public transportation card, and a library card. In a related embodiment, the process is continued by receiving a physical credential from the individual, using the physical credential in manually determining that the set of credentials pertains to the individual, creating the digitally signed document, and entrusting the device to the individual. Alternatively or in addition, the set of credentials includes a virtual credential. The process may be continued by obtaining biometric data of the individual and including the biometric data in the authentication data.

In some embodiments, a digital signature in the digitally signed document is able to be validated using a public signature key of the individual or of a third party. In other, related embodiments, the process includes storing a private encryption key or private signature key of the individual in the electronic device. In yet another embodiment, the electronic device includes WORM memory, and storing the digitally signed document in the electronic device includes storing the document in the WORM memory.

In another embodiment there is provided a computer-implemented method of developing information pertinent to authentication of a set of credentials for each of a plurality of individuals, the set of credentials having a corresponding set of credential data derived from the set of credentials. This method includes, for each of the individuals, placing the individual's credential data in a digitally signed document, and storing the digitally signed document in a credential database. The method also includes, in a computer process, automatically and repetitively checking for revocation of any credentials in the

Petitioner Exhibit 1002-0742

credential database and, for any credentials revoked, storing data identifying such credentials.

Storing data identifying credentials that have been revoked may include updating the credential database, or storing in a revocation database a listing of credentials that have been revoked. Checking may be checking at least as often as once per day, or checking in conformity with a PKI standard. In a related embodiment, the method further includes, for each of the individuals, storing the digitally signed document in a token entrusted to the individual.

In another embodiment there is provided a computer-implemented method of authenticating a given individual's set of credentials, the set of credentials having a corresponding set of credential data derived from the set of credentials, each credential in the set having been authenticated as of a given time. This method includes receiving the set of credential data over a communications network, and in a computer process, using the credential data to compare the set of credentials against a database listing of revoked credentials to identify a credential in the set that has been revoked since the given time. Receiving the set of credential data may include receiving them from a federated data store, or uploading a digital document from a token in the possession of the given individual, the digitally signed document containing the individual's set of credential data. In a related embodiment, identifying credentials of the individual that have been revoked implicitly determines that all other credentials of the given individual have not been revoked. Further, comparing may be performed in a batch computer process.

In another embodiment there is provided a computer-implemented method of processing transactions between a relying party having a transaction system, and a set of individuals, each individual in the set of individuals having an electronic device capable of communication with the transaction system. The method includes obtaining access to a first digitally signed document created in the transaction system of the relying party, the document containing one or more transaction records, each transaction record having data pertaining to a selected transaction between the relying party and a selected individual in the set of individuals. The method next includes, for each selected transaction, (1) obtaining access to a second digitally signed document created in the electronic device of the selected individual, the document containing a transaction record corresponding to the selected

Petitioner Exhibit 1002-0743

transaction; and (2) in a computer process, checking for consistency between the transaction record in the first digitally signed document and the transaction record in the second digitally signed document.

The process may include validating a digital signature of the first digitally signed document, using a public signature key of the relying party. It may also include validating a digital signature of the second digitally signed document of the selected individual, using a public signature key of the selected individual. The process may also include, in the event that checking yields an inconsistency, communicating a warning to the relying party or the selected individual. Each transaction record may contain data pertaining to at least one of a transaction time, a transaction date, a purchase amount, a loan number, a financial account number, a physical location, an address of a web page, an identifier of a computing resource, a file name, an HTTP cookie name, and a medical condition. Obtaining access to the first digitally signed document may include receiving the first digitally signed document over a computer data network, and obtaining access to the second digitally signed document may include receiving the second digitally signed document over a computer data network. Checking may be performed in a batch computer process, or in a process substantially contemporaneously with the selected transaction.

Another embodiment of the invention provides a system enabling a second party to obtain data in a secure manner from a first party. The system has a receiving port for securely receiving the data, along with a digitally signed document associated with the first party and a reference to the second party. The system also has a physical data storage medium for storing the received data and the digitally signed document in association with the second party. The system includes a processor for verifying that the sender of the received data is the first party using the digitally signed document, and for determining whether to securely forward data stored in the storage area to the second party according to a rule associated with the first party and the second party. The system further has a transmitting port for forwarding the data to a computer facility of the second party. The storage area may be readable only by the first party and the second party, and it may be associated with a URL.

In another embodiment there is provided a computerized method enabling a second party to obtain data in a secure manner from a first party. The method includes receiving

Petitioner Exhibit 1002-0744

from the first party items including the data, a digitally signed document associated with the data and with the first party, and a reference to the second party. The method also includes verifying that the received data were sent by the first party, by using the digitally signed document. The method further includes storing the data in association with the digitally signed document and with the reference. The method also includes making the stored data available to the second party using the reference, such that the second party may securely access the data. The data may have been encrypted using a public key of the second party. Further, the items may be included in a message that has been encrypted using a public key associated with the receiver, where receiving the items includes receiving the message from the first party, and decrypting the message using a private key associated with the public key.

In a related embodiment, the reference includes at least one of a digital certificate, a telephone number, a postal address, and an electronic address. Making the stored data available may include encrypting a second message, containing the data and the digitally signed document, using a public key of the second party; and transmitting the encrypted second message to the second party. The storage space may be readable only by the first party and the second party. Receiving the data from the first party may include using a secure communications link.

In a further related embodiment, the method includes deciding whether to forward the data to the second party according to a set of computer-implemented rules associated with the first party and the second party. In another related embodiment, the method includes forwarding the data to the second party. Forwarding the data to the second party may include using a secure communications link.

In yet another related embodiment, receiving the items from the first party includes receiving the items through a communications gateway that is not dedicated to handling trusted data from a particular source. The communications gateway may also handle data other than trusted data. Verifying that the received data were sent by the first party may be accomplished by the communications gateway. If so, doing so may include accessing an authorized certificate store to retrieve a certificate of the first party. In a related embodiment, making the stored data available to the second party using the reference is accomplished by the communications gateway. Storing the data in association with the digitally signed document and with the reference may be caused by the communications gateway.

Petitioner Exhibit 1002-0745

In still another related embodiment, the method may include, upon receiving the items from the first party, initiating communication with the second party to obtain authorization to cause storage of the data. If the second party has a mobile telephone, making the stored data available to the second party may include sending a communication to the mobile telephone identifying the received data and seeking authorization to make the received data available to the second party, and, upon such authorization, making the received data available to the second party. Making the received data available to the second party may include making the data accessible to the mobile telephone for storage in memory thereof. This memory may be flash memory. The data may include information relating to a credential, and making the data accessible to the mobile telephone for storage in memory thereof includes making the data accessible for storage only in a portion of such memory configured as WORM memory. The WORM memory may be implemented in flash memory. In a related embodiment, the data are digital media content encrypted with a public key of the second party.

In another embodiment, there is provided a computerized method for creating a virtual smartcard for an individual based on a physical credential applicable to the individual. The method includes receiving, over a communications network, credential data derived from the physical credential and authentication data pertinent to the individual. It further includes using a computer process to establish a pair of cryptographic keys. The method also includes creating a virtual smartcard for the individual by storing the credential data and the authentication data in association with the pair of cryptographic keys. The physical credential may be selected from the group consisting of a passport, a birth certificate, a Transportation Worker Identification Credential (TWIC), a smartcard, a driver's license, a pilot's certificate, an identification card, an organization membership card, an insurance card, a credit card, a debit card, a store discount card, a public transportation card, and a library card. Authentication data may be selected from the group consisting of biometric data and a passcode.

In another embodiment, there is provided a method of evaluating a primary credential issued by an agency. This method includes using the primary credential to access from storage a summary certificate associated in the storage with the primary credential, the summary certificate containing a collection of secondary credentials considered by the

Petitioner Exhibit 1002-0746

agency in issuing the primary credential. The method also includes, in a revocation computer process, collecting secondary credential revocation information by (i) identifying each of the secondary credentials that is the subject of a revocation, and, (ii) for each revoked credential, accessing data that characterize a basis for the revocation. The method includes, in an evaluation computer process, applying a set of policy rules to the collected secondary credential revocation information to evaluate its effect on the primary credential.

In a related embodiment, the revocation computer process includes accessing a database of revoked credentials, the database established by automatic, computer-implemented, repetitive checking for revocation of secondary credentials of a plurality of individuals. In another related embodiment, one of the secondary credentials that is the subject of revocation is another primary credential that has been previously revoked by operation of computer processes, so that processes herein may spawn a cascade of revocations when permitted by policy rules to do so. Accessing data that characterize a basis for the revocation may include accessing data indicating that a chain of trust for a secondary credential has been broken. In a related embodiment, the method further includes revoking the primary credential when the policy rules being applied so require. In another related embodiment, the method further includes, in a further revocation computer process, identifying a set of additional primary credentials, the set having at least one member, for which the primary credential serves as a secondary credential in a corresponding set of summary certificates; and also includes, in a further evaluation computer process, subjecting the set of primary credentials to evaluation in a manner generally analogous to the evaluation computer process.

In another embodiment there is provided a computerized method for responding to a given individual's request for access. This method includes receiving, over a first communications network, a first data set defining rights of the given individual to access. The method further includes receiving, over a second communications network, from a token possessed by the given individual, a digitally signed document including a second data set defining rights of the given individual relating to the access. The method finally includes, in a computer process, comparing the first access rights data and the second access rights data to respond to the given individual's access rights.

Petitioner Exhibit 1002-0747

In related embodiments, receiving over the first communications network includes receiving data from a cellular telephone network or the Internet. In the latter case, a virtual private network may be employed. Receiving over the second communications network may include receiving data from a Bluetooth network. The token may be a smartphone. The method may further include validating a digital signature of the digitally signed document. In this case, validating the digital signature may include receiving data from the token pertaining to a digital certificate, the digital certificate having a public signature key. If so, the data may incorporate a cached OCSP response.

In yet another embodiment there is provided a non-volatile memory device encoded with computer-readable data, such device including a first portion thereof configured as WORM memory in which are encoded credential data and a second portion thereof configured as WMRM memory. The device may be encoded with computer-readable instructions, such instructions including program code defining a cryptographic engine. The credential data may relate to a plurality of credentials of an individual. The device may be implemented in flash memory.

In still another embodiment there is provided a method for efficiently authenticating an individual in connection with a transaction, at a physical transaction location, such location using a public key infrastructure and having a terminal for use in the transaction. The method includes using data provided over a cellular telephone network to estimate a present location of a smartphone of the individual on which is stored credential data relating to a credential of the individual, such smartphone requiring the individual to authenticate himself to the smartphone as a condition of use of the credential data. Next, if the present location is determined to be within a specified range of the physical transaction location, the method requires sending data as to status of the credential to the terminal, so that the individual will be able to present the credential for use in the transaction only by authenticating himself to the smartphone, and status information of the credential will be available to the terminal for use in connection with the transaction when the individual appears at the physical location. The embodiment may estimate a present location using base station data or using GPS data from the smartphone.

In another embodiment there is provided a method for gating communication to a user's smartphone from a caller's smartphone based on a set of pre-specified criteria as to

Petitioner Exhibit 1002-0748

attributes of the caller. This method includes receiving on the user's smartphone a control message from the caller's smartphone constituting a request to establish communication with the user's smartphone, such control message including a credential of the caller. Next, using a process running on the user's smartphone, the method includes determining validity of the credential, and if the credential is determined to be valid, evaluating the credential for conformity with the set of criteria. If the credential is determined to be in conformity with the set of criteria, then the method requires allowing the communication to be established. The set of criteria may include presence of the name of the caller on a white list. Alternatively or in addition, the set of criteria may include a requirement that the caller have an age that is within two years of the user's age.

Another embodiment provides a data gathering device for communicating with a mobile electronic device of an individual, the mobile electronic device being capable of decrypting messages according to an encryption key of the individual. The data gathering device includes a sensor for gathering data; a cryptographic module for encrypting gathered data using the encryption key; and a transmitter for transmitting encrypted data to the mobile electronic device. The transmitter may be a Bluetooth transmitter. The cryptographic module may be a hardware security module, and it may be embedded within a smartcard. The data gathering device may also have a receiver for receiving encrypted data from the mobile electronic device and a display for displaying received data, wherein the cryptographic module is further capable of decrypting received data according to the encryption key. The display may be a video or an audio display, and it may be capable of displaying gathered data. The sensor of such embodiments may gather medical data, when the data gathering device is a medical device.

Yet another embodiment of the invention provides a method for securely obtaining, from a medical data gathering device, medical data pertinent to an individual. The method includes receiving the medical data over a wireless network from a smartphone of the individual coupled to the medical data gathering device. In this method, the smartphone stores and forwards, over the wireless network, the data from the medical data gathering device. Further, the medical data are encrypted with a public key of the individual. In a related embodiment, the smartphone is wirelessly coupled to the medical data gathering device. The smartphone may have flash memory in which are stored the medical data.

Petitioner Exhibit 1002-0749

In another, related embodiment, the smartphone may have a storage module in which is stored a digitally signed document containing a set of credentials of the individual. The storage module may also store authentication data of the individual, in which case the smartphone further includes a data entry arrangement for entering data into the device, and a controller, coupled to the storage module and the data entry arrangement. The controller is programmed to require, as a condition to using the stored set of credentials for authentication purposes, entry of the authentication data into the device via the data entry arrangement, so as to authenticate a would-be user of the device as the individual.

This embodied method may be extended by storing the data received over the wireless network in a database coupled to a server for access by authorized medical professionals. The method may be further extended by decrypting and granting access to the medical data in response to a request by a person determined to be an authorized medical professional.

Brief Description of the Drawings

The foregoing features of the invention will be more readily understood by reference to the following detailed description, taken with reference to the accompanying drawings, in which:

Fig. 1 is a block diagram of major functional components of an embodiment of the invention;

Fig. 2A is a block diagram of a process by which a person may activate a mobile electronic device in accordance with embodiments of the invention;

Fig. 2B is a block diagram of a process by which a person may use a mobile electronic device in accordance with embodiments of the invention;

Fig. 3 is a block diagram of a process by which a digital resume is created, authenticated, and stored, in accordance with an embodiment of the invention;

Fig. 4 is a block diagram of a process by which digital resumes are updated to account for revoked credentials, in accordance with an embodiment of the invention;

Fig. 5 is a block diagram overview of a prior art computer-implemented process by which credential certificates are verified using a public key infrastructure;

Petitioner Exhibit 1002-0750

Fig. 6 is a block diagram overview of a process by which certificates are verified using an extended public key infrastructure in accordance with an embodiment of the invention;

Fig. 7 is a block diagram detail of a process by which certificates are verified using a public key infrastructure in accordance with an embodiment of the invention;

Fig. 8 is a block diagram of a process by which a person may create a virtual smartcard in accordance with an embodiment of the invention;

Fig. 9 is a block diagram of a process by which a person may enable a device in accordance with an embodiment of the invention;

Fig. 10 is a block diagram of a process, in accordance with an embodiment of the present invention, for batch processing of secured transactions using a mobile device in the manner described and for rapidly detecting fraud;

Fig. 11 is a block diagram of a process by which a person may register a device in accordance with an embodiment of the invention to permit physical access to a secured area;

Fig. 12 is a block diagram of a process by which a person may use a device in accordance with an embodiment of the invention to access a secured area;

Fig. 13 is a block diagram of a process for updating a device in accordance with an embodiment of the invention to alter or revoke permission to access a secured area;

Fig. 14 is a schematic block diagram showing the relevant parts of a prior art system for providing business information;

Fig. 15A is a schematic block diagram showing the relevant parts of a system for providing business information in accordance with an embodiment of the invention;

Fig. 15B shows typical processes for implementing the deposit and secure access of trusted data according to the system of Fig. 15A;

Fig. 16 is a schematic block diagram showing preparation processes, in accordance with an embodiment of the present invention, of a trusted storage system for operation;

Fig. 17 is a schematic block diagram showing a process of updating a trusted storage system with new business data;

Fig. 18A is a block diagram of the flow of data at a business in a trusted system embodiment;

Petitioner Exhibit 1002-0751

Fig. 18B is a block diagram of the flow of data at a data service provider in the embodiment;

Fig. 18C is a block diagram of the flow of data into the local storage of an electronic device in accordance with this embodiment of the invention;

Fig. 18D is a block diagram, in accordance with an embodiment of the invention, of the retrieval of data from the local storage of an electronic device so that it may be consumed;

Fig. 19 is a block diagram showing an embodiment of the present invention wherein a trusted data storage arrangement is coupled to a general communications gateway environment;

Fig. 20 is a schematic block diagram of another embodiment of the present invention showing a memory device including dedicated write-once, read-many (WORM) storage areas for trusted data;

Fig. 21 is a block diagram, in accordance with a further embodiment of the present invention, showing a process for updating the memory device of Fig. 20 in a manner consistent with consumer needs and a relevant business environment;

Fig. 22 is a block diagram, in accordance with a further embodiment of the present invention, showing a process for downloading digital media content to the memory device of Fig. 20;

Fig. 23 is a block diagram, in accordance with a further embodiment of the present invention, of a process for playing digital media content, from the memory device of Fig. 20, after the content has been downloaded according to the process shown in Fig. 22;

Fig. 24 is a block diagram, in accordance with embodiments of the present invention, of processes for determining which sites require cached credentials;

Fig. 25 is a block diagram, in accordance with an embodiment of the present invention, of caching credentials at a site determined in Fig. 24;

Fig. 26 is a block diagram of a further embodiment of the present invention showing processes for initiating communications between two parties;

Fig. 27 is a block diagram of relevant processes for authorizing a mobile electronic device in accordance with embodiments of the invention to participate in credit transactions;

Petitioner Exhibit 1002-0752

Fig. 28 is a block diagram of processes by which a mobile electronic device in accordance with embodiments of the invention updates itself after a credit data network becomes available;

Fig. 29 is a block diagram of a method in accordance with an exemplary embodiment of the present invention, in which a phone as described above is prepared and used in card-not-present transactions;

Fig. 30 is a block diagram of a method for extending credit to an individual having a phone prepared as in Fig. 29;

Fig. 31 is a block diagram showing the operation of a single sign-on embodiment of the present invention;

Fig. 32 is a block timing diagram of an embodiment of the present invention in which cookie data is end-to-end encrypted;

Fig. 33 is a diagram showing the different components used in a method for acquiring data with a measuring device and publishing the data to trusted storage for later retrieval by a trusted individual, in accordance with an embodiment of the invention;

Fig. 34 is a block diagram of the process for uploading data in the method of Fig. 33;

Fig. 35 is a block diagram of a method for a trusted individual to access data acquired and published as in the embodiment of Fig. 34; and

Fig. 36 is a block diagram of a method for a trusted individual to transmit information to the measuring device of Fig. 33.

Detailed Description of Specific Embodiments

As used in this description and the accompanying claims, the following terms shall have the meanings indicated, unless the context otherwise requires:

A **digital signature** is an output of a public key (asymmetric cryptographic) algorithm used to simulate, in digital form, the endorsing properties of a physical signature. Algorithms for working with digital signature algorithms appear in pairs: one algorithm exists to create the signature, and one algorithm exists to validate the signature. Digital signature algorithms are well known in the art, an illustrative example being NIST, *FIPS 186: Digital Signature Standard (DSS)*, hereby incorporated by reference. (FIPS-186, like other FIPS standards, is an evolving standard. A version current as of the date of filing may

Petitioner Exhibit 1002-0753

be found at http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf.) The DSS specifies a Digital Signature Algorithm (DSA) which is partially described in U.S. Patent No. 4,995,082 (Schnorr) and U.S. Patent No. 5,231,668 (Kravitz). These patents are hereby incorporated by reference.

A **trusted authority** is an agency or organization that certifies information relating to third parties by issuing, and digitally signing, electronic documents containing the information. Third parties who wish to validate such information about each other can agree to trust documents promulgated by one or more commonly-trusted authorities.

An **identity certificate** is an electronic document issued by a trusted authority which incorporates a digital signature to associate an individual with a public encryption key. The individual can use the encryption key to digitally sign electronic documents. A third party can use the encryption key to securely communicate with the individual. By signing a summary certificate, a trusted authority attests that the encryption key is that of the individual. The trusted authority may revoke an identity certificate by publishing notice of revocation using well-known methods, described below.

Online Certificate Status Protocol (OCSP) is a protocol for interactively providing and obtaining the revocation status of certificates. The protocol is described in Internet Engineering Task Force, *Request for Comments 2560: X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol – OCSP* (1999), and its successor documents, hereby incorporated by reference. (RFC 2560 may be found on the Internet at http://tools.ietf.org/html/rfc2560.)

A **credential** is data representing an attestation of qualification, competence, or authority issued to an individual by a third party having authority to do so. A credential may be embodied in a physical form, which we denote herein a **physical credential**. An example of a physical credential is a driver's license. A credential may also exist in electronic form, which we denote herein an **electronic credential**. An example of an electronic credential is a virtual smartcard in accordance with an embodiment of the present invention. A credential should be distinguished from the identity of its holder – a credential may expire, while the identity of its holder does not.

A **smartcard** is a vehicle—physical or virtual—for providing one or more credentials. When the vehicle is physical, the physical smartcard is typically implemented as

Petitioner Exhibit 1002-0754

a pocket-sized card with embedded integrated circuits which can securely store and process information such as encryption keys, biometric data, and personal identification numbers. When the vehicle is virtual, the virtual smartcard is a computer system that simulates the behavior of a physical smartcard. Smartcards may comply with federal standards for use as identity credentials such as Federal Information Processing Standard 201 (**FIPS-201**), described in National Institute of Standards and Technology (NIST), *FIPS 201: Personal Identity Verification (PIV) of Federal Employees and Contractors*, hereby incorporated by reference. (FIPS-201 is an evolving standard. A current version may be found online at http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.)

A **hardware security module (HSM)** is a device for generating and storing long term secrets for use in cryptography, and for physically protecting the access to and use of those secrets over time. Such secrets may include private keys for use in a public key encryption algorithm. For maximum secrecy, a secret generated using the hardware security module is never transferred from the module to other hardware or software. An HSM provides cryptographic services to a user of the smartcard, such services including creation and secure storage of encryption keys, and implementation of cryptographic algorithms. HSMs are well known in the art, for example as described in NIST, *FIPS 140: Security Requirements for Cryptographic Modules* (May 2001), hereby incorporated by reference. (FIPS-140 is an evolving standard. A current version of this evolving stand may be found at http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.) Smartcards having an HSM are known in the art. Such smartcards typically present a programming interface that allows software, such as a host operating system, to access HSM functions. An illustrative example of a standard specifying such an interface is described in RSA Laboratories, *PKCS #11: Cryptographic Token Interface Standard*, hereby incorporated by reference. (PKCS #11 is an evolving standard. A version current as of filing is ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20.pdf. The standard has been amended three times, with two additional amendments proposed.)

A **credential certificate** is an electronic credential issued by a trusted authority which incorporates a digital signature to associate the credential data with an individual. By signing a credential certificate, a trusted authority attests that the individual possesses the

Petitioner Exhibit 1002-0755

credential. The trusted authority may revoke a credential certificate by publishing notice of revocation using well-known methods.

A **summary certificate** is an electronic credential issued by a trusted authority which incorporates a digital signature to associate a primary credential with one or more secondary credentials upon which the issuance of the primary credential relied. A summary certificate represents indirect trusts, rather than identities. By signing a summary certificate, a trusted authority attests that the secondary credentials were considered in the process of, and relied upon in the issuing of, the primary credential. A method for revoking a summary certificate in accordance with an embodiment of the invention is depicted in **Fig. 6** and described below.

A **digital resume** is an electronic document issued by a trusted authority which incorporates a digital signature to associate an individual with a collection of credential certificates, summary certificates, or both. By signing a digital resume, a trusted authority attests that the collection of certificates is properly associated with the individual.

A **trust chain**, or **chain of trust**, is a list of trusted authorities wherein each trusted authority obtains its own identity certificate from the next trusted authority in the list. Such certificates, wherein one authority certifies another, are known as **cross-certificates**. A chain of trust terminates with a **root authority**, or **trust anchor**, which issues an identity certificate for itself that has both the root authority's public key and a **self-signature** which may be validated using the same key. As the root authority attests to its own identity, it must be a well-known and broadly trusted agency or organization.

An **authentication token** is a device that an authority gives a user of computer services to aid in authenticating the user to those services. An authentication token is typically small enough to be carried inconspicuously on the user. A common example of an authentication token is a wallet-sized smartcard having a hardware security module that stores data that may also be pertinent to authentication.

A **virtual smartcard** is a set of data and computer-implemented algorithms, associated with an individual, which simulate an authentication token containing a hardware security module.

A **message digest** is a fixed-length set of data which encodes other data of any size using a non-reversible hash function. Such hash functions are well known in the art. An

Petitioner Exhibit 1002-0756

example hash function is described in NIST, *FIPS 180: Secure Hash Standard*, which is hereby incorporated by reference. (FIPS-180 is an evolving standard. A current version is http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf.) Since the hash function is non-reversible, a relying party may be confident that two digests are equal only if their inputs are equal. (As digests may be created that are smaller than their inputs, collisions can occur. However, a judicious choice of a hash function can make it difficult for an untrusted third party to construct colliding inputs. A "good" hash function has the property that each bit altered in the message data will result in approximately half of the output bits being altered.)

Wi-Fi Protected Access (WPA) is a communications security protocol described in Institute of Electrical and Electronics Engineers (IEEE), *IEEE Standard for Information technology--Telecommunications and information exchange between system--Local and metropolitan area networks--Specific requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications--Amendment 6: Medium Access Control (MAC) Security Enhancements* ("802.11i"), hereby incorporated by reference. (802.11i is an evolving standard. A version current as of the date of filing may be found at http://standards.ieee.org/getieee802/download/802.11i-2004.pdf.)

A **PKI standard** is a standard governing the implementation of public key infrastructure, established either de facto or by a standards-setting body. At present, the X.509 standard, established by the International Telecommunication Union, and referenced below in this description, governs implementation of public key infrastructure and satisfies this definition.

A **federated data store** is a collection of two or more data storage devices connected by a communications network, where each data storage device is operated by a different data service provider, and the data service providers act in concert to provide data storage.

An **access control system** is a set of devices for permitting a person access to a physical space. An access seeker presents a token, such as a smartcard, to the system. An access control system **headend**, or central controller, responds by validating the individual's credential, and if authorized, sending electrical signals to various physical barrier controls, such as magnetic door locks, causing them to unlock and permit the individual access to the area beyond. A typical example of an access control system is a subway turnstile.

Petitioner Exhibit 1002-0757

A **transaction** is an activity, such as physical access to premises or to a region, purchase of a good or service, extension of credit, or performance of a service, with respect to which authentication or authorization (or both authentication and authorization) of an individual is desired.

A **credential service** is a service by which desired authentication or authorization (or both authentication and authorization) of an individual may be determined for purposes of a transaction.

A **smartphone** is a cellular telephone providing storage capacity and processing capacity to permit the telephone to handle computational tasks (in particular to run applications) in addition to wireless telephone service and to handle data in addition to cellular telephone data.

A **payment token** is a number that has certain properties that allow its uniqueness and association with a particular user to be determined mathematically. Creation and use of payment tokens is described in, among many places, U.S. Patent 5,224,162 (Okamoto et al.) and U.S. Patent 6,236,981 (Hill), hereby incorporated by reference.

Write-once, read-many (WORM) storage refers to a computer data storage arrangement, including computer memory, to any portion of which data can be written only a single time (wherein data thus written cannot be altered) and from which data can be read multiple times. Typically, the act of storing data to a WORM device includes physically altering the device irreversibly, so that the data being written cannot be rewritten. An example of WORM storage is a recordable compact disc (CD-R), whose substrate is irreversibly burned by a laser. Another example of WORM storage is a programmable read-only memory (PROM), where a bit of memory is permanently fixed as a zero or one by irreversibly burning an appropriate fuse.

A **passcode** is a secret character string that may be required as a condition for access to a digital resource (such as data, or a computer network, or a computer facility), as a measure to preclude unauthorized use of the resource.

Embodiments of the present invention provide an end-to-end arrangement permitting the rendering of credential services in a fashion that is scalable, dynamic, and individualized. Various embodiments utilize mobile telephones. In some of these embodiments, the telephones may be implemented using flash memory or other storage arrangements.

Petitioner Exhibit 1002-0758

Although not all embodiments require mobile telephones and not all of the mobile telephone embodiments require flash memory, those embodiments utilizing both offer enhanced functionalities.

Overview of Core System Components

Fig. 1 is a block diagram of major functional components of an embodiment of the invention. Functional components include an agency venue **110**, a data storage venue **120**, an application venue **130**, and an electronic device **140**. The illustrated arrangement of these components enables a data service provider to provide credential services to individuals on behalf of one or more agencies. With the components embodied and arranged as described below, the data service provider may scale its operations dynamically to service a large number of agencies, accommodate a large number of individuals, or both. Although we have here used the term "agency" for the credential issuer, we show in further detail below, that the architecture described in this embodiment is applicable to a wide range of credential issuers, including also, banks (with respect to bank accounts, loan accounts, and credit card accounts, among other things), other credit card issuers, enterprises (with respect to physical access to premises and access to computing facilities), health care institutions, educational institutions, etc.

An agency issues credentials to individuals. To service its personnel or the public, the agency establishes an agency venue **110**. For example, a state Department of Motor Vehicles (DMV) is an agency that establishes an office where citizens may obtain licenses allowing them to operate motor vehicles on state property. As another example, the Federal Aviation Administration is an agency that issues certificates to individuals allowing them to operate aircraft in the National Airspace System. This list is illustrative only, and it is to be understood that an agency may be any organization, public or private, that issues credentials to individuals. Also, an agency may establish multiple agency venues.

Typically, an agency will undergo a process **111** of vetting an individual, then issuing the individual a physical credential **112**. The vetting process may vary from one agency to the next. By way of illustration, a DMV may require a person to identify herself by presenting other credentials such as a passport, birth certificate, or foreign driver's license to an agent at an agency venue **110**. In addition to the identification credentials, the DMV may

Petitioner Exhibit 1002-0759

require the person to pass a series of tests, such as a vision test, a knowledge test, and a skills test, in order to satisfy the agency that she meets statutory requirements for operating a motor vehicle.

Once vetting is complete, the agency issues the individual a physical credential **112**, certifying that she has met the requirements for its issuance. Physical credential **112** may be, without limitation, a driver's license, a Transportation Worker Identification Credential (TWIC), or a FIPS-201 compliant smartcard. Physical credential **112** may also be a smartcard containing a hardware security module (HSM), in accordance with embodiments of the invention. In addition to (or in lieu of) issuing a physical credential **112**, an agency venue **110** may issue an electronic credential in accordance with an embodiment of the invention. To do so, the agency may participate in a public key infrastructure (PKI). The agency may establish a Certificate Authority (CA) **113**, such as that described in X.509, or the agency may contract with a third party CA. The CA issues an identity certificate **114** to the agency according to procedures well known in the art, such as may be found in X.509.

The agency creates a credential certificate by using identity certificate **114** to sign a credential using a digital signature algorithm. The presence of the agency's digital signature allows a party in possession of the credential to verify that its contents have not changed between the time of signing and the time of verification. A credential certificate may have substantially the same information as physical credential **112**, or it may contain additional or different data which better lends itself to digital manipulation. An agency may store a credential certificate in a data store **115** for its own records and for sharing with others.

Agency venue **110** may share its electronic credentials with a data service provider, which operates at least one data storage venue **120** according to an embodiment of the invention. A data service provider offers first responder agencies and other organizations with a data service for authenticating individuals. There can be many data service providers, and an agency may choose a data service provider based on its needs. Different data service providers may establish trust with one another, cooperating to form a network of highly-available, federated data storage and services using methods which should be apparent to those skilled in the art.

At any given data storage venue **120**, a data storage engine **121** receives electronic credentials from agency venue **110**, and place them in a data store **122**. The data service

Petitioner Exhibit 1002-0760

provider collects and maintains these credentials according to methods depicted in Fig. 3 through Fig. 7, and described in detail below. Data storage engine 121 may create a virtual smartcard 123 associated with the credentialed individual, using a method depicted in Fig. 8 and described in detail below. In order to create the virtual smart card, data storage engine 121 utilizes a CA 124. The storage provider that operates the data storage venue 120 may establish its own CA, or contract with a trusted third party for this purpose. Data storage venue 120 may publish credential certificates to an application venue 130 using a publisher 125, which may be a web server or other network service provider. Data storage venue 120 responds to certificate verification requests using an OCSP responder 126, which also may be a web server or other network service provider.

An application venue 130 is a site at which an individual must be certificated. Such sites include, by illustration and without limitation, a disaster area, a facility processing classified information, and a roadside car stopped by a law enforcement officer. Taking as example a disaster area, the venue may have on-site emergency management personnel, such as a guard 131. Guard 131 determines that certain software applications are required to deal with the emergency and that first responders must have certain privileges required to access the software. Guard 131 enters this information into management software in a command-and-control system 132. When a first responder 133 arrives, he presents at least one physical credential 112, which he earlier obtained from an agency venue 110, as well as additional information such as a password or personal identification number (PIN). Using the process depicted in Fig. 9 and described below, software on command-and-control system 132 verifies his credentials, and registers a mobile electronic device 140. Management personnel download software applications for first responder 133 onto mobile electronic device 140. The applications are chosen based upon the physical credential 112 presented by first responder 133. The first responder 133 may then use the applications on mobile electronic device 140 to respond to an incident.

Mobile electronic device 140 may be used, among other things, to provide first responders with application-specific software and data that they can use to deal with emergencies. More generally, as we describe in further detail below, the mobile electronic device may be used to authenticate a wide range of transactions, including physical access to a region or to premises, access to computational facilities, financial transactions, including

Petitioner Exhibit 1002-0761

the purchase of goods or services, the extension of credit, licensing of individuals in various contexts, including performance of health care services, operation of a motor vehicle, etc. The mobile electronic device **140** may be, among other things, a personal digital assistant (PDA), a cellular telephone, or a laptop computer.

In accordance with embodiments of the present invention, a person will be permitted to expose and use credentials on the device **140** for transactions only after the person has authenticated himself to the device **140**. In authenticating himself to the device **140**, the user may be required to provide multiple forms of identification (multi-factor authentication), including at least one physical credential **112**. In one embodiment, the user provide the physical credential by swiping a finger on a fingerprint reader **143**, which may be implemented in the device **140** (or which may be external to it), wherein the physical credential **112** is implemented as a biometric identifier. In addition, the user may also have to provide a personal identification number (PIN) to the device **140**. In another embodiment, physical credential **112** is implemented with a smartcard **141**, which is cradled in a receiver designed for that purpose. In this context, the smartcard **141** serves as a token. Smartcard **141** may be issued by a credentialing agency or another organization. In another embodiment, a user does not have a smartcard. Instead, physical credential **112** is, for example, a driver's license or a credit card (which are also tokens). Such physical credentials are challenged by scanning a 2-dimensional barcode or reading a magnetic stripe on the credential, rather than using cryptography. In these embodiments, the challenge response may be verified by comparing it to trusted external data provided by an issuing agency. Because the device **140** may itself serve as a token (because it embeds one or more credentials), requiring a biometric for the user to authenticate himself to the credential has the benefit of requiring a separate type of factor in the authentication process. Mobile electronic device **140** may have a hardware security module to facilitate the user authentication process. Authentication software may require that mobile electronic device **140** be docked or cradled to another device (not shown) that is connected to a keypad, keyboard, biometric device **143**, or other data entry arrangement such as a barcode scanner or magnetic stripe reader, in order to securely verify identity challenges using the phone's own HSM.

Petitioner Exhibit 1002-0762

Mobile electronic device **140** contains an identity certificate **144** for use in secure communications with another mobile electronic device **140**, application venue **130**, or data storage venue **120**. Using digital certificate **144**, the device can download from a data storage venue **120** a digital resume **145** containing additional credentials. A phone implementing device **140** may also have photo and video capture software **146**, building blueprints or site maps **147**, terrain data from a geographical information system (GIS), software for accessing a criminal records database or a security clearance database, a materials safety data sheet (MSDS), resource and incident management software, status reporting software, help functions **148** for any or all of these things, or other useful or necessary applications and data.

A mobile electronic device **140** has several functional components. Such a device includes a secure storage module which may store a digital resume containing a set of credentials and authentication data. An example of a storage module is a flash memory, or other non-volatile memory device such as a hard disk drive. Mobile electronic device **140** has a data entry arrangement, as described above, for entering authentication data. Device **140** has a controller, coupled to the storage module and the data entry arrangement. The controller may be a microprocessor or other computing means that can be programmed to require a user to enter into the device the stored authentication data before granting the user access to a stored digital resume. Device **140** also includes a communication port for receiving and transmitting data to other devices. A communication port may be a wire port, such as a socket for a networking cable plug, or it may be a wireless transceiver. Those skilled in the art will recognize that a mobile electronic device may be implemented using other types of hardware devices, suitably arranged and functionally connected.

It should also be appreciated by those skilled in the art that the foregoing features of a mobile electronic device embodiment, such as encryption, data storage, communication by wired or wireless data network, and so on may be implemented by a number of other types of electronic device that lay within the scope of the invention. Such other devices may include desktop computers, server computers, mainframe computers, pagers, or any other electronic device with the appropriate functional components. For an example embodiment making use of a desktop computer, see **Fig. 15A** and the discussion thereof. These other embodiments may be used in addition to, or instead of, a mobile electronic device. Such use may occur, as

Petitioner Exhibit 1002-0763

an example, if a battery charger for a mobile electronic device cannot be found, or if an adequate power source for recharging the device cannot be found. In such a case, a desktop computer may be used, for example, to perform the security or encryption functions of a mobile electronic device.

A mobile electronic device **140**, such as a smartphone, has four key properties that render it particularly suitable for use in embodiments of the invention described herein: computing facilities, secure storage, updatability, and an association with a unique user. Each device **140**, as described above, contains computing facilities (e.g., a microprocessor). These facilities allow the device **140** to participate in encrypted transactions without the need to consult another device. Each device **140** also contains secure storage, which ensures that credential data stored on the device cannot be altered, either accidentally or deliberately. Each device **140** has the ability to update credentials stored on it, which enables the device to add or remove an individual's authorization to perform given tasks using the device on a near-real time basis. And each device **140** is associated with a unique user, allowing that user to use the device as a token for authentication.

Fig. 2A is a block diagram of a process by which a person may activate a mobile electronic device in accordance with embodiments of the invention. Illustrative embodiments employ a smartphone, but it should be understood to those skilled in the art that other electronic devices may be used, such as personal digital assistants (PDAs), laptops, and other computing devices. **Fig. 2A** and **Fig. 2B** depict the initialization and use of a phone **240** in accordance with embodiments (represented in the Figures as **240A** and **240B** for clarity of description). A user **210** (**210A** and **210B** in the Figures) obtains an activated phone **240** that contains secure applications and data. These applications and data may be used by user **210**, for example, to respond to an emergency. Applications and data may also be used by a third party system **260** in order to securely transact with user **210**.

User **210** begins the activation process (for initially setting up the smartphone for use by the user) in **Fig. 2A** by presenting herself for identification at a security office, human resources office, or a similar processing location. A security officer (not shown) at the location accesses enrollment system **230**, a computing system that includes software that performs cryptographic functions and phone initialization functions. User **210** presents credentials **220A** to the security officer, who enters relevant data from the credentials into

Petitioner Exhibit 1002-0764

enrollment system **230**. Enrollment system **230** then verifies the user's identity in process **232**, described more fully below. Once the identity of user **210** has been proved, enrollment system **230** may take one of two paths to enable a phone, depending on the kind of credentials **220A** presented. First, if credentials **220A** include a smartcard having an HSM containing a private key, the system directly enables and programs phone **240A** in process **236**. But, if credentials **220A** do not include a smartcard having an HSM containing a private key, enrollment system **230** creates a private key for storage on the phone **240A** in process **234** first, then enables and programs the phone in process **236**. The private key stored on phone **240A** or on a smartcard, and the presented credentials, can later be used to prove the identity of user **210A** at a later time, as depicted in **Fig. 2B**.

Process **232** for proving a person's identity may be accomplished in two ways, again depending on the number and types of credentials **220A** presented. The process ensures multi-factor authentication with at least two factors. If credentials **220A** include a smartcard with an HSM (for example, a FIPS-201 identification card) then the card is read and its contents validated by an activation challenge such as a fingerprint or a PIN. Once this occurs, user **210A** has produced a physical token and a challenge response which satisfy two-factor authentication requirements. On the other hand, if credentials **220A** do not include a smartcard, a security officer may determine that several credentials are required to establish the identity of user **210A**. The officer enters information from these credentials into the enrollment system **230**. The officer may challenge user **210A** for a PIN or a biometric, such as a fingerprint, to guarantee multi-factor authentication. Credential data may be entered manually or through the use of technology such as a barcode scanner, fingerprint scanner, or other similar device.

Once credential data has been entered into enrollment system **230**, regardless whether it derives from smartcards, other identity documents, or a challenge response, the credentials themselves are tested for validity in accordance with embodiments of the invention, using the process depicted in **Fig. 4**. If one or more credentials are invalid, the security officer may require user **210A** to present alternate credentials, or take other remedial actions as appropriate. Credentials can be validated when a secure communications link can be established between the enrollment system **230** and a data service venue, such as that depicted in **Fig. 1**, that contains up-to-date credential validity data.

Petitioner Exhibit 1002-0765

Process **236** for enabling and programming a phone also entails several processes. Once a user has adequately identified herself to enrollment system **230** using credentials on hand, the system obtains additional credentials in the form of a digital resume using the processes depicted in **Fig. 3** and **Fig. 9** and described more fully below. Alternatively or in addition, user **210A** may wish to create a virtual backup of her physical credentials, in case the latter are lost or misplaced. User **210A** can create a virtual smartcard that represents data stored on a physical credential, in accordance with embodiments of the invention, as depicted in **Fig. 8** and described more fully below. At the same time, the enrollment system **230** creates a virtual smartcard for phone **240A** using a private key stored in the phone's own HSM by the same process. Then, if a user loses a first phone **240A**, another phone in accordance with embodiments may be given to the user, and data encrypted using the first phone's private key may still be accessed using the old phone's virtual smartcard.

Process **236** may also create an authentication digest for storage on phone **240A** using credential data. The digest can be used later in process **242** to show that user **210A** is the same as user **210B**, that credentials **220A** are the same as credentials **220B**, and that phone **240A** is the same as phone **240B**. Equality may be shown by recomputing the digest using the same hash function on the phone, and comparing it to that stored on the phone or at a trusted back-up data storage venue. If the two digests are equal, all inputs almost certainly match. If they differ, then the current inputs must differ from the inputs used to compute the first digest, and further security procedures may be invoked.

In addition to storing an authentication digest on the phone **240A** and software necessary to calculate the hash function, process **236** may upload sensitive or classified software applications, data, or both to the phone. These applications and data may be used by user **210** according to conditions programmed by the enrollment system **230**. For example, some or all of these applications and data may not be accessible unless a person authenticates herself to the phone, as in **Fig. 2B**. Or, applications may only be accessible within a certain physical area. In which case, process **236** installs software on phone **240A** that can lock and unlock other applications in response to certain messages received by the phone from a trusted access control system. The design of such software should be apparent to one having skill in the art. Also or alternatively, process **236** may install software that interfaces with third-party systems, such as credit card processing systems. Other types of software which

Petitioner Exhibit 1002-0766

might be installed on a phone, and the methods for doing so, should be apparent to those skilled in the art.

Fig. 2B is a block diagram of a process by which a person may use a mobile electronic device in accordance with embodiments of the invention. The process does not assume that user **210B** is the same as user **210A**. For example, the phone may have been lost by legitimate user **210A** and found by malicious user **210B**. The process does not assume that credentials **220B** are the same as credentials **220A**. For example, the user may have forgotten or misplaced credentials **220A**, and may attempt to use different (or even false) credentials **220B** to authenticate herself so that she may use the phone. The process does not assume that phone **240A** is the same as phone **240B**. For example, a user may have attempted to copy data from one phone to another, to make a backup, or for malicious purposes. At the conclusion of the process depicted in **Fig. 2A**, phone **240A** has been enabled and programmed with applications and data, and given to user **210A**. Further, phone **240A** contains an authentication digest which allows user **210A** to identify himself to the phone. Now, user **210A** may use phone **240A** to engage in a wide range of transactions, with respect to which security is provided by the use of credentials in the manner we describe herein.

To authenticate a phone in the field, a user docks the phone to a service station and answers various challenges to reproduce the digest. It will be understood that a user may communicate with a service station in a variety of methods, including by local wired or wireless methods. Communication with a central data store or a data service provider is not necessary. Such a system is advantageous, for example, at an airport security checkpoint. In this example, a security worker may securely verify a person's identity and validate the data stored on a phone simultaneously, based only on a person's non-electronic physical credential, while the person waits in line, without needing to contact the agency that issued the credential.

The process for using the phone begins with the phone **240B** in a locked state. To protect sensitive or classified applications and data stored on phone **240B**, the phone must enter a locked state after a period of inactivity or after a triggering event, such as deactivation by user **210B**. Thus, user **210B** must first re-prove her identity in order to unlock the phone, in process **242**. Process **242** is similar to process **232**: user **210B** presents credentials **220B**

Petitioner Exhibit 1002-0767

to the phone to authenticate the user. Such authentication may take the form, for example, of entering a personal identification code (PIN) and swiping a finger for a fingerprint. After receiving these credentials, the phone **240B** processes these credentials to authenticate the user. In one embodiment, the phone calculates a digest of the credentials using software on the phone, and compares the calculated digest to the previously stored digest. If the two digests match, then the software concludes that the user **210B**, the credentials **220B**, and the phone **240B** are the same as user **210A**, credentials **220A**, and phone **240A** respectively (referred hereinafter without suffix). If the two digests differ, the phone software for authenticating a user may request that the credential data be input again, lock the phone against further attempts to authenticate, or take other appropriate action.

If the digests match, the authentication of the user to the phone has succeeded, permitting the phone to be used downstream in authenticating a transaction. Before the phone is used for transaction authentication, a number of additional processes are typically employed in embodiments of the present invention. In one embodiment, the phone may check stored credentials to verify their consistency. In this embodiment, the phone encrypts a random number with a public key of the user; it then decrypts with result with a stored private key of the user functioning as a credential of the user; if the results match, then the phone has verified the consistency of the public key and the store private key in the credential. After this verification, the phone software determines which applications to enable in process **244**. Next, there may be processing on the basis of data external to the phone to determine whether credentials presented in the phone are still valid, in accordance processes depicted in **Fig. 4** and batch processes described later. If the credentials are not all valid, phone **240** may indicate to user **210** that, while his credentials are recognized, they must be renewed before access to certain applications and data is granted. If the credentials are all valid, or if the software determines that not all credentials must be current, access to secure applications and data may be enabled in accordance with the limitations and conditions programmed into the phone by enrollment system **230**. At this point, user **210** can expose the user's credentials for use in a wide range of transactions, such as access to premises or computing facilities or financial transactions involving purchases or the extension of credit or both.

Petitioner Exhibit 1002-0768

Accordingly user **210** may use a phone **240** in accordance with embodiments of the invention to securely identify herself to a relying party and engage in various secure transactions. Such transactions arise, for example, in a marketplace, where a merchant wishes to identify an individual and charge a purchase to that individual's credit. Or, an organization may wish to identify an individual for the purpose of granting that individual access to areas within a campus or building that require special permission to enter. Other, similar secure transactions may be readily envisioned by a person skilled in the art.

A secure transaction begins with process **246**, where phone **240** presents the credentials of user **210** to a relying party system **260**. The communication of credentials may occur using a secure communications link **250**, which may be, without limitation, a wireless communications network or a physical, wired connection between phone **240** and relying party system **260**. Communications security may be provided, for example, by the use of WPA or another communications security protocol.

Once the phone has presented the credentials of user **210**, relying party system **260** receives them in process **262**. Next, relying party system **260** evaluates the credentials in process **264**. This process may be manual, for example displaying the credentials to a human guard or merchant on a computer display for approval or disapproval. Process **264** may include automated processes, such as verifying that the credentials are still valid, as in **Fig. 4**. A merchant may wish to perform this check because it is possible that, at the time user **210** authenticated herself in process **242**, the latter process was unable to verify the credentials in accordance with **Fig. 4**, yet still determined that the phone **240** should be unlocked. Also, the merchant may have a hard-wired connection to a data service provider required by **Fig. 4**, while phone **240** may have only a less reliable, wireless connection.

Next, the relying party decides whether or not to transact with user **210** in process **266**. For example, a merchant or a security officer may decide that the credentials presented for evaluation in process **264** are not sufficient to adequately determine the identity of user **210**. Or, a merchant may use the credentials to fetch a credit score for user **210** that the merchant determines is insufficient to complete the transaction. Or, a security officer may use the credentials to fetch permissions for user **210** that the officer determines are insufficient to grant the user physical access to a secured area. If, however, the decision is positive, relying party system **260** securely transacts with phone **240** using secure

Petitioner Exhibit 1002-0769

communications link **250** in process **268**. Various embodiments of secure transactions are depicted in **Fig. 10** through **Fig. 13** and described below.

As a preliminary example use of a phone credential, an individual may store her driver's license, auto registration, and insurance information in credentials on the phone, and expose them to a police officer during a traffic stop. On the other hand, she may not wish to expose them for some reason. In such cases, a phone may be programmed to allow the police officer, or someone else with sufficient credentials, to retrieve certain of the individual's credentials in any event. In other words, the phone may have various overrides that allow certain others to access specific credentials in case of an emergency. A police officer may be able to engage an override, but still only get access to the individual's license and registration. A medical technician could engage an override, but only get access to the individual's drug prescriptions, or other necessary medical data. Furthermore, the override transaction can be logged by the phone for later auditing or evidentiary purposes, to determine that the override was proper. Thus, the phone can be viewed as a device that allows first responders to get access to important data, while preserving the privacy of those who may be involved in an emergency.

Digital Resumes

A digital resume is a collection of credentials which may be stored on a phone in accordance with various embodiments. These credentials may be used to authenticate a user during process **236** or **242**, or for presenting to a relying party **260** to initiate a secured transaction.

Fig. 3 is a block diagram of a process by which a digital resume is created, authenticated, and stored, in accordance with an embodiment of the invention. The process begins with credentialing agencies. Such agencies include, without limitation, the Department of Defense **310**, a state Department of Motor Vehicles **312**, other agencies of a state or the federal government **314**, and an independent licensing authority **316**. These credentialing agencies issue credential certificates to an individual, as described above in connection with **Fig. 1**. A data service provider accumulates these credential certificates at a data storage venue **120** to form a digital resume **320** for the individual. As more agencies issue certificates, they are added to the digital resume **320**.

Petitioner Exhibit 1002-0770

In process **330**, the data service provider processes each credential's trust chains using its digital signature, in accordance with the digital signature algorithm specified by the credentialing agency. For example, if the Department of Defense uses the DSA to sign a credential, the data service provider will authenticate the credential using the signature authentication algorithm specified by the DSS. Furthermore, the data service provider also communicates with the issuing CA **334** to determine whether a credential has been revoked. This check is performed using methods well known in the art. For example, the CA **334** may publish a Certificate Revocation List (CRL), as described in X.509, which lists certificates that the CA has decided to revoke. Alternatively or in addition, the CA **334** may participate in OCSP. Or, the CA may designate a responder to reply to authentication requests. The data service provider uses these CRLs and OCSP responses **332** as input to standard algorithms in process **330** for processing the trust chains. The details of processing the trust chains are described more fully below.

Once the trust chain of each credential in a digital resume **320** has been processed in process **330**, the data service provider digitally signs and stores in process **340** the digital resume. The data service provider utilizes a CA for the purpose of generating a digital certificate to use in signing resumes. The data service provider's signature on the resume allows a party in possession of the resume to verify that its contents have not changed between the time of signing and the time of verification. This signature thus encourages trust between a party and a data service provider that the contents of the resume (that is, agency-issued credentials) are authentic. Such parties may include emergency management personnel at an application venue, or authentication software in a mobile electronic device **360** used to unlock sensitive application software.

A data service provider places the digital resume and digital signature in a container **344**, and place the container into trusted storage **342**. The trusted storage **342** may be located at the data storage venue where the resume was digitally signed, or it may be located in federated storage at another data storage venue. Alternatively or in addition, the data service provider transmits the signed resume to a federated storage network **350**. A mobile electronic device **360** may then download the signed resume from the federated storage network **350** for use in registering and enabling the device, as described more fully below.

Petitioner Exhibit 1002-0771

Also, a data service provider may generate an index of credentials, matching to each credential a list of digital resumes containing that credential.

In addition to issuing credential certificates, agencies will have occasion from time to time to revoke certificates. Several types of credentials routinely expire after a fixed period of time. A familiar example of a regularly-expiring credential is a driver's license. An agency may also revoke credentials irregularly, due to the discovery of fault within the agency itself. For example, a DMV may revoke a driver's license because it discovers that the clerk who issued the license did so fraudulently, or because the clerk fraudulently obtained employment at the agency. In one embodiment, an agency generates and publishes from an agency venue a Certificate Revocation List (CRL) under well-known PKI algorithms, in order to notify those relying on its credential certificates that some of those certificates should not be honored. In accordance with another embodiment, the agency venue participates in OCSP, described above, or use another protocol for notifying third parties that a certificate has been revoked.

Fig. 4 is a block diagram of a process by which digital resumes are updated to account for revoked credentials, in accordance with an embodiment of the invention. A data service provider begins the revocation process **400** by gathering and processing CRLs in process **410** from each of several agency venues. The data service provider may perform this task on a preset schedule, typically once per day. The process for gathering a CRL from an agency venue is well known in the art of PKI. For each list gathered, the data service provider then can search through an index of credentials in process **420** to identify which digital resumes contain those certificates which are revoked. If a resume is identified, its trust chains are processed according to the processes depicted in **Fig. 5** through **Fig. 7**, more fully described below, and represented as process **430**. The processing results in a yes-or-no decision in process **440** whether to revoke the resume or any particular credential certificate within the resume. The use of revocation lists encourages trust between an agency and a data service provider that credentials stored by the provider are still valid and should be honored.

Once a data service provider has processed each resume, it may update any party which relies on having timely and accurate resumes. Depending on the outcome of process **440**, a data service provider in process **442** may send the party a confirmation notice if no updates occurred. Alternatively, if the outcome of process **440** triggers a revocation, then in

Petitioner Exhibit 1002-0772

process **444** a data service provider stores, in storage **446**, a revocation for auditing and efficient processing of later revocations, and in process **448** a revocation message is sent. The storage **446** may be on-site local storage. Alternatively in lieu of local storage, or in addition to it, there may be employed remote trusted storage identified as item **452**, accessible via federated storage network **450**. In the case where only a part of the resume was revoked, the provider first creates a new resume not containing the revoked credential and places it in signed container **454**. The data service provider sends the container to a trusted storage **452** located at a data storage venue under its control, or under the control of another trusted data service provider in federated storage network **450**. The newly signed and updated resume is then sent to a mobile electronic device **460**, such as a cellular telephone. Special-purpose software on the phone can replace a stored resume with an updated resume, or remove a revoked resume. Frequent and reliable re-signing of resumes encourages trust between a data service provider and a party relying on credentials contained in a resume that those credentials are still valid and should be honored.

Summary Certificates

A summary certificate is an electronic document issued by a trusted authority which incorporates a digital signature to associate a primary credential with one or more secondary credentials upon which the issuance of the primary credential relied. A summary certificate captures relationships between credentials, in an analogous manner to the way prior art PKI trust chains capture relationships between identities.

Consider, by way of illustration, a driver's license. Typically, a DMV will issue a driver's license to an individual only after the individual has presented an agent with several forms of identification. An agency may first verify that the credentials were properly issued, and then weigh their information to make a decision whether to issue a license. If the identification documents are digital, the agency may use a prior art PKI to verify credentials. The information used when deciding whether to issue, however, may be captured using an extended PKI in accordance with embodiments of this invention.

Perhaps an individual presents a social security card, a birth certificate, and a recent utility bill. These documents represent partial proofs of identity, citizenship, and residency respectively. The agency weighs the information contained in these certificates based upon

Petitioner Exhibit 1002-0773

the authority of the agencies issuing them – the Social Security Administration, a hospital, and a utility company. The agency may rely on the accuracy of these documents, or a subset of them, in whole or in part, when making its decision to issue the driver's license. The agency may also rely on various tests, such as an optometric examination, a written knowledge test, or a skills test. These tests may be conducted by a third party or by the agency itself. The agency may rely on doctors or agents to properly conduct these tests, and to certify that the individual has met the legal requirements for passage. An agency may choose to so rely if the doctors and agents are properly credentialed. A summary certificate, such as might be associated with an issued driver's license, is used to explicitly capture all of these indirect trusts upon which an agency formerly relied implicitly.

By capturing these indirect trusts, a summary certificate enables explicit, later re-evaluation of the basis for an agency's decision to grant an individual a credential. In the prior art PKI context, a revocation of authority of any certificate in a chain of trust causes explicit revocation of all the certificates which rely on that certificate. Extending PKI by the concept of summary certificates having multiple secondary credentials permits finer analysis than in prior art systems, potentially enabling elimination of the requirement that a single failed secondary credential would invalidate the rest of a chain of trust.

A summary certificate enables finer analysis of credentialing decisions by applying revocation policies to a group of secondary certificates. A credentialing agency may issue these policies at the same time it issues a credential certificate, or it may have already issued such policies with a prior certificate. An example policy may specify that a primary credential (e.g. a passport) will not issue unless an applicant presents one secondary credential from list A, or one secondary credential from list B and one from list C. However, an applicant may present multiple credentials from list A, each of which is sufficient to support issuing a primary credential. Alternately, an agency may revoke a secondary credential because it was due to expire, or because an individual obtained it through fraud. A summary certificate enables a later authority to distinguish among these cases. Like any certificate in prior art PKI, a summary certificate may contain an expiration date, which an agency may compare to the certificate's date of revocation. If the dates are identical, the primary issuing authority need not suspect foul play, while if they differ, further research may be warranted.

Petitioner Exhibit 1002-0774

Returning to the driver's license example, an individual seeking a license may present both a birth certificate and a passport as proof of citizenship. A DMV may rely on either document to establish this proof, but may not be legally required to rely on both. Still, both credentials are incorporated into a summary certificate. Later, if either credential turns out to be fraudulent or is revoked, the revocation policy may specify that the other secondary credential is still sufficient to support the original decision to issue a license. In such a case, the agency need not revoke the license. A similar result obtains if the agency discovers that the agent who issued the license obtained his employment through fraud. A summary certificate and associated policies can capture whether this discovery should require revoking the license.

Suppose now that the DMV merely suspects that an individual obtained a license by presenting a fraudulent birth certificate, and seeks to verify the accuracy of the certificate. The doctor who issued the certificate may have died or become mentally incompetent. In such a case, the DMV may be unable to consult the doctor who issued the certificate. Further, the hospital that issued the birth certificate may have closed, and their records lost or their whereabouts unknown. However, facts such as time and place of birth do not change, despite an inability by the individual who initially recorded them to verify the accuracy of the recording at a later time. The DMV may be satisfied if the issuing doctor was properly credentialed at the time she issued the certificate.

A summary certificate according to an embodiment can enable the DMV to investigate further, as it captures all of the data on which the decision to credential was made. In this case, the summary certificate will contain the issuing doctor's medical credentials in a nested summary certificate, signed by the credentialing agency. The doctor's medical credentials may contain, for example, a transcript from a medical school, the results of a board certification examination, or other credentials. The DMV may verify each of these credentials recursively, for example by verifying the medical school transcript credential, and proceeding to the others. If these secondary credentials are correct, then no doubt has been cast upon the basis for the original issuing decision, and the DMV may rely justifiably upon the conclusion that the doctor was properly credentialed at the time she issued the certificate. Then by implication, the birth certificate was properly issued, and the DMV should not revoke the individual's driver's license.

Petitioner Exhibit 1002-0775

However, the DMV need not suffer through this verification process, as summary certificates in accordance with embodiments of this invention may be revoked recursively, as in traditional PKI. This functionality enables a data service provider to cascade revocations in novel ways. Suppose an individual goes to a hospital and obtains a birth certificate from a doctor falsely claiming to have graduated from a certain medical school. This birth certificate may, for example, falsely indicate that the individual is of a certain age, when in fact he is not. Suppose that the individual uses that birth certificate to obtain a driver's license in one state, then takes that license to a second state and exchanges it for a driver's license in the second state. The second state's DMV may not be aware if the first state's DMV eventually revokes the license upon which the second state's DMV relied. Further compounding the fraud, the individual may use the second driver's license to obtain a passport, weapons permit, security clearance, or other follow-on credential. The use of summary certificates may alleviate these problems, by recursive revocation. Thus, for example, if the original 'doctor' claims graduation from a medical school that subsequently repudiates that claim, a data service provider may, automatically and without contacting any outside agency:

(a) apply a medical board's revocation policy to revoke the doctor's primary medical credential;

(b) apply the hospital's employee-hiring revocation policy to invalidate the birth certificate issued by the doctor;

(c) apply a first state DMV's revocation policy to invalidate the first driver's license obtained using the birth certificate;

(d) apply a second state DMV's revocation policy to invalidate the second driver's license obtained using the first driver's license; and

(e) apply the State Department's revocation policy to invalidate the passport obtained using the second driver's license.

A data service provider may apply any, all, or none of these policies as warranted.

A data storage engine in accordance with embodiments of the invention may advantageously process these revocations in near real-time, or on a regular basis. Further, the engine may notify each of the authorities in the chain that the policies in place call for revoking the respective certificates. This notification saves each authority from performing

Petitioner Exhibit 1002-0776

this check itself, and may indicate to an authority that it may wish to verify its own records independently. On the other hand, each revocation is based on application of policy rules (which may be implemented in computerized processes) to the pertinent secondary credentials in a summary certificate associated with the relevant primary credential. The use of summary certificates in this fashion is conducive to computerized application of policy rules that, under appropriate conditions, may permit a cascade of revocations. In each layer of the cascade, therefore, a primary credential is evaluated analogously in relation to the secondary credentials in view of applicable policy rules. Indeed, a primary credential in one layer may become a secondary credential in the next layer.

Fig. 5 is a block diagram overview of a prior art, computer-implemented process which verifies the identity of a certificate issuer using a public key infrastructure. The test may be required, for example, in order to grant a credential holder access to restricted or sensitive functionality, or to verify that the public key information in the certificate belongs to the person named therein. The process **500** operates on a certificate **510**, which has the digital signature of a trusted authority that attests to the authenticity of its information. For a credential certificate, this authority is likely the authority that issued the credential. However, a third party seeking access to a phone's sensitive functions may have signed credential certificate **510** using a fraudulent identity certificate. Thus, a party may wish to validate the chain of trust **520** to guarantee that each digital signature was issued by an authorized party.

The process begins with verifying the signing authority's identity certificate **522**. Identity certificate **522**, however, was digitally signed by a different trusted authority – the authority that issued identity certificate **522**. For the same reasons just discussed, the identity certificate **524** used to create this identity certificate **522** may not be trusted, and further verification sought. A computer implementing the process 'walks' trust chain **520** until it reaches a root certificate **526** that is "self-signed." Identity certificate **526** has a digital signature that may be validated using the public key stored in the same identity certificate **526**. By walking and validating a chain of trust **520**, one may verify that the information in certificate **510** was issued by an authorized agency, and reach a decision **530** whether it should be trusted. For each certificate in the chain, it is necessary to use process **540** to initiate a request for current status of the certificate so as to cause retrieval in process **550** of

Petitioner Exhibit 1002-0777

certificate status. This information is used in validation of the chain. A failure in trust chain **520** will cause a submitted certificate **510** to fail the test.

There are currently several different methods to verify certificates. For example, each intermediate identity certificate may be revoked using a CRL published by the trusted authority which issued the certificate. The root certificate may be revoked using a CRL issued by the root authority, as it self-signed the certificate. Alternately or in addition, certificates may be revoked using another protocol, such as OCSP. Referring back to **Fig. 1**, data storage venue **120** is depicted with an optional OCSP responder **126** for this purpose. Validating software, typically located on the device having the sensitive application, may check the CRL for each trusted authority recursively.

Fig. 6 is a block diagram overview of a process by which certificates are verified using an extended public key infrastructure in accordance with an embodiment of the invention. In this embodiment, public key infrastructure is extended by introducing the concept of a summary certificate. The process begins, as before, with a credential certificate or summary certificate **610** having data whose validity must be determined. A computer may optionally walk trust chain **620** as before to verify the identity of the signer of certificate **610**. (Alternatively, revocations may be processed in a batch mode as described above in connection with **Fig. 4**.) If certificate **610** is a summary certificate, it represents a primary credential that relies upon several secondary credentials for its validity. The identity chain of trust and the hierarchy of credentials for each of these secondary credentials may be checked as well, to determine whether they all remain valid. Thus for each secondary certificate in the chain, there may be employed process **640** to initiate a request for current status of the secondary certificate so as to cause retrieval in process **650** of secondary certificate status. This secondary credential information is made available for decision-making in relation to the primary credential. A data service provider may then apply policies determined by the agency issuing the certificate, to decide whether the agency would revoke the primary credential due to the revocation of one or more secondary credentials. For example, if a secondary credential is invalid due to a broken chain of trust, the policy may be to revoke the primary credential or not to revoke it, depending on which secondary credential is invalid.

Further, an identity certificate **630** may also be a summary certificate. This situation arises if a trusted authority used several credentials to prove its identity to an 'upstream'

Petitioner Exhibit 1002-0778

trusted authority which issued certificate **630**. In such a case, if the upstream authority discovers a fraud, it can revoke intermediate identity certificate **630**, thereby implicitly revoking certificate **622** and certificate **610** in accordance with existing PKI standards. Here, the credential represented by the identity certificate is the authority to attest to third-party information. Persons skilled in the art should recognize other, similar ways to extend existing PKI systems using summary certificates.

Fig. **7** is a block diagram detail of a process by which certificates are verified using a public key infrastructure in accordance with an embodiment of the invention. As discussed above, various agencies **710** issue credential certificates, including summary certificates. Certificates may be issued by, without limitation, a government agency CA **712**, a DMV CA **714**, a public library CA **716**, or a hospital or medical professional CA **718**. An agency may also issue a CRL, or participate in OCSP, in order to revoke certificates. Process **700** begins after agencies have issued credential certificates that a data service provider has collected. Some of these certificates may be summary certificates. The data service provider may participate in OCSP, whereby the provider accesses a responder network **720** of OCSP participating responders. The responder network **720** publishes certificate revocations **722** as they are received, in accordance with the OCSP standard. The revocations are received by a summary certificate policy engine **730**.

The summary certificate policy engine **730** determines whether or not a digital resume, or a given summary certificate within a digital resume, should be revoked. The policy engine **730** may maintain a reverse index, wherein each credential is associated to a list of one or more summary certificates containing the credential. As summary certificates are added to data storage, they are added to the index. Agencies issuing summary certificates may transmit an accompanying revocation policy that captures the complex interactions between secondary credentials, as described above. The policy engine **730** stores these policies, which allow the engine to later determine whether a primary credential should be revoked in response to the revocation of a secondary credential.

During normal operation, the engine **730** receives credential revocations from the responder network **720**. For each credential that is revoked, the engine retrieves from the reverse index the summary certificates associated to that credential. Some digital resumes may not contain a summary certificate associated with the revoked certificate. For these

Petitioner Exhibit 1002-0779

digital resumes, the engine **730** need not perform any action – the architecture of the system guarantees that a trust chain using that summary certificate is still valid. Some digital resumes will contain a summary certificate associated with the revoked certificate. For each of these summary certificates, the engine **730** applies the associated policy to determine whether to revoke the summary certificate, given that the secondary credential was revoked. If the policy is to revoke the certificate, the data service provider may publish this information to its own OCSP responder **732**, depicted in **Fig. 1** as responder **126**. A relying party **740**, such as a first responder possessing a mobile electronic device, may access the revocation notice from OCSP responder **732**.

Even if policy engine **730** does not revoke a summary certificate, a relying party **740** may be interested to know that a credentialing agency has revoked a credential on which the primary credential relies. In such circumstances, a relying party may subscribe with the data service provider to receive such 'partial' revocations independently. If this is the case, the policy engine results **750** are separately transmitted to a relying party **740**. In one embodiment of the invention, a data service provider may initiate contact, informing **760** relying parties of revocations. In another embodiment, a relying party **740** may contact a data service provider.

Virtual Smartcards

In prior art PKI systems, smartcards have cryptographic secrets, such as private encryption keys, that should only be used by one individual. An individual having a smartcard authenticates his ownership of those secrets by cradling the card in a device and responding to a series of challenges. A challenge may be biometric, such as collecting a fingerprint. A challenge may be knowledge-based, such as requesting a PIN or a password which only the authorized individual knows. Once the individual meets these challenges, the device allows software applications access to the cryptographic secrets stored on the smartcard (for example, by providing a PKCS #11 interface).

However, not all credentials support this mode of operation. Driver's licenses, passports, firearms permits, and many other credentials may not contain a smartcard or an HSM. Credentials such as these are not electronically verifiable, thus do not support a high level of assurance that the individual offering the credential is its true owner. Further, some

Petitioner Exhibit 1002-0780

individuals such as emergency medical personnel and hazardous materials response team members may benefit from the security features that smartcards provide. Yet a supporting infrastructure, such as a state environmental agency, may not be able to afford issuing authentication tokens to all of these personnel. At the same time, the agency may desire that sensitive information be available to the personnel at an application venue.

Even smartcards containing an HSM are subject to certain limitations. For instance, a smartcard HSM may contain the only copy of an individual's private encryption keys. If she were to lose her smartcard, or even misplace it temporarily, she would no longer be able to decrypt potentially time-critical communications sent to her. Nor would she be able to decrypt old, sensitive messages stored in an encrypted form. Additionally, she would have to request issuance of a new smartcard, incurring time and expense. If the smartcard also acted as an identity document, she may be denied entry to her workplace.

One solution to these problems is a virtual smartcard. Although the term "virtual smartcard" is known in the art, embodiments of the present invention achieve implementations that differ from the prior art. In exemplary embodiments of the present invention, a virtual smartcard is a set of computer-implemented processes, associated with an individual, which simulate an authentication token containing a hardware security module. Such a virtual smartcard is advantageously electronic in nature, and does not incur overhead costs associated with distribution of physical tokens, or the danger of being misplaced. An individual may only access her virtual smartcard if she has properly authenticated using a physical authentication token, biometric information, a secret known only to the individual such as a personal identification number (PIN), or a combination of these. In this way, the virtual smartcard may be associated with a physical credential, even if that credential is not a smartcard. In one embodiment, a virtual smartcard is associated with a single physical credential. In another embodiment, a virtual smartcard is associated with a number of different physical credentials. A single virtual smartcard may hold, for example, data associated with several credit cards, driver's licenses, bank accounts, a social security number, passport, or any combination of these. A virtual smartcard may act as a unified, secure mechanism by which a person may maintain and protect his credential data against the loss of a physical smartcard or of a non-smartcard credential, using ordinary PKI techniques.

Petitioner Exhibit 1002-0781

A virtual smartcard may have a unique set of public and private keys, different from those of a physical smartcard to which it is associated. However, a virtual smartcard can represent the data contained in the physical smartcard or other physical credential or token. Thus, if a person misplaces a physical token, such as a physical smartcard containing encryption keys, she may still access the keys if she had previously associated a virtual smartcard with the physical one. Additionally, the person may notify a data service provider of the loss, and the data service provider may place the certificate for the physical token in a certificate revocation list or publish it through OCSP. Meanwhile, the person may inform others to substitute the virtual smartcard certificate for the physical smartcard certificate. Since a virtual smartcard may emulate traditional PKI functions such as digital signing and message decrypting, and because the data encryption keys contained by the former may be the same as those in the latter even if the signing keys differ, the change may be nearly transparent to an end user of the PKI.

An individual may request access to a virtual smartcard using a networking device, such as a mobile electronic device in accordance with embodiments of the invention. The networking device securely communicates with a data service provider that provides the virtual smartcard. The data service provider replies with a series of challenges, similar to traditional PKI. When the individual meets these challenges, the data service provider allows the authenticated networking device to access the secrets stored by the virtual smartcard.

A virtual smartcard is used in one embodiment to encrypt sensitive data, such as a digital resume, so that only the individual associated with the resume may read it. A virtual smartcard is used in another embodiment to encrypt communications between individuals using mobile electronic devices. In another embodiment, a virtual smartcard is used to digitally sign email sent by an individual. It will be understood that a virtual smartcard may be used for other purposes that a traditional physical smartcard enables.

Fig. 8 is a block diagram of a process by which a person may create a virtual smartcard in accordance with an embodiment of the invention. The process begins with a first responder or other party **810**. The party may optionally possess a smartcard **840** having a hardware security module (HSM). Party **810** cradles smartcard **840** in a mobile electronic device in accordance with an embodiment of this invention. If the individual already has a smartcard, it may be used. If not, one may be provided by another party, such as a guard at a

Petitioner Exhibit 1002-0782

visitor control center. In the latter case, the individual may return to visitor control to access the virtual smartcard each time the certificate in resume container **884** expires. Next, in process **820** the device captures identity credentials, including biometrics like a fingerprint, or a secret known only to the individual. The electronic device uses smartcard software **830** on the mobile electronic device to transfer these identity credentials to smartcard firmware **842**, which generates encryption keys using the smartcard HSM in process **844**. Smartcard **840** stores private keys generated in the HSM for maximum security and later use. Software process **850** copies encryption keys from the smartcard, and collects information pertaining to the virtual smartcard in a storage certificate **852**. The mobile electronic device signs the certificate to prove its origin. The certificate **852** is packaged for transmission in process **860**, and sent via a federated storage network **870** to data storage venue **880**. There, a data service provider creates a record of the cryptographic keys, and provides an interface to accessing them. This interface may be implemented in accordance with smartcard interface standards, for example PKCS #11, thereby presenting to accessing applications the appearance of an interface with a real, physical smartcard. The data storage venue may use the virtual smartcard to issue an identity certificate **882**, or digitally sign the digital resume **884** of user **810** in accordance with PKI standards.

In an alternate embodiment, process **800** is performed without a smartcard **840**. Instead, a computer having a host operating system provides the cryptographic services required. In such an embodiment, smartcard **840** is replaced a software application programming interface, and communications processes **830** and **850** are replaced by software functions not relating to operating a smartcard, but that otherwise perform analogous operations.

Fig. 9 is a block diagram of a process by which a person may enable a mobile electronic device in accordance with an embodiment of the invention. At the completion of process **236**, a mobile electronic device, such as phone **910**, contains sensitive software applications. These applications may remain on the phone for an extended duration, during which the phone may pass out of the immediate control and possession of the first responder who registered it. To maintain maximum security of sensitive data, it is advantageous that a phone be disabled when not in use by an authorized first responder. A phone may disable

Petitioner Exhibit 1002-0783

access to sensitive applications and data when it is turned off, or after a fixed period of power-on idling.

Process **900** may be used to enable access to applications on a phone **910** in accordance with an embodiment of the invention. The phone first captures identity proofs, such as biometrics and knowledge challenges, in process **920**, from a user **902**. Once the identity proofs are assembled, process **930** transmits them securely via a storage network **940** to a data service provider **950**. Next, process **951** locates a digital resume associated with the user **902** using the received identity proofs and a reverse index in accordance with embodiments of the invention. In process **952** the data service provider **950** validates the trust chains for each credential certificate and summary certificate contained in the resume. This validation process serves two purposes: first, to verify the credentials presented to unlock the phone **910**, and second, to update the digital resume of user **902**.

In one embodiment, the data service provider applies revocation policies in process **954** to determine whether the credentials presented are still valid, and whether the individual's digital resume has been revoked. If the presented credentials are invalid, in process **956** the service provider transmits an INVALID message. If they are valid, the service provider in process **958** transmits a VALID message along with the updated digital resume. It transmits this decision to the phone, and the phone receives this data in process **960**. The phone then enables applications and updates the resume in process **970**. If the first responder's credentials are not valid, the phone will not enable access to the sensitive applications. If the credentials are valid, the phone then may enable access to at least some of the applications or data based on the resume that it received.

Each digital resume may contain dozens or hundreds of credentials. It may be inefficient to transmit the digital resume throughout a storage network or to phone **910**. However, a digital storage provider may advantageously transmit a digest of a digital resume, rather than the resume itself. A digest is as useful for validating a resume as the resume itself, because any change in a resume produces a different digest. (Also, referring to **Fig. 2**, the digest of the resume can be used as 'credential data' during authentication in process **242**.) The phone compares the received digest **960** to a digest already stored in the phone. If they are identical, then the mathematical properties of the digest hashing function strongly indicate that the individual's digital resume has not changed since the last time such

Petitioner Exhibit 1002-0784

a request was made. The phone may therefore enable the same applications as the last time the phone was activated. If the two digests are different, the phone may request from data service provider **950** that a new copy of the entire digital resume be sent to the phone, or that some portion of the digital resume be sent to the phone. In response the data service provider matches identity proofs it received from the phone with a virtual smartcard associated with user **902**, the virtual smartcard previously established in accordance with an embodiment of this invention as in process **800**. The data service provider encrypts the digital resume using the user's virtual smartcard, and securely transmits it to the phone. Now the phone may use up-to-date resume data to determine which applications and data the user should be allowed to access, and enable the corresponding software. It should be noted that several of the data transmissions described above may be combined for communications efficiency, using methods which should be apparent to those skilled in the art.

In the prior art, a device seeking to verify a set of credentials would verify each trust chain in a series. In particular, the device would consume network resources to download credentials and to validate digital signatures serially, and consume time to process the signatures. However, in embodiments of this invention, a data service provider, rather than the device, consumes the computing resources to check each credential's validity on demand. Embodiments of this invention thus advantageously allow a central service provider with large computing resources to process the trust chains, allowing for faster response time. Also, it is advantageous to transmit a resume digest instead of a resume. To authenticate user access, a mobile electronic device need not process a digital resume, but need only determine whether the digital resume has changed. Thus, a digital service provider need not always transmit the entire digital resume to the device, only whether it has changed. Transmitting only a digest saves computing resources, networking resources, and time. As a further advantage, the device need only verify a single digital signature of the data service provider attached to a resume digest, to determine that an entire digital resume of credential certificates and summary certificates has not changed. The phone may thus determine implicitly that none of the certificates in the digital resume has been revoked, by validating a single identity certificate.

The above process **900** for enabling a phone may be applied in a variety of situations. For example, in one embodiment the phone belongs to an ordinary citizen who is involved in

Petitioner Exhibit 1002-0785

a traffic accident. A first responder, such as a police officer or emergency medical technician, cradles his own smartcard in the phone **910**, and answers the phone's authentication challenges. This data is transmitted to a data service provider according to process **900** to access the first responder's virtual smartcard and download his digital resume. The phone then accesses the resume to determine, for example, that an EMT should be allowed to access the individual's medical history, or that a police officer should be allowed to access the individual's licensing, insurance, and vehicle registration data. Those skilled in the art may easily envision other uses to which this process may be applied and remain within the scope of the invention.

Batch Certificate Processing

Batch processing may be used to transact operations associated with large numbers of mobile electronic devices. Those mobile electronic devices carrying credentials in accordance with embodiments herein can have their credential certificates updated to reflect any revocations as a result of the batch processing. Classes of these mobile devices, such as smart mobile telephones, can be configured to cause such updates automatically whenever the devices are connected to their respective networks. With automatic updating, a mobile device that has been connected to the network for a period of time can be reasonably assumed to have updated credentials and therefore can be used immediately for a transaction, without the need for any further interaction with a remote source. This approach, discussed in the following paragraphs, is efficient and eliminates the need for network traffic and processing associated with separate authentication of each transaction. A flag can be pushed, for example, on a daily basis, to each mobile device indicating the continued validity of its credential, and this flag can be used as an indicia of validity of the credential for a transaction. Further, each transaction can be the subject of a direct query to a credential server to confirm validity of the relevant credential.

In using the mobile device in the fashion described, a user first authenticates himself to the device. Such authentication may take the form, for example, of entering a personal identification code (PIN) and swiping a finger for a fingerprint, all as described above in connection with **Fig. 2B**. This authentication (following an internal verification of the consistency of the user's credentials as explained in connection with **Fig. 2B**) permits the

Petitioner Exhibit 1002-0786

user to expose the user's credentials stored on the mobile device for use in a secure transaction, such as a retail purchase on credit. A party that relies on the security of the transaction, such as a merchant, using a suitable machine, obtains relevant credentials from the mobile device and keeps a log in which is stored information pertinent to each purchase. The mobile device itself keeps a log of the transactions in which it is used. A background batch process performed for example by the credit facility may compare data on merchants logs with data on logs of mobile devices, to reconcile successful transactions and detect fraudulent transactions.

Batch processing enables (among other things) rapid fraud detection, as depicted in **Fig. 10**. Batch processing also enables processing of transactions, such as micro-payments, in which a disconnected device participates, as depicted in **Figs. 27** and **28**.

Fig. 10 is a block diagram of a process, in accordance with an embodiment of the present invention, for batch processing of secured transactions using a mobile device in the manner described and for rapidly detecting fraud. The process begins with a person **1014** who has been previously authenticated to the device using process **242**. The person **1014** uses the mobile electronic device depicted as a smart phone **1012**, and the secure document **1016**, and together we have shown these as components of the identified party **1010**. The person **1014** enters into a secure transaction with a relying party **1020**, using the phone **1012** and the secure document **1016**. Additionally, the relying party (such as a merchant) will supply equipment such as a card-swipe machine or a barcode reader to read data from the secure document **1016**. A swipe machine may read credit information from a credit card, while a barcode reader may read a two-dimensional barcode from a driver's license. In either event, both the phone **1012** and the relying party **1020** store information about the secure transaction for later comparison. At this time, the relying party **1020** may transmit a message to phone **1012**, asking whether or not to confirm the transaction.

In process **1030** the relying party sends transaction logs over a network **1040** to trusted storage **1060** hosted by a data service provider. Communication may occur at once, as each transaction occurs, or as a bulk upload. Also, phone **1012** sends its own transaction logs to trusted storage **1060**, either at once or some time later. (See discussion below in connection with **Figs. 15-18** discussing trusted storage.) In process **1070**, the data service provider compares the two logs it received to look for discrepancies in a batch process. This

Petitioner Exhibit 1002-0787

comparison may occur on a regular basis, such as every night. If the comparison determines that there is a data match, then in process **1080**, fraud is unlikely, and no further processing is necessary. However, if the comparison determines that there is not a data match, then in process **1090**, further remedial steps are taken, including launching an investigation, freezing a credit card account, or sending notices of potential fraud to the person **1014**, the relying party **1020**, a credit card company, or another party with an interest in the transaction.

There are several advantages to comparing logs in a batch process, in the manner illustrated above. By performing comparisons on a regular and frequent basis, more fraud can be detected sooner, avoiding greater losses of money during the time lost in detecting the fraud. Comparing logs may be done at a central location. Thus, more processing resources such as disk space, memory, and CPU power can be brought to bear to reconcile the logs than if the comparison were done on the phone **1014**. Also, the system may be run automatically. Such a system provides fraud detection without human intervention such as visually scanning credit card bills for suspicious-looking transactions. The system can automatically notify a card holder and a merchant, allowing both parties to the secure transaction to begin to mitigate losses quickly. Additionally, once the infrastructure for batch processing is in place, there is no absolute need for each transaction to be cleared at a central server in real time; instead such an approach is merely an option for a merchant.

Accordingly, the phone may be used optionally for transactions, even when a network is unavailable, and an individual may use phone **1012** in a 'disconnected' state. The individual may enter into several transactions consecutively, carrying a log of all transactions on phone **1012** for uploading and verification when the network becomes available again. The phone itself may keep a running total of all purchases made, and compare that to a stored credit balance. When appropriate, the phone may warn the person that their credit has been or soon will be exceeded. When connectivity is restored, or simply on a periodic basis, the phone **1012** uploads transaction data in a batch process, similar to each relying party.

A phone **1012** may be used this way, for example, as a micro-payment device. Such a device may be used to pay for a soft drink, purchase small items like stamps or candy, pay a fee at a toll booth or a parking meter, or any of a myriad of other uses that may be envisioned by those skilled in the art, because its use on each occasion need not require communication with a central server on a network. Also, phone **1012** may contain wireless

Petitioner Exhibit 1002-0788

technology such as Bluetooth to communicate with a corresponding device of the relying party **1020**, thereby implementing secure, fraud-safe, wireless micro-payments. This embodiment of the invention provides a method of providing micro transactions with minimal communications that will work in any environment and device so enabled. Dispensing devices are protected by PKI and isolated to short-range communications, thus providing a very high level of security.

Since the cell phone may have a full PKI engine, the threat of replay attacks against transaction data may be reduced as well. Current OCSP servers send data across in clear text, thereby allowing the transaction data to be copied and replayed at a later time. All communications with the phone **1012** can be fully encrypted, thereby preventing a replay even if the data were intercepted. This is because the transaction described is localized, and does not require any network services.

Fig. 27 is a block diagram of relevant processes for using a mobile electronic device to make a micro-payment in accordance with embodiments of the invention. A device may store a cached certificate verification response, such as an OCSP response, for use in a transaction in which a data authentication network is not available. The user device provides the OCSP response certificate to the retail device. The retail device uses the OCSP response to validate the user's credentials, while validating the response certificate itself with a cross-certificate it has stored. In this way, all verification may be performed without contacting an authentication network. These procedures enable non-networked retail devices, such as parking meters and vending machines, to perform certificate validation without direct access to a validation server. In particular, a non-networked retail device may only need to store a small number of trust anchors and cross-certificates, whereby the last link in the trust chain (between the user credential certificate and a cross-certificate) is provided by the mobile electronic device itself at the time of a transaction.

A response issuer may set a cached response to expire after a given length of time, determined by an amount of risk tolerance. For example, a user of a phone on which a response is stored may purposely avoid connecting to a validation network in case she knows that the credential was revoked, while to a merchant, the response appears to validate the certificate. Thus, too long of an expiration may be undesirable for some applications. On the other hand, an expiration period that is too short results in too many validation requests, and

Petitioner Exhibit 1002-0789

defeats the purpose of caching. Embodiments of the invention allow for expiration times of all lengths, including no expiration length, in which a certificate response is valid until it is expressly revoked.

The process described above may be implemented in three phases as follows. Preliminarily, for any use of the phone, in process **2710** a user authenticates herself to a phone **1012** to become an identified party, as in **Fig. 10**. Also preliminarily, in process **2720** the phone **1012** is placed in communication with a credit company **2724** using a data network **2722** and receives a certificate having credit data for the identified individual, and a certificate verification. The credit data include information such as a balance or transaction limit. The certificate verification guarantees that the credit data will be valid for a certain period of time, and may be an OCSP response or other self-expiring certificate verification. At this point the phone can be used for transactions in the manner described. Once this preparation phase is complete, the user may engage in a secure transaction at some time later when the credit card data network **2722** happens to be unavailable.

Thus, in process **2730** the user approaches a micro-payment device, for example parking meter **2742**, to initiate a transaction. Initially, in the manner previously discussed in connection with **Fig. 9**, the user authenticates himself to the phone (e.g. by entering a personal identification code and a finger swipe). As the user approaches, the phone **1012** and device **2742** then establish a communications link using a wireless technology, such as Bluetooth. In order to provide a secure communications link using public key encryption in accordance with embodiments of this invention, the phone **1012** and device **2742** each have cryptographic hardware or software to implement physical or virtual smartcard functionality as described above in connection with **Fig. 8**. In process **2740** the phone **1012** and device **2742** engage in a secure transaction, for example as shown in **Fig. 2B**. As an example of a micro-payment transaction, a parking meter **2742** sends a message indicating how much each increment of time costs, and the user makes a selection of how much time to purchase. The meter decides whether to honor the transaction, and a record is generated. (We discuss in further detail below criteria for honoring the transaction.) Both the phone **1012** and device **2742** store a record of the transaction, as indicated in **Fig. 27**. If the transaction is successful a billing record will be established on the meter's memory and on the phone and the

Petitioner Exhibit 1002-0790

available amount on the phone of credit for future charges is reduced. All transactions are digitally signed by the phone or dispending device as appropriate.

Some time after the conclusion of the transaction phase, when the credit card data network **2722** is available again, phone **1012** must reconcile its transactions with the credit company **2724** so that the user's account may be debited. Thus, in process **2750** the phone transmits records of its micro-payment transactions to the credit company, and receives updates to the credit data and certificate verification. Process **2750** is described in greater detail in connection with **Fig. 28** below.

After process **2740** the device **2742** takes a different path. In retail fee-collection embodiments such as vending machines and parking meters, the device itself is a secure transacting party. For example, over the course of a day, a parking meter **2742** may accept coins or wirelessly deduct payments from several phones **1012** by storing payment tokens (obtained by whatever method). Throughout the day, records of transactions are stored inside the meter. At the end of the day, a collector may visit the parking meter **2742** and collect any physical coins stored in the meter. At the same time, in process **2760** she may wirelessly transfer the transaction log and payment tokens to her own phone (in the manner described herein), thereby 'emptying' the meter of its virtual money. She may then return with the log, along with logs from other parking meters **2742**, to a central location for batch uploading. Or, if the credit network is available from her phone, she may upload the logs and tokens to a credit card data network **2722** directly. Once both sets of logs have been uploaded to the credit card data network **2722**, the remainder of the procedures of fraud detection process described above may be applied. In particular, the transaction logs are compared. If the logs match, the appropriate credit account is charged, while if there is a discrepancy, settlement procedures may begin. Settled transactions can be archived for future reference and auditing.

In this embodiment, the parking meter **2742** need only have a short-range wireless capability to communicate with various phones **1012**, thereby saving manufacturing costs and load on the cellular networks or on wired networks, and increasing the security of the parking meter against electronic attack. Although described above in a context where a credit card data network **2722** is unavailable, the scope of this invention includes parking meters, vending machines, and similar PKI-using micro-payment devices that participate in

Petitioner Exhibit 1002-0791

such networks. Also included in the scope of the invention are devices that physically attach to a phone **1012** using a cord or cable to transfer credential data, instead of using a short- or long-range wireless connection.

Fig. 28 is a block diagram of processes in accordance with embodiments of the invention by which a mobile electronic device updates itself after a credit data network becomes available. This figure shows in more detail the process **2750**. In process **2810** the phone **1012** and credit company **2724** re-establish communications using data network **2722**. Once connected, phone **1012** uploads the log of transactions it has made for comparison with the logs uploaded by micro-payment device operators.

In process **2822** these logs are reconciled, as described above. There are three cases: the phone is uploading a record of a transaction for the second time (because a device operator has previously uploaded the record), it is uploading the record for the first time, or it is uploading a false record. In the first case, process **2822** may compare the records. If the records show an identical payment, the appropriate account may be debited in process **2824**. If the records do not match, the invalid transaction can be settled in process **2830** using known methods. In the second and third cases, there is no data to reconcile because only one copy of the transaction record is available. Thus, the record is placed into storage for a period of time that may be determined by the credit company, the user, or both. If the period expires, the purported relying party is notified that a record has been entered, and verification that the transaction occurred is requested. Thus, fraud may be detected if the relying party responds negatively to this request. If no response is forthcoming, the credit company may verify that the relying party is still conducting business, or take other remedial measures to resolve the transaction. Preferably, however, relying parties will upload their batch of records on a regular basis within the period of time specified, so that fraud may be detected sooner.

In process **2832** the credit company **2724** calculates new credit data. For example, if the phone **1012** has engaged in any transactions, the credit of the phone's user may have been decreased in process **2824**. Additionally, the user's credit limit or other pertinent information may have been changed during the time the network was unavailable. For example, the user's credit card may have expired, and the credit certificate may need to be revoked. This information is collected, then downloaded to phone **1012** in a signed

Petitioner Exhibit 1002-0792

certificate in process **2840**. At this point, the phone **1012** is synchronized with the current credit information. If the authorization to conduct secure transactions has not been revoked or the appropriate balance reduced to zero, such transactions may resume.

During disconnected transactions such as those just described, the relying party takes a risk in accepting credentials with only an attestation on the mobile electronic device. Additionally, if a user has not entered any transactions for a time, then updating credit information from the credit company **2724** may not be necessary, and doing so would place a burden on the network **2722**. To relieve these problems, a phone **1012** in accordance with embodiments of the invention receives from a credit company **2724** a digitally signed certificate containing the credit data and an expiration time. This expiration time allows the credit company **2724** to deal with the phone **1012** under conditions wherein it will refuse to honor a transaction occurring after the time. Software or hardware in the phone **1012** may compare an internal clock against the expiration time in the certificate. If the current time is after the expiration time, the phone **1012** may disable secure transactions that use an account associated with the credit data in the certificate (although other certificates and accounts may be available for conducting transactions). The phone may do so by revoking the certificate itself. As an added risk-abatement measure, a phone whose data has not been synchronized with a credit company for a period of time may be programmed by the credit company to reduce the balance available on the phone for use in secured transactions. As an additional measure, relying party systems may request from phone **1012** network connection data, including the time the device last synchronized, and how long the device was on the network. Then the relying party system can decide, based on desired parameters, how much risk to accept vis-à-vis a particular transaction.

In a related embodiment, the phone may maintain a record of when it was last connected to the network and for how long the network connection was maintained. In this embodiment, the credential is assumed to be good unless there is deemed to be an unacceptable risk that it has been revoked. Such a record may be used by a micro-payment device or by a merchant payment system to assess risk associated with a transaction with the user of the phone. Given the batch processing of certificate revocations, if the phone is connected to a network for a reasonable length of time, for example more than five minutes, there may be reasonable assurance that a certificate revocation that occurred during the last

Petitioner Exhibit 1002-0793

batch processing will be communicated to the phone, rendering the relevant credential invalid were a revocation effectuated. This approach works best when the phone's software and that of the server with which the phone is in communication is configured to make credential revocation a matter for priority communication. Consequently, if the data show, for example, that the phone is actively connected to the network at the time of the transaction, and has been connected to the network for the past five hours, the micro-payment device or the merchant payment system may be configured to accept the credential and enter into the transaction if the risk is deemed reasonable in view of the network connection data on the phone. On the other hand if the data show that the phone has not been connected to the network for more than a week, the micro-payment device or the merchant payment system may be programmed to refuse the transaction and send a message to the user to connect the phone to the network before seeking again to execute the transaction.

It will be understood that the system in various embodiments described above may be used without the need for a phone **1012** to store a long-term certificate. In one alternate embodiment, the credit company 'pushes' credit certificates to a phone **1012** on a regular basis, daily for example. This embodiment mitigates merchant risk further than the system described above, as the credit data is guaranteed to be no older than one day, but it requires more network traffic. Thus, the credit company may charge the user or merchant a fee for providing this service. In another embodiment, the phone **1012** or device **2742** contacts the credit company for each transaction. This embodiment mitigates merchant risk almost entirely, but requires the most network traffic of all. A credit company may charge a high fee for providing this service.

Physical Access Control

Fig. 11 is a block diagram of a process by which a person may register a device in accordance with an embodiment of the invention to permit physical access to a secured area. Some large organizations have a problem providing their employees with uniform physical access to various locations under their control. For example, a large corporation may have acquired many offices and buildings in different locations through acquisitions or growth. Each building or office campus may have a separate access control system that relies on a local access control system headend. A headend will control physical access to various

Petitioner Exhibit 1002-0794

portions of the physical location, for example by locking and unlocking doors and gates. The computer systems that control the headends may not be interoperable with the systems at other locations, making common access mechanisms difficult without custom software development at a cost in time and money. However, in embodiments of this invention, access control data is stored on a mobile electronic device and retrieved locally by a guard, substantially mitigating these costs. As we have described and defined above, authorization of access is a type of a transaction, but for the purposes of **Fig. 11**, the type of transaction involves physical access.

Access control in accordance with the embodiment of **Fig. 11** is implemented in two parts. During the first part, user data **1110** and rights data **1112** are entered into a database **1122** contained within an access control system headend **1120**. User data **1110** includes routine identification information, such as a name, address, telephone number, employee ID, administrative rank (such as employee, manager, or director), job title, or other similar data which may be later used to identify a person. Rights data **1112** includes access rights tied to an individual, job title, or administrative rank. For example, the organization may decide that only an employee with job title including "accountant" may have access to rooms containing financial data of the organization; or, employee John Smith may have access to only public areas. Once database entry is complete, a person may use the local access control system to enter protected areas on the site where the system is installed. Access control systems of this type are known in the art, for example subway turnstiles. In one embodiment, access data for off-site locations is also stored in the headend **1120**.

In the second part of access control in accordance with the embodiment of **Fig. 11**, a user seeks access to an off-site protected area. For example, an employee working at a headquarters campus traveling to a satellite office requires access to restricted areas there. A person **1130** determines that the user must have access at the remote site. Person **1130** may be a security officer, the user herself, her manager, a human resources staffer, or any other authorized person. Person **1130** initiates in process **1140** a query to the access control system headend **1120** using a computer (not shown), to retrieve the user's access rights data for the off-site location from database **1122**. Using the retrieved results, in process **1150** the computer creates a file containing the list of access rights for the off-site location. The computer first stores the file in local storage **1152**. This record of the rights may be used

Petitioner Exhibit 1002-0795

later for auditing and for determining what rights a traveling user has at any given moment. The file is also transferred to the user's phone **1170**, a device in accordance with embodiments of this invention, through communications network **1160**.

Fig. 12 is a block diagram of a process by which a person may use a device in accordance with an embodiment of the invention to access a secured area. Once a phone has been set up using the process of **Fig. 11**, a visitor uses the processes **1200** shown in **Fig. 12** to access various secure locations at a remote location. A secure location may be a building, a floor of a building, a room in a building, or any other area controlled by an access control system. These processes allow a visitor to securely identify herself to a perimeter control system guarding a secure area and transfer her access rights into the local access control system headend. After the rights have been transferred, the visitor may access secure areas inside the perimeter. The processes **1200** do not require contacting a remote location (such as a security office at a headquarters building) for authorization.

A user **1210** possessing a phone **1220** first approaches a perimeter control system **1240**. The system **1240** may be a guard with a computer at a gate, or it may be automatic, consisting entirely of electronic devices. When phone **1220** is within range to communicate with perimeter control system **1240**, the phone transmits the rights file it previously received in the embodiment of **Fig. 11** to the control system in process **1230**. The communications may be wireless, in which case the channel may be encrypted using the phone's built-in hardware security module. Or, for example, the user may dock the phone in a cradle connected to the control system. Once perimeter control system **1240** receives the rights file, then in process **1250** there is a determination of validity of the file. This process may be automatic or require human intervention from a security officer. Validity determination may include ensuring that the rights file is properly decrypted; checking the identity claimed in the file against physical credentials presented by the visitor; accessing the certificate associated with the rights file and verifying the digital signature; checking for revocation of this certificate; or any other appropriate validity check.

The perimeter control system **1240** (or the security officer, if the file requires manual verification) in process **1260** applies the results of the validity determination of process **1250** in deciding whether the visitor has the proper rights to enter any secured areas. If not, as in case **1270**, the perimeter control system **1240** stops processing and thus grants no access.

Petitioner Exhibit 1002-0796

Alternatively or in addition, the control system **1240** may take appropriate remedial measures, such as alerting security of an attempted unauthorized access. If the decision in process **1260** is that the visitor has acceptable credentials, he may be granted access, as in case **1280**. At this time, any secure applications or data in the phone relating to the secure area may be enabled by the perimeter control system **1240**. In one embodiment, a guard may issue the visitor a badge for display as identification. In another embodiment, the perimeter control system **1240** may log the visitor's entry in an audit record. To grant a user access to secured areas within the perimeter, the system may store the verified access rights file in its local access control system headend **1290**. This last process may require the phone to process the rights file into a given data format so that it may be recognized by the headend. At the conclusion of the processes of **Figs. 11** and **12**, a user has transferred an access control rights file from one site to another site, allowing the user access to secured areas at the second site, without the need for security personnel at the second site to contact the first site to verify her permissions or to authorize the user to access particular secured areas through manual data entry.

Fig. 13 is a block diagram of a process for updating a device in accordance with an embodiment of the invention to alter or revoke permission to access a secured area. On a company campus such as that described above, it may be necessary from time to time to alter the rights granted to a visitor. For example, an organization may have a standing policy to issue day pass cards to visitors, and revoke them at the end of each business day. Or, it may be policy to revoke a pass automatically if a visitor attempts to enter a secure area for which he has no clearance. Or, a visitor may legitimately need access to a location for which she was not originally granted clearance. An access control system in an embodiment of this invention may propagate rights changes so that access control headends have up-to-date information about these changes.

Process **1300** begins, as before, with organization headends **1310**. A single organization may have several headends. For example, there may be a headend **1312** at a corporate headquarters, a headend **1314** at a satellite campus, and a headend **1316** in a building at the satellite campus. Additional headends may be employed for, among other purposes, providing access rights information for secure areas controlled by several agencies or organizations with equal or hierarchical authority to issue access rights. In process **1320**,

Petitioner Exhibit 1002-0797

the headends **1310** publish rights data and rights data changes for authorized remote users to a campus-wide or organization-wide communications network **1330**. These changes propagate to a phone **1340** possessed by a visitor, which updates its rights data to reflect the changes. From this point forward, the phone will allow the visitor to access only those secure areas permitted by the new rights, even if the local access control system headend has not received a permissions update. Additionally or alternatively, in process **1350** headends **1310** may publish revocation lists to entirely revoke access rights for one or more visitors. A list travels through the communications network **1330** to arrive at phone **1340**, which responds by revoking the visitor's access rights to all secure areas. Alternatively or in addition, local headend **1360** may collect rights changes and revocation lists, if it did not issue these in the first place. Having local headend **1360** collect revocations provides an alternate means for altering or revoking a visitor's access to secured areas. Local headend system **1360** is consulted to determine a visitor's access rights in the case that headends **1310** cannot be contacted, or as a local cache to reduce communication with headends **1310**.

Trusted Data Storage

Fig. 14 is a schematic block diagram showing the relevant parts of a prior art system for providing business information. A business or agency **1410** may have one or more servers **1412** for providing business data. Such business data may include, for example, purchase order forms, tracking numbers, account numbers, balances, and other information that business **1410** wishes to make available to its customers, contractors, vendors, or other business associates. The servers **1412** may be, for example, web servers, or may be other types of data servers that rely on a known communications protocol for getting information. A small business may maintain only one server, while a larger business may maintain several servers **1412**. Data consumers, such as customer computer **1420**, contractor computer **1422**, and user smart phone **1424**, retrieve data from servers **1412** as needed. To do so, data consumers access the servers **1412** by sending requests through communication network **1430**, and receive responses from the servers **1412**. This access is indicated by lines **1426**.

Several problems exist with this model. Servers **1412** must communicate with several clients including desktop computers **1420** and **1422** and smart phone **1424**, perhaps simultaneously. This communication, represented by heavy line **1440**, may overwhelm the

Petitioner Exhibit 1002-0798

business's available resources, such as bandwidth or server processing capacity. Thus, communication may incur heavy bandwidth costs for the business, or force the business to purchase more servers **1412**. In addition, a business may internally agree on a service level for customer-facing systems, such as 99.99% uptime ("four-nines", or about one hour per year of service interruption). This level of service requires substantial investment in information technology infrastructure, which may be better spent on other business functions. Alternate methods of communicating business information, such as by email, suffer from other problems. For example, email is generally insecure, and email messages containing confidential business data may be intercepted or lost. Email may be made secure through the use of encryption, but such encrypted systems are not in widespread use, and require significant knowledge and training on the part of end users to work effectively.

Fig. 15A is a schematic block diagram showing the relevant parts of a system for providing business information in accordance with another embodiment of the present invention. In this embodiment, a data service provider provides trusted storage for business data other than resumes. The data service provider allocates a segregated storage area for each business, and allows only that business to write data into the segregated storage area. Access to the storage area may be granted only upon a data service provider's validating a business's identity, by using a digital signature for example. A business, in turn, accesses the trusted storage using a URL or other address that can be controlled by the data service provider. In this way, all parties are guaranteed that only valid business data from the business is stored in the segregated storage area. The data service provider then allows direct access to the trusted storage by data consumers. A PKI system in accordance with embodiments of this invention is used to facilitate the above process.

Continuing the discussion of **Fig. 15A**, business or agency **1510** acts as a trusted data source. A method in accordance with this embodiment may allow business **1510** to maintain only a single computer **1512**, although some businesses may employ more than one. Computer **1512** creates a digitally signed business document containing business data. Ultimately the digitally signed business document is hosted as item **1524** in trusted storage area **1522**. Initially, however the computer **1512** securely transmits the digitally signed business document over line **1514** to one of several servers **1520**, which may be a web server hosted by a data service provider. Computer **1512** may use a URL or other addressing device

Petitioner Exhibit 1002-0799

to designate the particular trusted storage it wishes to access. Server **1520** has a receiver for securely receiving the data from computer **1512**. The server **1520** verifies the identity of the business **1510** using public key encryption, as described above. Server **1520** may have a hardware or software processor to perform the necessary encryption algorithms to verify the identity of business **1510**. If the identity of the business is verified, server **1520** stores the data in trusted storage **1522**, which is configured so as to accept data only from business **1510**. Trusted storage **1522** is embodied as a physical data storage medium, such as a hard disk drive, or a portion of a hard disk drive. Then, server **1520** transmits the data to data consumers including desktop computers **1420** and **1422**, and mobile electronic device (implemented as a smart phone) **1424** by communication network **1430**. Server **1520** verifies the identity of a data consumer using its processor, and provides the consumer access to trusted storage via link **1534**. Server **1520** guarantees, using public key encryption, that only those areas of trusted storage **1522** for business **1510** are visible or readable to a data consumer, and that they are not visible to any other party (except the trusted data source). Data consumer access **1530** may be either "pull", if the data consumers request the data, or "push", if the data consumers subscribe to a service that sends them data as it becomes available from the business **1510**. In a "push" model, the processor in server **1520** applies business rules relating to the timing of storage and forwarding of the data to a particular data consumer, in order to decide when to forward the data. Both "push" and "pull" systems are within the scope of this invention.

Trusted data may be securely transferred from a trusted data source to a data service provider using a public key infrastructure. The ultimate data recipient may be, for example, the user of computer **1420** or smart phone **1424**. In order to ensure that the trusted data may be viewed only by the data recipient, and not the data service provider, computer **1512** uses a PKI to access a public key associated with the recipient and encrypt the trusted data using this public key, according to a well-known encryption algorithm. In addition, computer **1512** packages the trusted data with other information that uniquely identifies the data recipient, for example a PKI certificate number, an email address, a URL, a postal address, or a phone number. All of this data is combined with a digital signature of business **1510**, to form a digitally signed document **1524**. This document is transmitted to server **1520** for storage as shown. Server **1520** uses a PKI to access a public key of business **1510**, in order to verify

Petitioner Exhibit 1002-0800

the digital signature, providing assurances that the document was created by business **1510**, and not a fourth, possibly malicious party. In another embodiment, the encrypted data is hashed to form a digest, which is digitally signed instead of the encrypted data itself. A digest is usually much smaller than the encrypted data, and thus lends itself to faster signing and verification. Furthermore, a digest may be uniquely associated with the encrypted data, according to the mathematical properties of the hash function used to create the digest from the encrypted data. Once the data's origin has been positively identified, the data service provider uses the uniquely identifying information in the document to associate the data recipient with the document for later transmittal.

As an additional layer of security, computer **1512** may use a PKI to access a public key for the data service provider, to encrypt the digitally signed document **1524** in a manner that only the data service provider may decrypt. If this additional step is taken, the data service provider may decrypt the encrypted digitally signed document using its own private key to yield document **1524**. However, the encrypted data within document **1524** cannot be decrypted by the data service provider, which does not have access to the private key of the data recipient. This layer of security should be viewed separately from a digital signature -- while it obscures the contents of the transmission from fourth parties, it does not otherwise provide assurances that the sender vouches for those contents.

Trusted data also may be securely transferred from a data service provider to a data recipient using a public key infrastructure. Using a method similar to that described in the previous paragraph, server **1520** may use a PKI to access a public key for a computing device of the recipient, such as computer **1420** or smart phone **1424**. Such a device public key was established previously in accordance with an embodiment of the invention. Server **1520** encrypts digitally signed document **1524** using this public key, and transmits it to the computing device. In this way, the contents of the transmission are obscured from fourth parties. The computing device then decrypts the transmission using its private key, which is stored on a hardware security module internal to the device, as described above. The digitally signed document **1524** is then stored on the computing device.

When the data recipient wishes to view the data, she first authenticates herself to the device using a method in accordance with embodiments of the invention, as described above. Once authenticated, she may access the digitally signed document. The user accesses a PKI

Petitioner Exhibit 1002-0801

to obtain the public key for the document's signer (business **1510**), and verifies the signature using well-known methods. Once satisfied of the document's authenticity, the user uses her own private key to decrypt the data within, and uses the decrypted, trusted data for any purpose. The user's own private key may be stored, for example, on a removable smartcard, or in a virtual smartcard in accordance with an embodiment of this invention. As above, the business **1510** may have digitally signed a digest of the encrypted data, rather than the encrypted data. In this alternate embodiment, the end user may verify the signature of the digest before decrypting the data.

The apparatus of **Fig. 15A** has several advantages over the prior art. First, there are cost advantages. By transmitting secure documents to a trusted third party, a business such as **1510** may save substantial amounts of money in infrastructure development and bandwidth costs. Computer **1512** need not service large amounts of data requests, as this work may be done by the third party. A data service provider centralizes the costs of infrastructure development, and benefits from economies of scale. Several servers **1520** may be employed by a data services provider at a single storage venue, and a services provider may have several storage venues to provide availability. The system lends itself to simple automation, saving a business labor costs over the long term. Next, there are service-level advantages. Computer **1512** need not be always available to service customer requests. Availability of the data can be guaranteed by the data service provider under the terms of a service level agreement (SLA) with the business **1510**. Denial-of-service (DOS) attacks become much more difficult, as an attacker must now target the data service provider who may have countermeasures in place, rather than a small business that likely does not. And with a "push" data model, after the targeted data has been transmitted to the data consumer, a DOS attack becomes nearly impossible. Further, there are business operational advantages. The use of encryption and PKI in accordance with embodiments of the invention allows a business to honor its privacy policies for its vendors and customers. The system need not transmit to the data consumer "envelope" information, such as time of transmission, IP address, or other data that might be found in an email header. The system ensures that data was written only by the business **1510** using encryption techniques as described above. This provides a further guarantee to a data consumer, such as a business customer, that the data originated with the business, thereby reducing fraud that may be inherent in other third-party

Petitioner Exhibit 1002-0802

data storage systems. Also, the use of URLs to access a trusted data store simplifies management of data throughout the system.

Fig. 15B shows typical processes for implementing the deposit and secure access of trusted data according to the system of Fig. 15A. In accordance with the process 151, there are received from a first party a deposit of data, a digitally signed document associated with the data, as well as some form of identification of a second party for receipt of the data. In process 152, the digitally signed document is used to verify that the data were in fact sent by the first party. In process 153, the data from the first party are stored in association with the digitally signed document. Finally in process 154, the stored data are made available to the second party in a secure environment.

Fig. 16 is a flowchart showing processes in accordance with an embodiment of the present invention, to prepare a trusted storage system, such as that of Fig. 15A, for operation. A trusted storage system, such as that displayed in Fig. 15A, has three phases of operation. In the first phase, the system is initialized. In the second phase, the system receives data for trusted storage. In the third phase, a user may access data stored in trusted storage. Access may be of the "pull" variety, where the user accesses a data service provider. Access may also be of the "push" variety, where the data is already stored on an electronic device in accordance with an embodiment of the invention. Such devices include a user's phone, a computer, or other electronic device.

The initialization process of Fig. 16 begins by establishing necessary trust components of a PKI embodiment. Trusted data producers include banks, hospitals, credit card companies, utility companies, shipping companies, government agencies, and other groups or individuals that have confidential data to distribute. In particular, in process 1610 root certificates are installed on a user system, such as a phone. The certificates allow a consumer of the data to verify that the data has come from a trusted source, by validating a digital signature that may accompany the data. An example validation process is described in connection with Fig. 5. Once the certificates have been established, the system allocates storage for a particular trusted source in process 1620. Ordinarily, identity information about the source will be required by a data service provider, so that the latter may effectively determine whether any given data storage request originates from the trusted source. This identity information may be provided, for example, as a public key certificate or credential in

Petitioner Exhibit 1002-0803

accordance with embodiments of the invention. The data service provider may also allocate a URL to the storage area. Additionally in process **1620**, a data service provider may receive business rules governing data to be stored in the allocated, trusted storage space. These rules may be similar to the business policies described in connection with **Fig. 7** – they could instruct the data service provider to forward or not forward data based on a number of criteria. For example, the rules may instruct to only forward data once per day as a daily digest. This rule is appropriate where a trusted source generates many informational data messages. Or, the rules may instruct to deliver each message as it is received by the data service provider. This rule is better suited to infrequent data updates from the trusted source. Or, the rules may instruct to deliver only messages classified by the trusted source with a particular code or tag. This rule allows a trusted source to use trusted storage as an archive, while only transmitting to the end user data which is relevant to the user. Other rules falling within the scope of the invention may be envisioned by those having skill in the art. A data service provider may implement these rules using any convenient hardware or software, and methods for doing so should be readily apparent.

Each trusted source, such as a shipping company, may have many customers who desire to receive, for example, package tracking numbers and tracking updates securely. Once the rules have been established and installed, a customer (or more generally, a data consumer or user) makes a request to receive data from the trusted source. The user transmits a data message to the data service provider, which receives the request in process **1630**. The data service provider registers the user as a target of the business rules regarding forwarding of data. For example, the data service provider may store the user's identification in a database of users who should receive updates on a daily basis. Also, the data service provider may classify the user as a "pull" user or a "push" user. Classification may be done according to the wishes of the user, for example by including such a request in the subscription request. Or, classification may be done according to the business rules and policies of the trusted source, such as service-level guarantees to its customers. In another embodiment, the user sends the subscription request to the business, which forwards it to the data service provider. In this embodiment, the user need not know that the trusted storage is hosted by a data service provider. The data service provider then transmits data directly to the user's electronic device.

Petitioner Exhibit 1002-0804

In process **1640** a data service provider configures a user device, by transmitting to it an appropriate message over a secure communications link. Such communications links are described above. Data received from the trusted source is transmitted to a user's electronic device, such as a phone embodiment or a computer embodiment. Regardless of how the trusted data arrives at the user, by push or by pull, the user's electronic device may be configured to receive the data securely by receiving such a configuration message. The electronic device allocates storage space to receive the trusted data, thereby creating a trusted storage space on the device. Other functions of such configuration messages should be apparent.

Fig. 17 is a schematic block diagram showing a process of updating a trusted storage system with new business data. The process begins when a data service provider receives new data from a trusted source. The trusted source may produce data in batches, such as a daily update, or it may produce data on a continual basis, or it may produce data sporadically. In process **1710** the data service provider locates a digital signature associated with the business data, and tests it against the cryptographic key(s) provided by the trusted data source. The signature may be tested as described above in connection with **Fig. 5**. In decision process **1720** the signature is verified or not verified. If the signature is not verified, the data service provider rejects the data in process **1722**. Further, the data service provider may conclude that an intruder has attempted to inject data into the trusted data area, and issue an alert in process **1724** to the trusted source, the end user, or both. These parties may then investigate the improper data on their own.

If, however, the digital signature affirmatively verified in process **1720**, the new data is transferred to trusted storage in process **1730**. Once stored, the data may be securely accessed by the data consumer, using methods described above. After the data has been stored, a data service provider may also invoke business rules of the trusted source in process **1740**. These business rules may have been previously installed in process **1620** of **Fig. 16**, or they may be altered by providing a new set of rules or replacement rules with the updated business data. The rules may require that the new data be immediately transferred to the user, or not. This decision is made in process **1750**, and comes from a purely mechanical application of the business rules. If the decision is to not forward the data, then the process ends. This happens in a "pull" model of data transfer, where the user is expected to retrieve

Petitioner Exhibit 1002-0805

("pull") the content from the data service provider's trusted storage at a later time. Or the data may be transferred ("pulled") on a subsequent update. Otherwise, following a "push" model, the process continues to process **1760**, in which the data is transferred ("pushed") to the user without the user's taking any additional affirmative steps. The new business data is transferred to the user's electronic device, and placed therein, in a storage area associated with the trusted source. This storage area was created during the trusted storage system initialization process in process **1640**. The user's electronic device, in one embodiment, also verifies a digital signature of the trusted source, using public keys obtained from the PKI during system initialization. In another embodiment, the device verifies a digital signature of the data service provider, to ensure that the data is received from trusted storage and not from a fourth party.

In the third phase of operation, the user accesses the trusted data. The user accesses the phone, computer, or other electronic device by authenticating the user's identity to the device, as described above in connection with **Fig. 9**. Once authenticated, the user may access the files stored in the secure storage area on the device. The PKI used in embodiments of the invention guarantees that only a properly authenticated user may access the trusted data. For example, the electronic device may contain a credential that permits this user, or other authorized users such as police, to access the information, but no others may access it. In a "push" model, the secure storage area already contains the relevant information. In this model, a user simply logs in to his or her phone or computer, using the appropriate multi-factor security model, and sees updated data. In a "pull" model, the user initiates a request to a data service provider (or to a particular business, which forwards the request) for trusted storage. In this model, the data service provider communicates the data to the user's device on demand. In either case, the data is transferred to the electronic device via a secure communications link, to avoid fourth parties altering the data or substituting their own data.

Figs. 18A – 18D (collectively, **Fig. 18**) show the flow of data in the system of **Fig. 15A** in a secure fashion between a business **1510** of **Fig. 15A** and a data consumer, for example the owner of smart phone **1424** of **Fig. 15A** in accordance with an embodiment of the present invention. As noted above, a party participating in a public key encryption generates a pair of keys, public and private. Such key pairs are generated for purposes

Petitioner Exhibit 1002-0806

including digitally signing documents (for authenticating the sender) and encrypting data. These purposes are important and distinct. While some parties may generate a single key pair for use with both purposes, other parties may generate two key pairs, one for signing and one for encrypting. The scope of this invention includes the use of signing keys ("s-keys") and encryption keys ("e-keys") separately, and references to these keys as distinct entities are made where appropriate; however, it will be recognized that these key pairs may be identical in some embodiments.

At least four parties participate in a trusted system: a business (party "P1"), a data service provider or trusted party (party "P2"), an electronic device embodiment in accordance with the invention (party "P3"), and a data consumer (party "P4"). Additional parties may participate as well; for example, there may be additional trusted parties or intermediate systems that handle the business data, such as described in connection with Fig. 19, or others as will be evident to those of ordinary skill in the art.

Fig. 18A is a block diagram of the flow of data at a business in a trusted system embodiment. The data flow of **Fig. 18A** occurs inside a business computer, for example server **1512** of **Fig. 15A**. The process begins with business data **1810**. This data may be any data that the business P1 desires be securely transferred to the data consumer P4. In order to ensure data security, business P1 uses a PKI to retrieve consumer P4's public e-key, and encrypts the data **1810** using well-known techniques so that only a party having P4's private e-key may decrypt it (presumably, this party will be P4). Next, business P1 may wish to attest to the contents of the encrypted data **1820**. Thus, business P1 uses its own private s-key (without using PKI) to digitally sign the encrypted data **1820** so that anyone with the data and P1's public s-key may verify the signature. Business P1 places encrypted data **1820**, along with the signature **1832**, in a signed container **1830**. As described above, business P1 may decide to instead create a hash of the encrypted data, sign the hash, and place the data, hash, and signature in a container. In either case, the signed container **1830** is sent to a data service provider P2 for storage. As described above, business P1 may further encrypt signed container **1830** to avoid malicious tampering during the point-to-point communication. Thus, business P1 uses a PKI to retrieve the provider P2's public e-key, and encrypt the signed container **1830** using well-known techniques, so that only a party having P2's private e-key may decrypt it. The encrypted signed container **1840** can now be sent to

Petitioner Exhibit 1002-0807

the data service provider P2 in a tamper-proof form, even over an insecure communications link such as the Internet.

Fig. 18B is a block diagram of the flow of data at a data service provider in the embodiment. A data service provider P2 receives from a business P1 the encrypted signed container 1840 of Fig. 18A. Receiving here corresponds to process 1514, and occurs between the data flows of Fig. 18A and Fig. 18B. The provider P2 now uses its own private e-key (without using a PKI) to decrypt and retrieve the signed container 1830, much like peeling the outer skin off an onion. However the provider P2 cannot peel the 'inner skin', namely the encryption on the encrypted data 1820 in the signed container, because provider P2 does not possess, and generally cannot obtain, the data consumer P4's private e-key.

At this time, the provider P2 may perform the process of Fig. 17. Provider P2 may obtain business P1's public s-key using a PKI to validate the digital signature in the signed container 1830 using well-known techniques. If the P1 signature is valid, the signed container 1830 is stored in trusted storage 1522, as also shown in Fig. 15A. Business rules may instruct the provider P2 to forward (push) the signed container 1830 to electronic device P3. Or, in a "pull" model, the consumer P4 may request the signed container 1830. In either case, the provider P2 then uses a PKI to retrieve the public e-key for the electronic device P3, and encrypt the signed container 1830 using this key to form a second encrypted signed container 1850 for secure point-to-point transmission to the device P3.

Fig. 18C is a block diagram of the flow of data into the local storage of an electronic device in accordance with an embodiment of the invention. An electronic device P3 receives from a data service provider P2 the encrypted, signed container 1850 of Fig. 18B. Receiving here corresponds to process 1530, and occurs between the data flows of Fig. 18B and Fig. 18C. The device P3 uses its own private e-key (without using a PKI) to decrypt and retrieve the signed container 1830. The device P3 may use a PKI to retrieve business P1's public s-key to verify the digital signature in process 1852. The device P3 may also use a CRL or OCSP as described above to check whether business P1's public s-key has been revoked. If so, then the data in the signed container is out-of-date, and device P3 requests replacement data. This mechanism allows a business P1 to signal electronic devices P3 that, for example, a business data format has changed and a system-wide update is in progress. Electronic device P3 then requests new data without the intervention (or even knowledge) of the data

Petitioner Exhibit 1002-0808

consumer P4. The electronic device P3 stores the signed container **1830** in its local storage **1860** until the data consumer P4 requests it.

Fig. 18D is a block diagram of the retrieval of data from the local storage of an electronic device so that it may be consumed. A data consumer P4 first authenticates herself to the electronic device P3, for example as in **Fig. 9**. Authentication may include inserting a physical smartcard containing data consumer P4's private e-key into the device P3. Data consumer P4 may choose to re-verify business P1's digital signature in process **1862**, by obtaining business P1's public s-key from a PKI. Data consumer P4 may wish to do this for a number of reasons, including that quite a bit of time may have passed between the storage of the signed container in **Fig. 18C** and the present access. Once the signature has been verified, data consumer P4 extracts the encrypted data **1820** from the signed container. Finally, data consumer P4 uses her own private e-key (without using PKI) to decrypt the encrypted data **1820**, yielding the original business data **1810**.

It may be seen from the above description that the end-to-end process of transferring data in a trusted system embodiment is secure. Each of the four parties uses a PKI in accordance with the embodiment to retrieve the public key of another party. Each of the four parties uses a private key to decrypt at least some data or create a digital signature. As each party in a PKI is the only entity that knows its own private keys, the system can only successfully transfer the business data end-to-end if all parties are who they claim to be, and all encryption and signature protocols are properly implemented. Also, the use of a CRL or OCSP ensures that the data arrives in a timely manner. The trusted storage system thus provides data from businesses to consumers in a secure and timely fashion.

Another embodiment performs encryption for point-to-point transmission differently. For example, one embodiment encrypts data using the sender's private e-key rather than the receiver's public e-key. In such embodiments, the receiver consults a PKI to retrieve the sender's public e-key to perform the decryption. The use of such an alternate embodiment may be advantageous in certain circumstances, as it shifts the additional use of PKI from the sender to the receiver, saving the receiver computing resources and network bandwidth. In another embodiment, the data service provider P2 uses its private s-key to digitally sign the signed container **1830** as an added assurance that the contents are correct. In this embodiment, electronic device P3 and the data consumer P4 take the additional step of using

Petitioner Exhibit 1002-0809

a PKI to retrieve the provider P2's public s-key to check the extra signature, and take appropriate action if the signature does not verify. Or, in yet another embodiment, the device P3 verifies the signature automatically, transparently to the consumer P4, so that consumer P4 never needs to know that provider P2 signed the container **1830**.

Fig. 19 is a block diagram showing an embodiment of the present invention wherein a trusted data storage arrangement, such as illustrated in **Fig. 15A**, is coupled to a general communications gateway environment. The external communications gateway provides communications services to the trusted data source, for example real-time chat, email, single sign-on (authentication), web hosting, domain name system (DNS) provision, or other similar services. The communications gateway therefore is not dedicated to handling trusted data from a particular source, and in fact may not necessarily be dedicated uniquely to handling trusted data—in other words, the communications gateway may also handle data other than trusted data. An example of such a communications gateway is Microsoft® Windows Live™ online services, although the scope invention is not limited to this example. In accordance with this embodiment, such a communications gateway may be integrated into a trusted system as described above, allowing the communications gateway to offer trusted data storage as an additional service. This embodiment enables one or more trusted data sources, such as a government agency, bank, credit issuer, or business, to use the communications gateway as an intermediary for placing data into trusted storage that is made accessible to a targeted individual, potentially reducing or eliminating significant system integration costs that might otherwise be borne by the organizations that originate the trusted data.

In the embodiment of **Fig. 19**, an organization data source (corresponding to item **1510** in **Fig. 15A**) originates trusted data destined for trusted storage of a targeted individual (using the computer **1420** or smart phone **1424** of **Fig. 15A**), as described above. In the fashion described herein, the gateway **1920** and trusted storage data network **1970** of **Fig. 19** together implement some or all of the communication network **1430** of **Fig. 15A**. The data transferred in **Fig. 19** may be Internal Revenue Service data **1910**, or bank data **1912**, credit issuer data **1914**, or other business data **1916**. The data source, for example, a bank, may have an online web site to support customer transactions. In the present embodiment of the invention, this web site, in turn, may be coupled to an external communications gateway

Petitioner Exhibit 1002-0810

1920 to provide a variety of services to customers. The web site typically sends requests for certain URLs to its own web servers, and other URLs to the communications gateway for further processing, depending on the distribution of services between the host organization and the gateway organization.

Although some services offered via the gateway in this arrangement may include traditional ones such as chat and e-mail, the gateway **1920** of **Fig. 19** may function in a new way to provide more secure communications. In accordance with this embodiment, a user requests a high value transaction, such as a balance transfer, from the web site. In response the data source sends a request for a secure transactional write to the communications gateway **1920**. Gateway **1920** determines in process **1930** whether each request it receives is a request for a write into trusted storage. This determination may be made, for example, on the basis of the URL requested, or on information send along with the request such as HTTP headers. If the request is not for a write into trusted storage, in process **1932** the gateway **1920** sends the request to another gateway process for handling the request (e.g., a chat process). Otherwise, the request is examined in process **1940** to identify appropriate credential certificates for use in the trusted system, and to determine whether to proceed with the transaction. Process **1940** may consult an authorized certificate store **1942** to determine the validity of the credentials for both the data source and the end user. Authorized certificate store **1942** may be, for example, a CA or OCSP responder **1942A** within the trusted system. Or, the store could be a memory on the end user device used to request the transaction. Or, the store could be storage **1942B** internal to the gateway, or any combination of the above. As an added layer of security, process **1940** may send a secondary, out-of-band message to the end user to verify the transaction, as described below. In process **1950** the gateway determines whether to proceed with the transaction, based on the results of process **1940**. If not, then the process ends and the failed transaction is logged in process **1952**. At this time, the data source may also be contacted and informed of the failed transaction.

If the transaction should proceed, the gateway ensures that the trusted data is digitally signed in process **1960**. If the data source provided the data to the communications gateway **1920** already signed, then process **1960** is complete. Otherwise, communications gateway **1920** must sign the data. If the data source has provided its certificate to the gateway in the

Petitioner Exhibit 1002-0811

authorized certificate store **1942**, the gateway may sign the data on behalf of the data source. In this way, the data appears to the user as if it were signed by the data source in the first instance, allowing the operation of the communications gateway **1920** to remain hidden from the end user. Alternatively, the communications gateway **1920** may sign the data using its own credential certificate. In this way, a user may be assured that the data has been validated by the gateway, a party whose data security practices the end user may trust more than those of the data source. Once the data has been appropriately signed, it may be sent to trusted storage data network **1970** for distribution to trusted storage. Network **1970** may correspond, for example, to a portion of communication network **1430** which is connected to trusted storage **1522**. From this point onward, the end user may retrieve the data from trusted storage in accordance with the process described above in connection with **Fig. 15A**. Optionally, the trusted storage **1522** may be hosted and managed by the operator of the gateway **1920**. The end user is protected from data attacks directed to the operator of the communications gateway **1920** and of the trusted storage **1522** because the end user's data cannot be decrypted without the end user's private key, and the end user's private key is not in the trusted storage **1522** (as discussed in connection with **Figs. 18A** through **18D**.

In process **1940**, the gateway may send a separate, out-of-band message to the user to verify the secure transaction. The message may be sent to a device other than the device making the original request. For example, the user may use a computer to access the web site of the trusted data source, while the gateway **1920** sends a verification message to a PDA, phone, or other mobile electronic device. Such a verification message can be a text message, a picture message, or in other suitable format. The end user may respond to this message by sending a permission code, such as a pin number, biometric data, or other credential. The end user may digitally sign the response for added security. The gateway **1920** may then verify the response, and decide whether to proceed as above.

This embodiment provides several improvements over current systems. As the verification message is performed out-of-band, the requesting device and the verifying device need not share data or communications services. Logging, tracking, and location services may be added to the gateway, to improve gateway performance and detect and prevent fraud on a real-time basis. For example, the gateway could determine to proceed in

Petitioner Exhibit 1002-0812

process **1950** only with transactions that have a low risk profile. Also, this embodiment gives an end user immediate notice of an attempted fraudulent transaction in her name.

Trusted Storage on a Memory Device

Fig. 20 is a schematic block diagram of another embodiment of the present invention showing a memory device including dedicated write-once, read-many (WORM) storage areas for trusted data. Memory device **2010** may be, for example, a Flash memory or other non-volatile memory device. One application of the memory device of **Fig. 20** is for use in receiving secure data from trusted storage source **1522** as illustrated in **Fig. 15A**; the secure data may be deposited, for example, in flash memory associated with smart phone **1424** of **Fig. 15A**, and the flash memory may be structured as the memory device illustrated in **Fig. 20**. Memory device **2010** may contain several memory areas that serve different purposes. Memory device **2010** may have a standard, read-write memory area **2020**, which may be used to store e.g. text and data files, web pages, image files, and so on. This area is configured as standard write-many, read-many (WMRM) memory. Memory device **2010** may also have memory areas useful for performing cryptography, such as memory area **2030** that has a cryptographic engine with instructions that may be executed on a microprocessor. Memory area **2030** may be used, for example, to implement the encryption functionality of a smartcard, in a manner described in connection with Fig. 8. Memory areas **2040**, **2042**, and **2044** are write-once, read-many (WORM) memory areas. These areas can be programmed with data only a single time, for example by physically burning a fuse or anti-fuse for each bit of memory. In this way, these memory areas offer protection against tampering with data stored inside. Such secure storage areas may be used to implement a smartcard, as described below. Memory area **2050** contains a table for cross-referencing data stored in WORM memory with other data, such as dates, times, memory addresses, processing instructions, and so on. Memory area **2050** may be used, for example, to locate a particular data file secured in WORM memory, or compile statistics on the status of WORM memory, or perform similar useful functions.

As described in connection with **Figs. 8** and **9**, when a memory device **2010** is used to implement a smartcard, the device serves as a credential for the purposes of authenticating the holder of the device to a trusted system as described above. In this embodiment, WORM

Petitioner Exhibit 1002-0813

memory areas **2040**, **2042**, and/or **2044** are used to store credential data, such as biometric information or passwords. This data cannot be altered once written, thereby ensuring its security. The memory device **2010** may be combined with a mobile electronic device in accordance with embodiments of this invention (or another electronic device with similar secure functionality) as a substitute for a special-purpose smartcard device. The memory device **2010** possesses all the necessary functionality of a Hardware Security Module (HSM), and can therefore be used in any place a dedicated smartcard can be used. For example, by configuring the memory device **2010** in such a way that the memory addresses of WORM memory **2040**, **2042**, and/or **2044** are only accessible to cryptographic engine **2030**, memory device **2010** provides a private storage area for private keys generated by the device. When used in combination with a mobile electronic device, memory device **2010** provides secure credential data for comparison with credential data provided by a user seeking access to the mobile electronic device, as described above in connection with **Fig. 9**.

In a further related embodiment, memory device **2010** is used as a repository of trusted data that resists tampering. For example, memory device **2010** stores a number of certificates in WORM memory **2040**, **2042**, and/or **2044**. Such certificates are issued by a CA and programmed onto the memory device **2010** either before or after a user takes possession of the device. The cryptographic engine in memory area **2030** is employed to perform the cryptographic processes necessary to use a stored certificate in the customary manner known in the art, or for purposes related to virtual smartcards in accordance with embodiments of this invention. The write-once nature of WORM memory ensures that the certificate, once issued, cannot be deleted, replaced, or updated, thereby enhancing the security of the certificate against forgery. As an added security measure, a certificate expiration date may be stored in memory area **2050**, and the cryptographic engine configured to as refuse to read WORM memory after the expiration date. In this way, data encrypted using the certificate's keys cannot be decrypted after the expiration date, and data signed using the certificate's keys cannot be authenticated. This security feature may also be accomplished by using software (not shown) to erase the association data in memory area **2050** after the certificate expiration date. In this way, the cryptographic engine will be unable to locate in memory the proper certificate to employ, thereby decertifying any data associated with that certificate. Thus, in accordance with this embodiment, after a certificate

Petitioner Exhibit 1002-0814

is deemed inappropriate for further use by the individual, the certificate is rendered unreadable, and any data associated with that certificate may no longer be read.

This embodiment lends itself to ready integration with a PKI infrastructure in accordance with this invention. A certificate stored on memory device **2010** may itself act as a unique characteristic of the device, transforming the device into a physical credential. This physical credential can be presented as an authentication token in accordance with, for example, the creation of a virtual smartcard as described above. Furthermore, the processes described herein for updating certificates, using summary certificates, and so on may be applied to certificates stored on memory device **2010**.

Additionally, the embodiment of **Fig. 20** lends itself to integration with a trusted storage system as described above. For example, memory device **2010** may be used as local storage **1860** of **Fig. 18**. Using techniques known in the art, the process of **Fig. 18D** is extended so that trusted data **1810** is stored first in WORM memory, so that subsequent operations on the data may verify that it has not been altered. Memory device **2010** is thus be employed as a vehicle for trusted business transactions.

Fig. 21 is a block diagram, in accordance with a further embodiment of the present invention, showing a process for updating the memory device of **Fig. 20** in a manner consistent with consumer needs and a relevant business environment. Memory device **2010** may store advertising for display to a user via a computer display or speakers. An advertising agency allocates a separate WORM area to each business, for example memory area **2040**. The business places data in that area, such as images, sounds, web pages, software, or other advertising tools in process **2110**. Further, the business may place data in memory area **2050** indicating that the business data stored in the WORM memory should expire under a particular set of conditions. The conditions derive from parameters such as time or number of purchases. Revenues resulting from sales generated by the advertising may be used to offset the cost of the memory device **2010**, possibly allowing the business or device manufacturer to offer the device to consumers at reduced cost, or even no cost. Because the business data are stored in WORM memory, a user may be assured that offers and applications found therein are genuine, and not 'phishing' attempts for improperly obtaining the user's personal information. Thus, the memory device is used to enable a secure advertising and sales model.

Petitioner Exhibit 1002-0815

Once the memory device has been initialized with business data in process **2110**, the memory device is delivered to a user, who installs it into another, transactional device in process **2120**. The transactional device is depicted as phone **2122**, although it should be understood that the transactional device may be any electronic device capable of reading and writing data on the memory device. Next, a period of time passes, depicted as block **2130**, until a transaction is requested in process **2140**. The transaction may be requested, for example, by the user activating an application such as a web browser and viewing a page, or on a certain date, or after the passage of a period of time since the last time it was requested, or by another similar method. The transactional device **2122** then determines in process **2150** whether to perform the transaction, by consulting the business using a communications network (not shown), or by consulting business rules stored in the memory device. Process **2150** applies instructions or rules to determine whether to proceed with the transaction. If the transaction should not proceed, transactional device updates the memory device to disable business data in process **2152**. This business data is in WORM memory, so disabling the data may involve updating a table such as the table in memory area **2050**, as described above. If the transaction should proceed, the business data stored on the memory device in trusted storage is used to execute the transaction in process **2160**. The business data may be usable only once, in which case the transactional device may optionally execute process **2152** to disable the business data. Otherwise, the business data is at a later time, as indicated in the figure.

A business may carry out and terminate an advertising campaign using this embodiment. For example, the business data stored on the memory device may be a credential certificate stored in WORM memory **2040**, and advertisements stored in standard memory **2020** and digitally signed using the certificate. The business offers purchasers of the memory device a trial product or service, where the offer is good until a certain date, or for a number of days after the first use of the memory device, or until a retail version is purchased. The business can revoke the credential using PKI methods known in the art, and this embodiment will invalidate the corresponding certificate, thereby effectively disabling the advertisement. If the same certificate is installed on many memory devices by repeatedly applying process **2110**, revocation of the certificate will disable all of the advertisements on all of the devices. Such an application is useful, for instance, to cease advertising a certain

Petitioner Exhibit 1002-0816

discontinued product. Or, different certificates could be used on each memory device, allowing the business to revoke only that device's certificate when the user purchases a retail version of the trial product or service. The advertisements may be downloaded from the business automatically, and may be replaced by new advertisements until the certificate is revoked. Advertisements may also be statically installed on the memory device in process **2110**.

Fig. 22 is a block diagram, in accordance with a further embodiment of the present invention, showing a process for downloading digital media content to the memory device of **Fig. 20**. This process enables a digital media content distributor, such as a record label or movie distributor, to provide downloadable media content (music, movies, or other content in digital form) to individuals so that only that individual may play the content.

An individual begins the process by accessing a digital media content order site in process **2210**. The individual will typically browse the site to find appropriate media content for download. After the individual selects the content, she supplies the site with a public encryption key unique to herself, in process **2220**. Software at the site then encrypts the selected digital media content according to well-known methods, using the user encryption key in process **2230**. Optionally, in process **2232** the software may also encrypt the media content using a second encryption key associated with a media content player installed on an electronic device of the individual. Although the figure depicts the user encryption before the player encryption, these may occur in any order. Once the content is encrypted, it is sent to the individual in process **2240**. Sending is done via any communications medium having sufficient transfer speed to ensure that the transfer will complete in a reasonable length of time. In process **2250** the individual receives the encrypted content, and stores it on the memory device of **Fig. 20**.

The public encryption key used in optional process **2232** may be unique to the individual's media content player, and may include information about the particular hardware or software configuration of the device on which it is installed. However, the public encryption key used in processes **2220**, **2230** is unique to the individual, not to any particular hardware or software. The latter may be a private key obtained from a smartcard or other physical credential, or it may derive from a virtual smartcard in accordance with an embodiment of this invention, such as described in relation to **Figs. 8** and **20**, among others.

Petitioner Exhibit 1002-0817

The user encryption key may be stored on a mobile electronic device **2222** or on another electronic device. The key may be stored in the memory device of **Fig. 20**. Or, the key may be stored in a public key storage area, in accordance with PKI standards.

Because the public encryption key is unique to the individual, only that individual's paired private key may be used to decrypt the media content. Thus, only someone in possession of the private key (presumably the individual) can unlock the content. This restriction permits copies of the encrypted content to be made without the chance that the content can be played by others (notwithstanding that related embodiments may employ copy-protection mechanisms). Also, unlike some current systems, a user may access the content on devices other than the one used to select and download the content. The media content is thus both portable and playback-protected.

Fig. 23 is a block diagram, in accordance with a further embodiment of the present invention, of a process for playing digital media content, from the memory device of **Fig. 20**, after the content has been downloaded according to the process shown in **Fig. 22**. At the beginning of the process, the media content has been encrypted using a key unique to the listener, and optionally a key unique to a media content player. In process **2310** the listener first selects the content to be played. This selection may be made, for example, by clicking a file icon in a user interface, inputting a command into a command window, selecting a file name in a media content player, or other similar method. In process **2320** the content is decrypted and presented to the appropriate content player. Decryption includes decryption using a user private key, and may include decryption using a content player private key, depending on whether optional process **2232** was followed. Once the content has been decrypted, the media content player has access to the media content in its native format. In optional process **2322** the content player verifies that it is licensed to play the content. This process may include analyzing playback restrictions that accompany the media content, sending a request to a central licensing server to determine that the player executable file is unaltered, or other processes known in the art. In process **2330** the content player plays the media content, i.e. renders it in an auditory, visual, or audiovisual manner.

The use of a user encryption key in **Figs. 22, 23** in embodiments of the invention permits the distributor of media content to retain control over the playback of the content, even if the content is freely copied. Thus, risk of infringement of a copyright held on the

Petitioner Exhibit 1002-0818

content is reduced, as individuals are less likely to copy content that they know they will be unable to play. Alternate embodiments include additional processes for preventing or restricting copying in the first instance, providing additional restrictions on the playback of the media content, and curtailing copyright infringement by taking any other steps that are enabled by this invention.

The use of the user-specific encryption key is enabled by embodiments of the invention described herein, and in particular by the combination of PKI embodiments, trusted storage embodiments, and secure transaction embodiments. These embodiments, and others described herein, can be combined in other applications which may be apparent to a person skilled in the art. The scope of the invention also includes these combinations.

Pre-Caching of Certificate Validation Requests

In order to provide rapid response to data requests across a network, several different strategies have been followed depending on data types and requirements. In the case of certificate validation, one industry practice has been to pre-construct necessary data packets and distribute them though the Internet to secondary certificate authorities (CAs) closer to the actual usage, thus providing less hops and more servers to respond to the validation requests. This is a sound strategy for small numbers of credentials, but breaks down as the number of credentials increases. When hundreds of millions of credentials need to be distributed, and the potential number of distribution sites rises into the thousands, the network traffic to load the distribution sites with the necessary certificates becomes very large, and the computers at those sites need to be specialized in order to handle the size and number of potential requests. This problem increases each day as the number of certificates continues to grow and the number of secondary sites requesting them grows proportionately.

Consider as an example, one hundred million credential certificates in use globally. Suppose that there are 1000 sites scattered around the world acting as certificate caches, each of which must re-verify each certificate once per day. Suppose also that each verification request requires the transfer of 1,500 bytes. Multiplying the numbers, merely verifying the certificates worldwide will result in a daily bandwidth cost of 150 terabytes ($150*10^{12}$ bytes). Current network systems would find this a significant load. Additionally, because of the amount of data transfer, network configuration issues would likely force most secondary

Petitioner Exhibit 1002-0819

CAs to reside outside corporate boundaries, resulting in the potential for a man-in-the-middle data attack.

The likelihood that an individual will need to authenticate on more then a few servers is very low, however. For example, in the case of physical access described above in connection with **Figs. 11-13**, an individual can only be in one part of the globe at any given time. This is true for any type of access that requires a physical presence. In the case an individual wishes to travel to a satellite office complex to access a computer, only a small subset of individuals will need to validate over more than just a few networks. By monitoring an individual's usage patterns and physical locations, it is possible for a single validation site to fetch and load only the certificate status responses that are likely to be requested at that site, thereby greatly reducing the size of the data load both locally and globally. Such an approach reduces the data set to be moved to a size compatible for storage and access within an enterprise firewall, and allows data transfer systems to eliminate the man-in-the-middle attack.

In one embodiment of the present invention, the decision of where to cache response data is made on the basis of geographic positioning. By the use of cell phone location, which may be obtained using e.g. a cellular network or a global positioning system (GPS), a cache local to an area may load only the status responses of people found in that area. For example, if a company employee travels to Paris and needs access to a building in Paris, then only the company's Paris certificate cache would validate his certificates using the originating CA. The other corporate caches around the globe would not need to load his status response data. The Paris cache could be collocated with the physical access server inside a Paris office intranet, providing a secure physical access request infrastructure.

In another embodiment of the present invention, the decision of where to cache data is made on the basis of site-specific usage patterns. The validation response servers request from an originating CA only those responses they are likely to need based on the credential requests they have served over a recent timeframe, for example the previous 24 hours. The servers which already track credential requests provide the certificate numbers, and forward those numbers to the appropriate caches. Again, this embodiment eliminates from the cache the credential data of all those who do not use the service, and keeps the number of validation responses to the originating CA small.

Petitioner Exhibit 1002-0820

When validating a certificate, a security system may first consult its local cache. In the event a response is not found, the system reverts back to the standard way of producing a response; that is, it will issue a request back to the certificate authority. This back-up procedure is normally slow; however, because it is only used in the exceptional case, the overall validation response time is improved and the overall network load is reduced. In one embodiment, the validating system may request a nonce, or one-time cryptographic data, to protect the request to the originating CA. Requesting a nonce may be too expense to do for every request, but here it is used only when there is a cache miss. Use of a nonce protects certificate validation requests against a man-in-the-middle attack when a local cache does not contain the appropriate certificate.

Fig. 24 is a block diagram, in accordance with embodiments of the present invention, of processes for determining sites that require cached credentials. The figure depicts a process of determining response-caching sites based on geographic positioning, as described above. In accordance with the embodiment shown, an individual who requires services enabled by credential verification, possesses a mobile electronic device **2410**, shown here as a cell phone. This cell phone is detected by a positioning network **2420**. Using algorithms known in the art, in process **2430** the network **2420** determines the distances of the phone **2410** to each of a number of reference points, thereby providing an estimate of the individual's location. In one embodiment, accuracy of only hundreds of feet is sufficient to determine a caching site. In this embodiment, network **2420** may be a cellular telephone network, wherein the reference points are cell towers. In another embodiment where caching sites are densely distributed, a Global Positioning System (GPS) may be employed for finer spatial resolution. In an embodiment using a GPS, the reference points may be satellites in orbit above the Earth. Other positioning networks **2420** that provide this functionality may be used in accordance with embodiments of this invention.

In process **2440**, the device position is correlated to the positions of the caching locations to determine the closest response cache, using methods known in the art. To perform process **2440**, a database **2442** containing the locations of the response caches may be consulted. The database may contain any information necessary to associate a physical location with a certificate authority, including geographic coordinates (latitude and longitude), cache names, Internet addresses, physical and logical topologies of data

Petitioner Exhibit 1002-0821

networks, a list of users whose certificate responses are authorized to be cached at a given location, and any other useful information.

Once an association has been made between a caching site and a CA, two paths are followed. In process **2450** each CA **2460** is notified of the certificates for which it will have to serve validation responses. In process **2462**, each CA prepares to serve validation responses by associating each potential request with a caching site from which it is expecting that request. This process allows CAs to deny requests for status responses from locations other than that of the device **2410** authorized to carry a certificate. Thus, process **2462** provides the system with an additional layer of security. In process **2464**, each CA activates its certificate status responders to respond to validity status requests. In the second path, process **2470** sends each caching site data representing the list of CAs that site may be contacting to validate certificates. The site then caches credentials from each CA, which has activated a responder to validate those credentials, as depicted in **Fig. 25**.

Fig. 25 is a block diagram, in accordance with an embodiment of the present invention, of caching credentials at a site determined by the processes of **Fig. 24**. Certificate data is received at the site **2500** in process **2470**. In process **2510**, the caching site **2500** determines the CA to contact for each certificate, and loads the response data. If current response data is already in the response cache database **2516**, process **2510** need not request another validation status. Otherwise, in one embodiment the caching site **2500** sends a validation request for each certificate to the appropriate CA **2460** using a data network **2512**. In another embodiment, the validation request is deferred until actually required by a user. As described above, these requests may contain a cryptographic nonce for additional security. The responses are then stored in database **2516**. Database **2516** containing the sensitive response data may be advantageously located behind a network firewall **2514**, and therefore inaccessible to a malicious user (man-in-the-middle) **2518**.

In process **2520** the caching site prepares to service authentication requests. Process **2520** may include, for example, activating point-of-sale devices (e.g. credit card readers), physical access systems and headends, web servers, and other devices and processes. In process **2530** the caching system receives a request to validate a certificate from mobile electronic device **2410**, according to a process described above. By way of example and not limitation, process **2530** may be a request for physical access to a secure location, executed

Petitioner Exhibit 1002-0822

as part of process **1250** depicted in **Fig. 12**, or a request to access trusted storage as part of process **154** as shown in **Fig. 15B**. In process **2540** the caching site accesses its response cache database **2516** to determine whether the presented certificate is valid. If the response is not present, then the site requests a response from CA **2460**. If the response is present, the site determines a validation result is process **2540**. The site may then return that result to the device **2410** as depicted. If the result is favorable, then the site instructs the service for which the validation request was made to proceed.

Edge-Trusted Computing: Associative Storage

This section provides another perspective on various concepts discussed above, particularly in the section immediately above and the section entitled "Batch Certificate Processing" and in connection with Fig. 10 and related figures. In order for two parties to perform transactions in a trusted way using a chain of trust, the chain should be validated in two ways. First, the integrity of the chain is tested by walking the chain and checking the signatures of each cross-certificate until a trust anchor is reached. If a single signature is invalid, then the chain itself is invalid. The second check is performed on each certificate in the chain, and may be done as each certificate's signature is being checked. The second check ensures that the cross-certificate is still valid, by consulting a certificate revocation list (CRL) or by making an OCSP request, as described above.

Within an enterprise, performing these processes is fairly straightforward, since they may be done by a single administrative entity; however, cross-enterprise trust is different, and presents further complications. The paths leading from one enterprise to another, and the lengths of the trust chains, can both become quite large. For example, for any given two users in different enterprises, thousands of potential validating CAs give rise to millions of potential trust chains between them, and verifying each chain may require dozens of OCSP requests. Even under the best of conditions, locating a complete trust chain and validating it could take several seconds, which for many transactions is too long. To date, systems have used the non-linear approach of contacting central servers to validate chains, but this approach will not handle the volume of transactions and certificates required to deploy PKI systems to the general population. This problem of scale is one of the reasons usernames and passwords remain as a primary security measure.

Petitioner Exhibit 1002-0823

The problems of cross-enterprise trust may be addressed in accordance with embodiments of the present invention by moving trust transactions to the 'edge' of the enterprise – namely to the mobile electronic device (phone or PDA) used to enter into a transaction. In such embodiments, the phone acts as a CRL or OCSP cache for the purposes of validating its own certificate. A possible caching mechanism is described in connection with **Figs. 24** and **25** above, although other caching processes may be used. Thus, the phone provides precisely the information necessary for the other (trusting) party to a transaction to validate the trust chain of a certificate presented by the phone. The remainder of the trust chain is contained in cross-certificates already possessed by the trusting party, obtained and stored according to processes convenient to the trusting party. Thus, *at the time of the transaction*, a trusting party no longer needs to contact a central validation server or OCSP responder to validate the entire trust chain.

The functioning of such a system is aided by the convergence of two facts. First, a phone may be uniquely associated with an individual, through the use of strong authentication protocols. Thus, the multi-factor authentication processes described above, especially in connection with **Fig. 2**, permit a phone to be used only by a single person (with certain strictly delimited exceptions as described herein). Thus, a relying party may be assured that the individual possessing and presenting a phone to enter into a transaction is the individual whose credentials, stored in the phone, are being offered for use in the transaction.

There are two requirements for such a system. First, the phone user and the relying party must agree on a trust endpoint (CA) to sign the certificate presented by the user through the phone. The parties must agree to a common CA, because that CA will be used to link the two partial trust chains of each party into a complete trust chain that the relying party may validate. Second, the phone must possess and transmit a certificate validation response having certain qualities to the relying party. The relying party may want assurances that the validation response presented by the phone user is reasonably current. This goal may be achieved by regular cache refreshes, for example, every three hours, twice each day, once each day, or at any other interval. Each validation response may include a timestamp, so that the relying party may verify its recency. Or, the validation response may not include a timestamp, in which case the phone includes, in its transmission to the relying party, additional data allowing the relying party to infer the likely time that the response was

Petitioner Exhibit 1002-0824

generated. These data may include, among other things, the time that the phone most recently connected to the validation network (e.g. Internet or cellular network), and the length of time the phone was connected to the network. As an example, if the phone were last connected the day prior to the transaction for ten minutes and the day before that for five hours, and if the caching mechanism refreshes every three hours, than it would be reasonable to infer that the validation response was likely not updated during the ten minute window, but was certainly updated during the five hour window, and thus that the response being presented for use in the current transaction is two days old.

Different trusting parties may employ different logic, based on each party's risk tolerance, for processing such connection information. Consider two examples: a parking meter purchase and a car purchase, both on credit. The amounts involved in renting a parking space tend to run to a few dollars at most. Thus, the owner of the space may be willing to accept a lower level of assurance that the credit credential being presented by a phone to a meter is still valid. In this context, discussed in some detail above in connection with micropayments and Fig. 27, the decision whether to allow a transaction proceed can be premised on data received from the smartphone by the micropayment device indicating that (i) the smartphone has been connected to a network for a period in excess of, for example, 15 minutes within the past 24 hours and (ii) the credential on the phone is still functional. (We assume here handling of certificate revocations using batched transactions as described above in connection with Fig. 10.) This small transaction can be reasonably handled with such an inexpensive determination of certificate status.

However, the amounts involved in purchasing the car that occupies that space are generally much higher, and the owner of a car dealership may require much higher assurances that the credit credential is still valid. In this example, the merchant may require as a condition of allowing the transaction to proceed, an active determination of non-revocation of the pertinent credential. Such a determination may involve a communication from the merchant to the CA (or a validation authority in communication with the CA); in this communication, the merchant sends the identification number of the certificate carried in the phone of the user (exposed to the merchant by the user's two-factor authentication to the phone). In response to this communication, the CA provides status information pertaining to the certificate. In fact, the dealership may require multiple forms of identification credentials,

Petitioner Exhibit 1002-0825

as well as access to the credit of a co-signer, access to a credit report from a major credit bureau, and other assurances beyond simply the credit card number of a would-be purchaser. Thus, knowing that the credential is valid is only a starting point for the dealership to enter into a transaction with the owner of a phone.

Between the levels of risk involved in the parking meter scenario (phone connected to the network and the certificate not revoked) and the automobile purchase scenario (concurrent determination, by merchant communication with CA, that certificate is not revoked), is an intermediate level of risk involving actively pushed certificate status information that is stored on the phone. In this scenario, at periodic intervals, for example, a message is sent from the CA to the phone indicating that the certificate has not been revoked, and this status information is stored on the phone in association with the certificate. Under this scenario, the merchant accessing the certificate gets status information concerning the certificate at the same time.

Generally, edge-trusted transactions occur in three scenarios. The first example involves two networked organizations having individuals attempting to exchange data. The method currently used in the art is to retrieve the chain of trust and validate each cross-certificate from both organizations using verification authorities (VA), which are typically centralized certificate authorities. However, this process is inefficient – the two organizations already trust each other enough to enter into a transaction. Instead of consulting a central authority to determine whether an agent or employee is trusted, each party may simply query the other party, thereby pushing validation to the edge. The internal details of one party's validation process should be unimportant to the other party, the important issue is whether each party trusts the other to properly validate its own employee's certificates. The encryption employed in PKI ensures that this validation can be trusted. The only certificate that needs to be validated by each organization is its own trust anchor. This validation can be done on a regular basis (e.g., every three hours, enterprise-wide) and updated to each agent or employee phone as needed. The complexity of validating the trust chain, and changes to the process, are hidden from other parties. A relying party simply receives a yes or no as to the validity of a user without the details. With this methodology the expansion an external storage of trust chains is unnecessary. Each party answers the question, "is this certificate

Petitioner Exhibit 1002-0826

valid". As described above, this answer can be precompiled and distributed for improved performance.

Each party no longer needs to possess an entire trust chain. Instead, the party merely determines whether or not the other party may be trusted. Each party still receives an end entity certificate and a validation response to provide assurance that the certificate is valid. The computational effort to validate certificates is distributed among the parties, and unnecessary intermediate checks to walk trust chains are removed. It is the responsibility of each organization to represent the trust of the individual, and not for the inquiring party to hunt through trust chains. It is also simple for each organization to verify that an end entity's certificate is valid. Each end entity is paired with at least one anchor, making easy to find out immediately if that end entity is available to enter a trusted transaction without building a huge database of trust chains.

As an example of the usefulness of this embodiment, consider Microsoft's Active Directory (AD). This software is an implementation of directory services, similar to LDAP, for authenticating and authorizing services in Microsoft Windows environments. AD maintains trees ('domains') of certificates, and each tree requires the same administration privileges. Thus, joining the certificate trees of two organizations that likely have different privilege structures is difficult at best. Even accessing domains or subdomains of a foreign tree requires the creation of various trust models (one-way, two-way, transitive and intransitive trusts, and so on). However, in accordance with this embodiment of the present invention, certificate trees no longer need to be joined, and access is greatly simplified. Each domain or subdomain in a foreign tree may be queried directly, without the need to set up complicated trust models.

The second major scenario involves an individual transacting with a networked device. In current systems, it is important that an enterprise validate a certificate it has received from an individual in order to send transaction data to the individual using the proper encryption keys. However, in embodiments of the present invention, this need not be the case. Consider the exemplary situation where the user requests data through a trusted gateway, as described above in connection with **Fig. 19**. The gateway service validates the individual's credentials before data or log on is permitted. The user requests, directly or indirectly, that this data be forwarded to the gateway. By gating the transaction through an

Petitioner Exhibit 1002-0827

intermediary trusted party, this scenario may be transformed into the scenario as described above. The enterprise uses the certificate from the gateway without checking it, as before, because it need not concern itself with validation details. (The chain of trust for the certificate was walked by the gateway when the user created an account with the gateway and added a certificate to the account.) There is thus no reason for the enterprise to check the chain's validity at the time of the transaction. This shortcut represents a large reduction in network and cryptographic load for the enterprise. The gateway's business policies ensure that a certificate is not presented to the enterprise for access to private data unless the certificate is valid and current. The enterprise will become aware that a certificate is not valid or current when the sending of data using that certificate's keys fails. The overhead here is not significant, as the gateway can ensure, through certificate management processes known in the art, that certificate invalidity occurs in only a tiny fraction of total requests (if ever). There is no need for the gateway to distribute validation responses to the enterprise, because those responses are stored with the user.

As another example of this embodiment of the invention, consider an individual who wishes to withdraw money from an automated teller machine (ATM). Typically, a credit card company has a contract with a bank to allow the bank to offer a credit card branded with the company's name. However, to access the actual credit card account from a bank ATM, the banks must be tied to the credit card company. This is accomplished by the creation of interbank networks, such as STAR (First Data), PLUS and INTERLINK (Visa), PULSE (Discover), and CIRRUS (MasterCard, Diners Club). Creating these networks requires data integration between each bank and the credit card company, and maintenance of the networks gives rise to ATM usage fees. However, with an edge trusted computing embodiment, an ATM could verify that an individual has sufficient credit to make a given withdrawal using only data on the phone. Then, the ATM could generate a debit record encrypted with the public key of a credit processor. The individual would be unable to tamper with the record, so it is safe to transfer the record to the phone for upload to the credit processor for debiting at the next update cycle. Combined with pre-caching of certificate validation responses having expiration dates and daily limits on withdrawals, this system ensures that no individual can withdraw money exceeding their available credit limit. Additionally, in this embodiment there is no need for interbank networks to transfer debit

Petitioner Exhibit 1002-0828

information to a credit processor, as a cellular telephone network (or the Internet) assumes that role. Thus, in this embodiment of the invention, ATM fees may be reduced or eliminated. The expense passed on to the individual by an alternate network provider for shifting data transfer from an interbank network would likely be less than current ATM fees.

The third major scenario involves transactions between an individual and a non-networked device. The individual requests data or a service from the device, by sending a packet that contains a certificate, a trust chain (excluding the anchor), and the OCSP validations for the elements of the chain. The device has all information needed to validate the individual's certificate except the anchor certificate in the message. However, the device has negotiated a particular anchor to use in the transaction, as described above, and has validated this anchor prior to the transaction. All the computations to validate the entire trust chain may thus be done without any network validation requests. The device encrypts the transaction data, and the individual can validate the entire returned data set. This process works because the paths in each trust chain are hidden, and all validation can be done inside the domains (i.e., hardware or software) of the individual and the device. The certificate validations are performed on the individual cell phones and transactional devices (parking meters and so on), making this approach scalable and avoiding the storage of unnecessary, redundant data.

Preventing Replay Attacks

Embodiments of the present invention are designed to prevent replay attacks, where eavesdropping by a third party on a communication, for example, between a user's smartphone and a terminal device can be used to capture data that are replayed for use in a transaction not authorized by the user of the smartphone. A replay attack typically takes advantage of the fact that valuable data, such as a certificate status response for an individual, are transmitted over a network. This response is typically used legitimately by the individual. However, a third party may intercept the data for later fraudulent use. In particular, the third party fraudulently present the saved data as a legitimate response to a status query for the individual's certificate, thereby causing a relying party to believe erroneously that the third party is, in fact, the individual.

Petitioner Exhibit 1002-0829

To prevent these types of attacks, a PKI provider in currently available systems must typically take several steps designed to verify that the certificate status request actually reached a party who can legitimately validate it (i.e., the issuing CA). In a typical scenario, the relying party, for example, a merchant, will create a cryptographic nonce, or one-time message. The merchant then encrypts the nonce, along with the certificate validation request, in a message to the CA using the CA's public encryption key. The CA decrypts the message, and transmits the nonce and the response back to the merchant, this time encrypted with the CA's private encryption key. The merchant can decrypt the reply (again using the CA's public key), and verify that the nonce is the same as the one originally sent. The security of the system relies on the fact that the reply returns in a span of time too short for a malicious third party to intercept and decrypt the message, and determine the nonce (which is unique to the request). It also relies on the merchant having an accurate copy of the CA's public encryption key.

However, approaches such as described in the previous paragraph do not scale well. A principal reason is that the data traffic experienced by the server of the CA is proportional to the number of certificate status requests involving certificates it has issued. In addition, the certificate authority is a central point of failure, and is also vulnerable to denial of service attacks. For example, if the Visa CA is taken offline by a denial of service attack, merchants would be unable to verify that Visa credential certificates presented by patrons were still valid. In turn, they would have to make a choice as to whether or not to honor the certificate, knowing that the credit card might have been revoked.

Embodiments of the present invention overcome the scalability and single point of failure problems, by modifying the above procedure for validating certificates. In one embodiment, rather than contact the CA directly, a merchant contacts a validation gateway. (For example, Windows Live, a service of Microsoft Corporation, Redmund, Washington, which today operates as a password storage vehicle, could be established to operate as a validation gateway in the manner described herein.) In this embodiment, the merchant transmits a nonce and status request, as before, using the cryptographic keys of the gateway. However, in this embodiment, the transmission is to the validation gateway, and here the validation gateway acts in effect as a proxy for the CA. The validation gateway returns an encrypted certificate status response to the merchant, along with the nonce, which the

Petitioner Exhibit 1002-0830

merchant can verify as before. In this way, the validation gateway shoulders the brunt of the validation traffic. This is a desirable outcome, as the gateway may use a significantly more robust infrastructure (established for the purpose of validation), than a particular certificate-granting agency or organization, such as a state Department of Motor Vehicles.

In another embodiment, the mobile electronic device (smartphone) used in a transaction may itself carry validation data. As discussed in the previous section, this embodiment can be effectuated by actively pushing certificate status information to the phone. Thus, at periodic intervals, for example, a message is sent from the CA to the phone indicating that the certificate has not been revoked, and this status information is stored on the phone in association with the certificate. Thus in this embodiment, the merchant accessing the certificate gets status information concerning the certificate at the same time. In a related embodiment, the certificate status information is sent from the CA first to the validation gateway described in the previous paragraph. Then the validation gateway pushes the status information to the smartphone, where it is stored, as before, in association with the certificate. As discussed in the previous section, because there is typically a delay between the time when the status information is pushed to the smartphone and the time when a merchant may want the status information, this approach carries a greater risk than the approach described in the preceding paragraph. On the other hand, it has a reduced overhead, and may suffice for a wide range of transactions.

In a related embodiment, the validation gateway and the smartphone used in a transaction both contain the same validation data. The phone receives, as before, the pushed certificate status data from the CA. In addition the data is pushed to the validation gateway, as discussed above in connection with batch processing of certificate validations and **Figs. 10, 27, and 28**. Thus, a merchant may query an individual's phone in addition to querying the validation gateway, to compare the responses. If they differ, then the merchant may suspect a replay attack and take any corrective measures, such as requesting a different method of payment, in addition to reporting a possible attempt to enter a fraudulent transaction to a credit issuer.

Restricted Communications

Petitioner Exhibit 1002-0831

With the growth of the Internet, cell phones, and other digital electronic communications channels, it has become possible to contact minors in an anonymous and potentially inappropriate manner. However, communications channels in accordance with embodiments of the present invention may be opened in such a way as to prevent anonymous contact with minors. Indeed, in various embodiments, many useful restrictions may be placed on communications channels, to provide various desirable features: forming a limited list of parties to the communications, limiting the age of the other party to a communication, limiting the geographic location of the other party, and so on.

In one embodiment of the invention, all data being communicated to a recipient is identified with a identity certificate signed with the sender's public key. By validating the certificate, all data can be traced to the originator. Further, by providing information in the identity certificate such as age of the party, name of the party, geographic location of the party, and other useful information, a software program may filter would-be communications based on pre-selected criteria. For example, in a related embodiment, in order to pass the filter anyone attempting to contacting a minor is required to have a valid identity certificate showing that the person is younger than a given age, or within two years of the minor's age. In this embodiment, the minor may not initiate a conversation with an adult, or vice versa. Thus, would-be predators are deterred. However, certain adults may be granted access. The filter may be configured to recognize the certificates of the minor's parents or teachers, for example. In a similar related embodiment, the filter is configured by a parent to allow a child to contact only those on a 'whitelist' of allowed friends, thereby achieving a similar result. In another embodiment, a web site requires each visitor to present an identity certificate before displaying web pages, and refuses to display certain pages to those presenting certificates belonging to minors. In this way, minors are shielded from viewing age-inappropriate materials, without the active oversight of their parents. Techniques for programming filters are known in the art, but in accordance with this invention, the data being input to a filter from an identity certificate is attested by the presence of a digital signature. Devices that process the certificates may contain a list of acceptable certificate signers, to prevent individuals from creating and signing their own age data.

Fig. 26 is a block diagram of a further embodiment of the present invention showing processes for initiating communications between two parties. A first initiating party is

Petitioner Exhibit 1002-0832

represented by phone **2610**, and a second responding party is represented by phone **2620**. Although the parties are represented by cell phones **2610, 2620**, it will be understood that the invention is not limited to this exemplary embodiment. The initiating party attempts to open a communications channel by sending a request to the responding party in process **2630**. The request includes an identity certificate, and may include communications parameters such as bandwidth, a communications protocol designation, encryption keys or encryption algorithm initialization vectors, or other initialization data. In process **2632** the responding party uses information in the identity certificate, such as the initiating party's name, to validate the certificate using methods described herein or those known in the art, thereby demonstrating the authenticity of its contents. In particular, the certificate may be signed using the initiating party's private key, or the private key of a third party trusted by the receiving party. In process **2634** a relevant parameter is extracted from the identity certificate, and processed using a filter. Parameters may include, without limitation, the age of the initiating party, the party's name, and the party's geographical location. These parameters, alone or in combination, may be used in the filter to determine whether phone **2620** is configured to accept communication. The result of this determination is sent to phone **2610** in process **2640**. If the result is NO, then the process terminates, and a communications link is not established. If the result is YES, then phone **2620** may send an identity certificate of the responding party. In this case, the initiating party proceeds in a symmetrical fashion to validate the responding party's identity certificate in process **2642** and to apply a criteria to information from that certificate in process **2644**. It should be noted that the criteria used in processes **2634, 2644** may be different, as the two parties may have different groups of peers with whom they are willing or able to communicate. As before, process **2644** results in a decision whether the party is configured to accept communication, and the result is returned to the responding party in process **2650**. As before, if the result is NO, a communications link is not established. If the result is YES, then each device is configured to communicate with the other, and a link is established. From this point, phones **2610, 2620** may exchange communications with each other in process **2660**. In order that the communications may be guaranteed against interception and man-in-the-middle attacks, the communications may be encrypted, as described above in connection with **Fig. 18**, or each portion of exchanged data

Petitioner Exhibit 1002-0833

may be digitally signed. It will be understood that processes **2632, 2634** may be performed in any order, and similarly for processes **2642, 2644**.

Purchases, Including Those without Divulgation of Credit Card Number

Credit card fraud is a large and growing problem. The ease with which a credit card number may be obtained (especially over the Internet), the relatively low risk of detection, and the potentially high reward for obtaining a credit card number combine to create an strong enticement for would-be criminals. Once obtained, a person may use a credit card number to fraudulently purchase goods or services over a telephone, in a scenario known as "card not present." Credit card companies have attempted to address the problem of fraud using various security measures, including the introduction of a security number imprinted on the physical card or encoded in a card's magnetic stripe, known variously as a Card Verification Value (CVV), Card Verification Code (CVC), or Card Identification (CID) number. Such codes have little security value if the physical credit card on which they are located is stolen.

When a charge is made via a phone in accordance with embodiments of this invention, however, a transaction from the phone to the credit processor company does not need to reveal the credit card number. Instead, for example, the hardware security module on the phone may encrypt the credit card number and charge amount with the public key of the appropriate credit card processor. The seller of the product or service never possesses the credit card number in an unencrypted form. All the seller can do is forward a message with the encrypted data to the processor, and the encryption algorithm ensures that only the processor can decrypt the number. After the processor verifies that the credential is valid, the seller receives an authorization code, similar to the credit processing systems of today. The credit card number never leaves the buyer's phone unencrypted, thereby making the number secure for the transaction.

Fig. 29 is a block diagram of a method in accordance with an exemplary embodiment of the present invention, in which a phone as described above is prepared and used in card-not-present transactions. In process **2905** the owner of the phone preliminarily registers the phone with the credit card company, using identity credentials of the owner and the phone to uniquely associate the phone with the owner. The owner's identity credentials were created earlier, as described in connection with **Fig. 2A**, while the phone's identity credential is

Petitioner Exhibit 1002-0834

described in connection with **Fig. 1**. Once process **2905** is complete, the credit card company has identified the owner and the phone, and is ready to accept requests for credit authorization. In process **2910** the phone requests a credit authorization certificate from the credit card company. This request may be made over any data network, including the cellular telephone network and the Internet. A request may include an amount, for example $500. The request may include an expiration date, such as 24 hours. By combining these data into a single request, the phone may request an authorization for $500 per day. Other obvious combinations of request parameters are contemplated. This functionality permits the phone to limit the amount of credit that is 'borrowed' by the phone during any particular period of time.

After the credit card company receives such a request, in process **2920** it generates a credit certificate for the phone. This certificate is unique to the phone and to the owner, and has data recognizable only by the credit card company, such as a nonce encrypted with the company's public key. In process **2930** the phone receives this certificate from the credit card company, and stores it. The phone's hardware security module now has the credit card certificate, and when combined with software on the phone, may generate payment tokens for use in card-not-present transactions. A transaction is represented by process **2932**, and is explained in detail below in connection with **Fig. 30**. At some point later, in process **2940** the credit certificate expires, and the user or phone may request a replacement certificate, as indicated in the figure by line **2942**. Such a replacement certificate will have a different cryptographic nonce, thereby assuring the credit card company that the certificate is not being reused ('replayed') at a later time. In an alternate embodiment, the credit certificate does not expire, but remains valid until it is revoked by the credit card company. Such an alternate embodiment is useful, for example, in scenarios wherein the phone does not (or cannot) connect to a data network for an extended period of time, such as when the owner takes the phone on travel to another continent with an incompatible cellular network. Non-expiring credit certificates may be used to make purchases in such situations, especially when used in combination with cached validity responses as described above.

Fig. 30 is a block diagram of a method for extending credit to an individual having a phone prepared as in **Fig. 29**. As an example, suppose the individual wishes to purchase a meal she has just consumed. Preliminarily, a waitress totals the charges, and obtains a billing

Petitioner Exhibit 1002-0835

folder to present to the individual. The folder may contain the customary paper bill, but also embedded within the folder is a small transactional device, for example a microprocessor, memory, and short range wireless transceiver. Bluetooth, or another short range wireless protocol, may be used for compatibility with the individual's phone. The waitress programs the transactional device with the charge information, and presents the folder to the individual. Other sellers of goods and services may take other steps to prepare to transact with a customer, but the preparation will be substantially the same.

In process **3010** the transactional device posts a request to the phone that a seller wishes to debit an account of the individual. Typically, in response to receiving this request, the phone notifies the individual that a charge has been requested, by flashing an indicator light, displaying an interaction dialog, or other suitable means. After the individual authenticates herself to the phone, as described above in connection with **Fig. 9**, software on the phone asks her for an authorization and debit amount. The individual may have stored certificates for several credit accounts, e.g. Visa, Mastercard, American Express, or Discover, in the course of preparing her phone as described above. She may now choose which of these certificates she wishes to expose to the seller. In process **3020** she exposes a credential certificate carrying the name of the credit processor, and encrypts an authorization for the debit amount. The encrypted authorization and amount is sent to the transactional device, which stores this data in process **3030**. In process **3040** the seller or seller's agent (i.e., the waitress) takes the transactional device to a merchant computer, where data is read from the device and sent to a credit card processor. Communication with the credit card processor may be done using methods and data networks known in the art. In process **3050** the credit card processor agrees to the transaction, and returns to the seller a payment token containing an authorization code. Such authorization codes are known in the art, and signify to the seller that the processor recognized the party as one having an account containing sufficient credit. As part of process **3050**, the processor reads the cryptographic nonce stored in the certificate in process **2920** and validates it using a private encryption key. In process **3060** the authorization code is stored to the transactional device, along with a receipt. In process **3070** the individual's phone receives the receipt from the transactional device and optionally stores a record of the transaction in a record log.

Petitioner Exhibit 1002-0836

In the above embodiment, the work flow in the exemplary restaurant does not change. The credit card number is never exposed to the seller, thereby making it secure, and a second tip transaction is avoided, thus reducing costs to the seller. These processes may be used in other situations where a seller requires a credit card authorization to extend credit, and the scope of the invention includes these other uses and situations. In an alternate embodiment, the user may only write a phone number on the paper bill. The merchant may then transmit that phone number, along with the purchase amount, to the credit processor, who calls the number. In response to the phone call, the phone receives certificate data from the credit processor, and presents a message to the user that the processor wishes to debit the user's account. From this point, the process may continue analogously to that depicted in **Fig. 30**, i.e. the credit card processor, having received a response from the phone over the cellular network, can proceed directory to process **3050** and accept the transaction. Optionally, the processor can transmit to the phone a receipt for the transaction immediately, while the phone call is ongoing.

With only a slight modification, the above processes may be followed to allow an individual to make a secure purchase using a desktop computer on the Internet. In order that the process might work, the phone may be connected to the computer via a Universal Serial Bus (USB) connection, or other wired or wireless connection. Resting the phone in a docking cradle may provide this connection, as well as allowing the individual to simultaneously charge the phone. Then, rather than receiving a transactional device in a physical folder, the individual receives an order page on a website. Software on the individual's computer passes data from the page to the phone. Such software is known in the art, an example being Microsoft ActiveSync, which exposes an API allowing a web page to discover whether a phone is present, and to discover the phone's cryptographic capabilities. The user authenticates herself to the phone as before, authorizes the transaction and amount, and transmits these data to the seller (by an Internet connection rather than a short-range wireless connection). In some embodiments, this out-of-band authorization may be sufficient for dollar amounts only up to a certain limit, such as the user's credit limit. The seller's website then forwards the data to a credit card processor, receives an authorization, and completes the purchase, in a manner analogous to that described above. The individual

Petitioner Exhibit 1002-0837

receives an order confirmation page containing a receipt, which software on the computer forwards to the phone for recordation.

This process improves privacy, by making information purely transactional. An individual's credit card number is used to generate a specific transactional message that has no value outside of its context. If the message between the seller and the processor is intercepted, it has no value to the interceptor. This embodiment allows individuals to buy something without disclosing anything about themselves. Their data is protected by their identity certificates, which must be validated before they can use any information stored on the phone. With a widespread deployment of these embodiments, parties no longer would have to exchange credit card numbers, only authorizations to receive money. These embodiments of the invention thus enhance both security and privacy, while making secure and trusted transactions easier. In addition, by providing receipts to both the purchaser and the merchant, these embodiments lend themselves well to fast fraud detection, as described above in accordance with **Fig. 10**.

Phone as Source of Stored Credentials for Use in Lieu of Passwords

Single sign-on systems allow a user to store logon credentials for many different Internet services in a single location. The user can then access the central location using a single password, and ask the system to log the user onto a chosen service by transmitting an authentication token. In this way, the user does not have to remember dozens or hundreds of different passwords or credentials. In effect, the single location acts as a 'wallet', containing credentials for the user

Single sign-on systems are typically implemented as large, central password repositories that are administered by a company in which the user must place significant trust. While all credential data are encrypted, many attack vectors exist to recover the data. For example, the password must be sent in clear text at least for some part of the transport between the user and the requested service, and the repository typically protects stored passwords for large groups of users with a single storage key. The prevention of multiple logons from different locations is also difficult, due to the stateless nature of HTTP. In fact, since the central server has no contact with the user, a lost connection or a second logon are difficult even to detect. While providing some convenience to the user, the security and

Petitioner Exhibit 1002-0838

privacy overhead for storing passwords centrally is high, and systems that need to communicate for speed need redundant data and services. These types of services are also subject to denial of service attacks, due to their central location in the logon topology. Further, many existing repositories work with different services and do not interoperate, requiring users to maintain accounts with several repositories.

By placing the user credentials on a cell phone and updating the phone with OCSP responses, single sign-on embodiments of this invention have several benefits over existing systems. First, the credentials are stored in a mobile electronic device over which the user has direct, physical control, so there is no need to place trust in a third party storage company. Second, the number of attack vectors to recover the stored credentials is greatly reduced, because the credentials are in the physical possession of the user. Even if the user loses the phone, in order to access the credentials in software, an individual must first authenticate to the phone as described above in connection with **Fig. 9**. Even if a malicious individual disassembles the phone, the credentials may be stored in trusted storage, such as a Flash memory card with smartcard capabilities, as described above in connection with **Fig. 20**, to which the individual must present proper authenticate to unlock the credentials. Further, the credentials may be encrypted between the phone and the service, eliminating another attack vector. Third, by storing logon state on the cell phone, it is now possible to determine if a second logon is attempted by another user, as described below. Fourth, it is no longer necessary to contact a central server to have single sign-on functionality. As a corollary benefit, additional network traffic is not required during the sign-on process. As another corollary benefit, denial of service attacks are mitigated, as there is no central server that can be targeted for attack. Fifth, there is no need to integrate several different repository services, and the system may be realized using currently deployed PKI technology. Finally, the system provides for true lock-out of compromised credentials. If the password of an individual to an account in a current central storage system is compromised, the account can be deactivated by the system, but such deactivation does not also deactivate the various logon credentials stored within the account. However, the credentials on a phone can only be accessed using the private key of the individual who owns the phone. So if the individual's identity certificate is revoked for whatever reason, all of the associated logon credentials are instantly rendered useless, thereby guaranteeing the security of the associated accounts.

Petitioner Exhibit 1002-0839

Fig. 31 is a block diagram showing the operation of a single sign-on embodiment of the present invention. In process **3110** the phone queries for and receives a daily certificate status response for each of the logon credentials stored in the phone's trusted storage. In an alternate embodiment, the response could be cached, as described above. In process **3120** the user attaches the phone to his computer, using USB, Bluetooth, or a cellular network. (In some phone embodiments already containing a web browser, wherein the user is seeking to access a web site directly from the phone, this step is unnecessary.) In process **3130** the user navigates to a website and identifies his user name for entry into a restricted area. Normally, at this point, the website would request the user's password. However, in process **3140** in this embodiment, the web page uses special software to contact the user's phone to issue an identity challenge. The user authenticates himself to his phone, as described above in **Fig. 9** (not shown). In process **3150** the phone and site validate certificates and perform a key exchange to generate a shared secret, each party using its own private key and the other party's public key. Such exchanges are known in the art: the Diffie-Hellman key exchange is a widely known example. If the shared secret is identical for both phone and website, then the website may permit access, as in process **3160**. Advantageously, the shared secret may now be used to perform symmetric cryptography between the browser and the site. Once access has been granted, the phone and website generate records of the access, and store them locally in logs in process **3170**. These logs may be compared later using batch processing, as described above in connection with **Fig. 10**.

This sequence of processes does not exchange any private information – the validity of the user's identity certificate is all that is required for entry into the secured area. Any secondary logon to the site will be detected by the phone, and a message will be sent to the site that the same user is logging on from another location. The site may then act in accordance with site rules to address the multiple-logon situation. In an alternate embodiment, the user need not even enter a username. Instead, this information is replaced by a certificate number, or kept on the phone in a database allow the user to keep this information in one place. Finally, because this embodiment uses standard PKI logic, one can build upon it to create a set of single sign-on protocols that are interoperable across systems and sites.

Petitioner Exhibit 1002-0840

Preventing Multiple Contemporaneous Accesses to Secure Sites

Physical perimeter controls are often set up at incident sites. An authorized individual is checked by security personnel, and allowed in the site if her credentials are acceptable. Nevertheless, such a system properly processes only those individuals who choose to enter the site through the front door. Generally speaking, security is only as strong as its weakest point, and the front door is usually not a location's weakest entry point. Malicious individuals may enter through lower-security areas, and once on-site, may gain access to unprotected areas without undergoing further security checks.

What we have said in the context of perimeter controls for physical access applies equally to access to computing resources, including to computer systems and to web sites. More generally, "access control" thus can refer to control of physical access or to control of access to computing resources. An access control system may be foiled not simply by avoiding the "front door" but also by a fake or copied credential

In accordance with an embodiment of this invention, the above problems may be addressed through storing a token on a mobile electronic device. At the front door, which may be a physical barrier or a logon screen, when an individual is permitted on site, a token is placed on the phone. The token includes one or more credentials from the phone, so as to associate the token uniquely to the phone. The token is signed using a private key of the access control system. Each point in the interior of the site can validate that the gatekeeper was seen and passed properly, by (1) determining that the token is present on the phone, and (2) assuring that the phone has an original token (as opposed to a copied token) by verifying that the credential used in the token matches a corresponding credential of the phone. Only phones containing the proper token may be used to access secure areas. The token cannot be used on another phone that has different identity credentials. Using this embodiment, it becomes possible to thwart duplicate entry even at interior points that have a lower threshold of security, and even if a passed user attempts to copy a valid token to another phone.

Secure and Portable HTTP Cookies

HTTP connections, used in web-page based sessions between a user and a web site, are stateless. In order to preserve session state, many websites employ cookies, which are name value pairs that are retrieved from the website on one connection, and sent by the

Petitioner Exhibit 1002-0841

browser to the website on a subsequence connection. For the most part, cookie data are maintained in clear text in a web browser or on a user's hard drive, making this information easy to maliciously forge or alter. In addition, cookie data are typically stored on the computer running the web browser, so that if the user wishes to access the website from a different computer, he must re-establish his cookies. In particular, cookies containing logon data will be missing on the second computer. In other words, current implementations of cookies are device-specific, not user-specific.

In accordance with embodiments of this invention, cookie data are encrypted end-to-end, between the website and a mobile electronic device like a phone or PDA. By encrypting the cookies this way, we can realize several important advantages over plain-text cookies. First, users of the computer running the browser cannot read the cookies. The browser itself may continue to store the (encrypted) cookies as normal, but the data stored within are useless to anyone who attempts to simply read them from the hard drive. Second, state is kept securely on the phone. The cookie data are stored in encrypted form on the phone, and only decrypted inside the phone's cryptographic hardware (hardware security module). Third, state can now move between devices. The previous problem of establishing cookies on a new computer is solved, because the phone acts as a cookie storage device. A user merely connects his phone to the new computer, and all of his state is recovered. Last, the key used to encrypt the cookie data can be based in part on the user's identity credentials. Thus, the cookie data may only be decrypted by the user, even if the cookie data are copied to another phone.

Fig. 32 is a block timing diagram of an embodiment of the present invention in which cookie data are end-to-end encrypted. The depicted embodiment shows a three-phase process for end-to-end cookie encryption. In the first, preparation phase, a web browser **3212** establishes a new session with a web server **3214**. In the second, interaction phase, the web browser and web server interact within the session, using cookies that are stored on, and encrypted by, a phone **3210**. In the third, clean-up phase, stale cookies are removed from the browser cache, leaving the browser in a pristine condition for the next user or session. It should be noted that the web browser **3212** may run on the phone **3210** as an application; in such a case, it should be noted that cryptographic secrets on the phone are stored in a hardware security module, and are inaccessible to other phone applications.

Petitioner Exhibit 1002-0842

The preparation phase begins when the browser **3212** initiates a session in process **3220**. Typically, the session begins when the browser requests a logon page from a website, although a session may be restarted due to an inactivity timeout. In process **3222** the user interacts with the logon page to logon to the website, using methods known in the art or in accordance with embodiments of this invention. Now, in process **3230**, the web server **3214** and phone **3210** establish a shared secret, or 'session key'. This session key is used to securely transfer cookie data between the phone **3210** and web server **3214**. It may be established using any technique for doing so known in the art, especially, for example, the Diffie-Hellman key exchange described above. This shared secret is known only to the phone **3210** and web server **3214**, and not to the browser **3212**. Furthermore, the shared secret is stored in the phone's hardware security module, so that even someone in possession of the phone may not easily extract it. The session key itself may be re-established each time a new session begins, providing additional security. To do so, a timestamp, or even a completely random number, may be used as the input into the shared secret generation algorithm. Once the session key is established, existing cookies left over from previous sessions are optionally encrypted with the session key in process **3240**. Process **3240** may require that the stored cookies that were previously encrypted with an old session key be decrypted. To this end, the previous session key is stored in a hardware security module of the phone **3210** (i.e., in an internal smartcard, or in an identity credential of the owner having a smartcard with an HSM). Or, the cookies may be decrypted using another private key (for example, a private key of the phone or of the owner) if they were encrypted with that key for intra-session storage. When the cookies have been encrypted using the proper session key, in process **3242** they are copied to the browser cache for use by the browser, completing preparation for interacting with the website.

Once the user has logged onto the website, the interaction phase begins. This phase may be repeated a number of times during the course of a single session. First, the user directs the web browser **3212** to request a web page in process **3250**. Typically, the server **3214** will require cookies to construct the requested web page. Thus, these cookies are sent with the web page request, using methods such as HTTP headers that are well known in the art. Cookie metadata, such as domains and paths, are kept unencrypted so that a browser **3212** may identify in process **3250** the proper cookies to send in any given request. In

Petitioner Exhibit 1002-0843

process **3252** the web server **3214** receives the cookies and decrypts them using the session key established in process **3230**. Using the decrypted cookies, the web server **3214** creates a web page and creates or updates cookies. In process **3254** the web server provides the web page and cookies to the browser. The cookies that the web server provides in process **3254** are encrypted using the same session key established in process **3230**. By using a symmetric encryption and a shared secret, no network communication by the web server to validate certificates is required for the server to perform cookie decryption. In process **3260** the browser renders the web page provided in process **3254**. The web page may contain instructions, such as Microsoft ActiveSync described above, for updating cookies on the phone in optional process **3262**. In this way, each web page may ensure that any cookies it sends are properly stored on the phone **3210**. If a page contains these instructions, then the phone stores the new or updated cookies in process **3270**. Regardless of whether these cookies are immediately stored on the phone, once the browser has rendered the web page in process **3260**, the user is free to begin the interaction phase again by requesting a new web page in process **3250**. Any cookies that were provided in process **3254** were encrypted using the session key, which the web server can use to decrypt them.

Once a sessions ends, the clean-up phase occurs. In process **3280** the cookies are deleted from the browser cache and moved to the phone, where they are stored, encrypted, until the next session is started. Deleting cookies from the browser cache keeps the computer running browser **3212** 'fresh'. Storing the cookies on the phone makes them portable and secure, requiring no complex network or server interactions.

Real-Time Certificate Updates

In current systems, there are two methods to check whether a certificate is still valid: checking a Certificate Revocation List (CRL) that is regularly updated, and checking status in real-time using an interactive status protocol. In the first method, a Certificate Authority (CA) provides a CRL to anyone seeking a list of revoked certificates. This list is produced on a regular basis, and contains all revoked certificates that have not expired. In the second method, a certificate's status is requested interactively. The status may be obtained from the CA, or produced from a batch process when the CRL is produced. The interactive request

Petitioner Exhibit 1002-0844

requires complex computations, and requires the CA to provide Internet connections that form a security risk.

In current systems, there is a lag time between actual revocation and notice of the revocation to users. Hundreds of servers need to be updated with millions of statuses, providing additional delay. In a typical example, the Department of Defense may require 18-24 hours for the notice to propagate to interested users. Thus, there exists a window of up to 24 hours for a malicious individual to take advantage of a revoked certificate.

However, real-time updates are possible in accordance with embodiments of this invention. As revocations are produced at a responsible CA, the CA determines which cellular devices are associated with the revoked certificate, as described above in connection with **Fig. 7**. In particular, process **760** includes informing parties that rely on the certificate revocations. These parties, or nearby caches, may be determined as described above in connection with **Figs. 24** and **25**. Typically, less than .01% of certificates are revoked each day. Because of the low volume, updating is a low cost process. The receiving phone can confirm the reception of the status, and the update is completed in seconds instead of the hours or even days that the update might take in current systems. CRL lists are as short as one entry long, because of the frequency and rapidity of these updates.

To ensure that the security of the system cannot be defeated, the relying party to a transaction must be assured that the cell phone presenting a certificate has been recently connected for sufficient time, and that there are no outstanding updates to the certificate's revocation status. We have described a number of methods of ensuring security of the system above under the heading "Batch Certificate Processing", including discussion of Fig. 10 and related figures. There are two cases to consider. If the relying party requires low to moderate assurance, the relying party device is likely a cellular device as well. It therefore can determine that connectivity is available and that the device offering the certificate has connectivity. Under these circumstances the relying party can depend on the phone's being updated and accurate. If there is no cellular signal available, then various timing factors are applied as described above in connection with **Fig. 27**, and depending on the location and status the relying party will determine whether or not to grant access.

On the other hand, some systems, such as physical access systems, require high levels of assurance. In these systems, the cellular system supplies updates to phones in the same

Petitioner Exhibit 1002-0845

venue as the relying parties. Now, an acknowledgement system is used, whereby each phone must acknowledge each revocation update that it receives. A phone's refusal to acknowledge a revocation update triggers the CA to notify relying parties using the same cellular tower. Depending on load, the system can send a message to all relying parties with phones that have rejected requests or could not be notified within the acceptable parameters. This real-time system updates the requestor, and also notifies relying parties of failures.

Secure Electronic Car Keys

An increasing number of cars are being equipped with smart car keys. A smart key is a key that contains a small fob or circuit for sending a cryptographic message to the car in order to enable the car to start. Any holder of the key fob can start the car -- the fob does not authenticate its user before activation.

In accordance with an embodiment of this invention, the car authenticates its owner using PKI. The car's PKI hardware and/or software is embodied in the car's computer system, or in a separate system if necessary. The owner's hardware and/or software is embodied in a key fob, or in a cell phone or PDA. In the latter cases, a car key *per se* is no longer necessary, as the purpose of the key is to authenticate its holder to the machinery, to gain access to the passenger compartment and to the starter motor. In accordance with this embodiment, the cell phone performs the authentication. Further, if the phone key certificate is revoked, the car will not start. Such a use may be very desirable to, for example, the holders of defaulted car loans who need to repossess an automobile. Merely by revoking a certificate, the driver of the car can be prevented from driving off, thereby reducing or eliminating tense confrontations between the driver and a repossession agent.

In a related embodiment, the key's use may be restricted to certain dates or times by adding software to the phone. This embodiment is useful to car rental companies, who may deactivate cars when they are not rented. In this way, a renter who exceeds the terms of his rental agreement may be prevented from entering the passenger compartment, and must call the rental company to reactivate his key. (Luckily, perhaps, his key is embodied as a cell phone.) In another related embodiment, the key software may use a GPS device in the phone. In this embodiment, the key may monitor the position or speed of the vehicle, which is useful to ensure that the driver is not exceeding a posted speed limit. Those skilled in the

Petitioner Exhibit 1002-0846

art may appreciate additional uses for a PKI-based car key that are within the scope of the invention.

Similarly, a user, having a secure electronic car key, may also permit another person to drive the user's car by providing transfer of a proxy credential to the other person's phone. The proxy credential include conditions of use (for example for only three days) established by the user.

Phone as Gateway for Trusted Data Acquisition and Storage

The mobile electronic device as described above, and especially as embodied as a smartphone, acts as a "personal" endpoint in a secure data distribution network. The endpoint is "personal," in that access to the network may be obtained only by the person who is authorized to use the particular endpoint. The network is secured using the various encryption schemes described herein, or their obvious variations.

A wide range of electronic data gathering devices can utilize a smartphone in accordance with an embodiment of the invention to take advantage of the personal and secure nature of this network. There are a proliferation of data devices available in the market that collect data personal to an individual in some way. Some of these devices may be found in the smartphone itself: for example, cameras and microphones for recording video and audio data. Some devices are not found in the phone----examples of these external devices are external audio or visual equipment, thermometers, glucose meters and other medical devices, radar guns, computers, tape recorders, and even other, wire-line telephones. An expanded PKI network as described herein may be expanded to incorporate these devices securely, so that the data gathered from, and even displayed using, these devices may be associated to a single individual and a single mobile electronic device.

By way of illustration only, and not by way of limiting the invention, this process is given concrete description below using a glucose meter (glucometer) as an exemplary data gathering device. The exemplary meter has a lancet for pricking the skin and drawing blood, a sensor for detecting the amount of glucose in a blood sample, and a digital video and audio display for reading out the detected glucose level and other information useful to a patient. The device also has a short-range wireless transceiver, such as a Bluetooth transceiver, and a cryptographic module, such as a hardware security module on a smartcard, for transacting

Petitioner Exhibit 1002-0847

with a smartphone connected to the PKI network. The device may be configured or disabled remotely. The exemplary glucometer is battery operated. Other devices, such as those listed above, and similar devices not listed for the sake of brevity, can be adapted by those having ordinary skill in the art to embody the invention described herein without undue experimentation.

Fig. 33 is a diagram showing the different components used in a method for acquiring data with an electronic data gathering device and publishing the data to trusted storage for later retrieval by a trusted individual, in accordance with an embodiment of the invention. An individual, such as patient **3310**, possesses the exemplary glucometer **3320** and a smartphone **3330**, as indicated by the broken lines. The glucometer communicates with the smartphone using Bluetooth, or other communications technology. In this embodiment, the patient receives glucometer **3320** from his doctor **3360** at a visit in which the doctor programs the glucometer with encryption information, as described more fully below. Patient **3310** proceeds to use glucometer **3320** according to its intended purpose; however, in embodiments according to this invention, the glucometer automatically transmits its glucose reading to smartphone **3330**. Upon receiving the data, smartphone **3330** attempts to save the data to a medical database in trusted storage **3350**. In particular, smartphone **3330** will determine which communications network **3340**, if any, may be used to upload the data. If none is available, smartphone **3330** may wait for a period of time and retry the upload. This process is repeated until the upload succeeds. Once the data have been uploaded, the patient's doctor **3360**, or other authorized individual, may use her own smartphone **3370** to access the medical data stored in trusted storage **3350**, using processes described above.

The above process generally requires some initialization before it can work as described. A patient is first vetted using appropriate health system standards. For instance, research into the patient's medical history may be conducted in order to satisfy insurance requirements. Once the patient is qualified to receive the device, a medical computer system issues digital encryption credentials. These credentials, in the form of public and private encryption keys, may be used to verify the patient's identity or the device identity, encrypt and decrypt medical records, or communicate securely with the data gathering device. The medical computer system also issues certificates for these credentials, which are stored on the smartphone and the device.

Petitioner Exhibit 1002-0848

The data gathering device is programmed with several encryption keys and certificates. Programming may be done during an office visit or consultation, for example. In order for the doctor to program the device, the device itself must be present, along with access to the user's key. This key is stored on the user's phone, which the patient brings to the doctor's office. The doctor may access using a docking station or cradle. The docking station itself may connect to the data gathering device using a data connection. Or, the docking station may be a computer, in which case the device is programmed by executing a suitable computer program, connecting the phone and device to the computer in turn. Once the key is stored in the device, the onboard cryptographic module may use the key to encrypt and decrypt data. Although the example of a glucometer is used, other medical and non-medical embodiments of the invention may use analogous initialization procedures to prepare the device for use.

Fig. 34 is a block diagram of the process for uploading data in the method of Fig. 33. The method begins with process **3410**, in which a user acquires data using a data gathering device. In an exemplary embodiment, a glucometer senses a concentration of glucose in a patient blood sample. In process **3420** the gathered data are encrypted in the device, using a public encryption key of the phone's user. As described above, this key was pre-programmed into the data gathering device. In process **3430** the encrypted data are transmitted from the device to the user's smartphone. Because the data are encrypted such that only the user may decrypt it, the transmission in process **3430** may be done without further channel-level encryption, although such encryption may be optionally performed using device-specific encryption keys for the data gathering device or the smartphone. Once the data appear in the smartphone, the phone attempts to publish it to trusted storage in process **3440**. In process **3440** the phone attempts to contact trusted storage using several alternate forms of communication. In an exemplary embodiment, the phone may attempt to access a wireless cellular telephone network or the Internet. When a connection is established, the phone uploads the data to the trusted storage database. Once stored in the database, the data are now available for retrieval by appropriate, authorized individuals, such as doctors, police officers, co-workers, or others. An individual may be authorized to view that data based on several criteria which are discussed above. For example, data regarding a patient's blood glucose may be released to the patient's doctor, but also to an emergency

Petitioner Exhibit 1002-0849

medical technician (EMT) at the scene of an emergency if the EMT requests the data using proper, verifiable medical credentials in a mobile electronic device.

Fig. 35 is a block diagram of a method for a trusted individual to access data acquired and published as in the embodiment of Fig. 34. In process **3510** an authorized individual constructs a request for the data. Such a request may take the form of a database query, for example. This request also contains cryptographic information regarding the requesting individual, including that individual's credentials and certificates, or sufficient information to locate them. The credentials may be sent in the form of a digital resume, as described above. In process **3520** the request is transmitted to a system having control over the trusted storage. The request may be sent using any convenient mechanism, including web-based services. In process **3530** the trusted storage system determines whether to honor the request for the data. The determination includes evaluating at least the credentials of the individual, and may incorporate such other factors as the system operator or application requires. These factors are contained within trust chains associated with the patient, or other data depositor. When the appropriate information has been assembled and evaluated, and all trust chains have been walked and validated, process **3540** determines one of two outcomes. If the request should be denied, in process **3542** a denial notice is sent back to the requesting individual, and appropriate security measures may be taken to validate the access. If the request should be honored, in process **3550** the data (after being decrypted using the individual's private key) are thereafter encrypted using the requestor's public encryption key and transmitted to the requestor. Upon receiving the response, the requestor can decrypt it using her own private encryption key, and use the data contained within.

In addition to viewing the data, a doctor or other authorized individual may analyze it. In such cases, the doctor may decide that a message should be sent to the patient regarding his health care. According to an embodiment of this invention, the data gathering device may also act as an informational device for such communications. In such cases, the device may be equipped with a data receiver to receive data from the mobile electronic device, and an audio or video display to display the received data. Of course, the display also may be used to display data gathered by the sensor.

Fig. 36 is a block diagram of a method for a trusted individual to transmit information to the measuring device of Fig. 33. In process **3610** the trusted individual, such as the

Petitioner Exhibit 1002-0850

doctor, retrieves a public encryption key for the target device from a database. As mentioned above, this key is created before the device is placed in service, and may be stored on a hardware security module embedded within the device. The database itself is stored in trusted storage. In process **3620** the doctor uses her phone to encrypt data for the target patient device, using techniques known in the art. In process **3630** the doctor's phone determines the best communications channel for contacting the target device and uploads the message, in the manner of process **3440**. At this point, the individual's phone cannot display the message because it has been encrypted with the device's public encryption key, the decryption key for which is stored only in the device itself. In process **3640** the phone transmits the data to the target device. As before, this message may be transmitted without channel encryption, because only the target device can decrypt it. Finally, in process **3650** the device decrypts the data for display using the video and/or audio displays.

The embodiment described above has several advantages. All data are encrypted using the patient's public encryption key. The patient validates his identity and controls the transmission of all data which is protected by his encryption key. The data gathering device can also be updated, and transmissions to the device will be encrypted, with the device public encryption key. Thus even software updates must be validated. The use of these encryption keys enhances overall system security.

As a further advantage, the smartphone acts as a local data server. It has all of the necessary certificates for data gathering devices and trusted storage servers to validate system communications. Each system component validates each message before it makes any acknowledgements of them. Each system component has its own certificate, including the patient phone. The user has an identity certificate that is used to issue a challenge for any sensitive transactions. Since a smartphone in accordance with an embodiment of the invention can include significant memory, all communications between the data gathering device and the phone can be done without a cellular network. This feature can represent a significant cost savings for manufacturers of data gathering devices who wish for their devices to take advantage of the PKI network system described herein.

As an additional advantage, the trusted cloud server has a certificate and is treated like any other device on the network. All communications are encrypted by the patient's encryption keys. Therefore there is no single key that can decode all of the data on the

Petitioner Exhibit 1002-0851

trusted storage server, enhancing overall security. A trusted storage server can be configured to deny general logins, and to only process trusted transactions. Based on a transaction's content, its data may be published to various distributed trusted servers. Patient data may be published to a patient-accessible server in which all data remains encrypted until requested by the patient. Such data can be accessed only by that patient, or an authorized individual. An enterprise server and database may be created to house this data. Access to patient-identifying data, including that covered by laws such as HIPAA, requires validation of a trust chain and a high level of assurance. Thus, the system can be configured with sufficient security features to comply with applicable governing laws.

The present invention may be embodied in many different forms, including, but not limited to, computer program logic for use with a processor (e.g., a microprocessor, microcontroller, digital signal processor, or general purpose computer), programmable logic for use with a programmable logic device (e.g., a Field Programmable Gate Array (FPGA) or other PLD), discrete components, integrated circuitry (e.g., an Application Specific Integrated Circuit (ASIC)), or any other means including any combination thereof.

Computer program logic implementing all or part of the functionality previously described herein may be embodied in various forms, including, but in no way limited to, a source code form, a computer executable form, and various intermediate forms (e.g., forms generated by an assembler, compiler, linker, or locator). Source code may include a series of computer program instructions implemented in any of various programming languages (e.g., an object code, an assembly language, or a high-level language such as Fortran, C, C++, JAVA, or HTML) for use with various operating systems or operating environments. The source code may define and use various data structures and communication messages. The source code may be in a computer executable form (e.g., via an interpreter), or the source code may be converted (e.g., via a translator, assembler, or compiler) into a computer executable form.

The computer program may be fixed in any form (e.g., source code form, computer executable form, or an intermediate form) either permanently or transitorily in a tangible storage medium, such as a semiconductor memory device (e.g., a RAM, ROM, PROM, EEPROM, or Flash-Programmable RAM), a magnetic memory device (e.g., a diskette or fixed disk), an optical memory device (e.g., a CD-ROM), a PC card (e.g., PCMCIA card), or

Petitioner Exhibit 1002-0852

other memory device. The computer program may be fixed in any form in a signal that is transmittable to a computer using any of various communication technologies, including, but in no way limited to, analog technologies, digital technologies, optical technologies, wireless technologies (e.g., Bluetooth), networking technologies, and internetworking technologies. The computer program may be distributed in any form as a removable storage medium with accompanying printed or electronic documentation (e.g., shrink wrapped software), preloaded with a computer system (e.g., on system ROM or fixed disk), or distributed from a server or electronic bulletin board over the communication system (e.g., the Internet or World Wide Web).

Hardware logic (including programmable logic for use with a programmable logic device) implementing all or part of the functionality previously described herein may be designed using traditional manual methods, or may be designed, captured, simulated, or documented electronically using various tools, such as Computer Aided Design (CAD), a hardware description language (e.g., VHDL or AHDL), or a PLD programming language (e.g., PALASM, ABEL, or CUPL).

Programmable logic may be fixed either permanently or transitorily in a tangible storage medium, such as a semiconductor memory device (e.g., a RAM, ROM, PROM, EEPROM, or Flash-Programmable RAM), a magnetic memory device (e.g., a diskette or fixed disk), an optical memory device (e.g., a CD-ROM), or other memory device. The programmable logic may be fixed in a signal that is transmittable to a computer using any of various communication technologies, including, but in no way limited to, analog technologies, digital technologies, optical technologies, wireless technologies (e.g., Bluetooth), networking technologies, and internetworking technologies. The programmable logic may be distributed as a removable storage medium with accompanying printed or electronic documentation (e.g., shrink wrapped software), preloaded with a computer system (e.g., on system ROM or fixed disk), or distributed from a server or electronic bulletin board over the communication system (e.g., the Internet or World Wide Web).

The present invention may be embodied in other specific forms without departing from the true scope of the invention. Any references to the "invention" are intended to refer to exemplary embodiments of the invention and should not be construed to refer to all embodiments of the invention unless the context otherwise requires. The described

Petitioner Exhibit 1002-0853

embodiments are to be considered in all respects only as illustrative and not restrictive. Numerous variations and modifications will be apparent to those skilled in the art. All such variations and modifications are intended to be within the scope of the present invention as defined in any appended claims.

Petitioner Exhibit 1002-0854

What is claimed is:

1. A process for authenticating an individual to participate in a transaction with a relying party, the process comprising:

producing a mobile electronic device, the device storing a digitally signed document containing a set of credential data of the individual, and requiring, as a condition to using the stored set of credential data for authentication purposes, entry into the device of authentication data authenticating a would-be user of the device as the individual;

entering the authentication data into the device to authenticate the individual to the device, so that the individual can use the stored set of credential data; and

causing the device to communicate the set of credential data to a system of the relying party, for purposes of authenticating the individual to participate in the transaction.

2. A process according to claim 1, wherein the transaction includes a purchase.

3. A process according to claim 1, wherein the transaction includes receiving an extension of credit.

4. A process according to claim 1, wherein the transaction includes obtaining access to money stored in a financial account.

5. A process according to claim 1, wherein the transaction includes obtaining access to a physical location.

6. A process according to claim 1, wherein the transaction includes obtaining access to a web page.

7. A process according to claim 1, wherein the transaction includes obtaining access to a computing resource.

8. A process according to claim 1, wherein the transaction includes obtaining access to data by downloading.

9. A process according to claim 1, wherein the transaction includes receiving an HTTP cookie.

10. A process according to claim 1, wherein the transaction includes uploading medical data of the individual.

11. A process according to claim 1, wherein the mobile electronic device includes one of a smartphone and a personal digital assistant.

12. A process according to claim 1, wherein the mobile electronic device includes WORM

Petitioner Exhibit 1002-0855

memory.

13. A process according to claim 12, wherein the WORM memory includes a set of encryption data, the set having a private encryption key of the individual.

14. A process according to claim 12, wherein the WORM memory includes a set of encryption data, the set having a private signature key of the individual.

15. A process according to claim 12, wherein the mobile electronic device includes a display and an advertisement associated with an item in the set of encryption data, the process further comprising displaying the advertisement on the display in connection with use of the device.

16. A process according to claim 15, wherein the advertisement is stored in the WORM memory.

17. A process according to claim 1, wherein the set of credential data is derived from one or more of: a passport, a birth certificate, a Transportation Worker Identification Credential (TWIC), a Common Access Card (CAC), a smartcard, a driver's license, a pilot's certificate, an identification card, an organization membership card, an insurance card, a credit card, a debit card, a store discount card, a public transportation card, or a library card.

18. A process according to claim 1, wherein entering authentication data includes entering data pertaining to one of: a fingerprint, a handprint, a photograph, an iris scan, a retina scan, a password, an authorization code, or a personal identification number.

19. A process according to claim 1, wherein entering authentication data includes providing two-factor authentication data.

20. A process according to claim 19, wherein entering authentication data includes providing a password and biometric data.

21. A process according to claim 1, wherein causing the device to communicate includes triggering wireless communication by the device.

22. A process according to claim 1, wherein the system of the relying party includes one of: a vending machine, a parking meter, an electronic toll collection system, a physical access system, and a magnetic stripe reader.

23. A process according to claim 1, wherein a suite of applications is stored on the device, and the set of credential data identifies a subset of the suite of applications to be made available to the individual upon authentication of the would-be user as the individual.

24. A process according to claim 1, further comprising:

Petitioner Exhibit 1002-0856

causing the device to run an application loaded thereon, the application being unavailable for use until there has been entry into the device of authentication data authenticating the would-be user of the device as the individual.

25. A process according to claim 1, further comprising:

receiving at the mobile electronic device, from the system of the relying party, a response to the communication of the set of credentials.

26. A process according to claim 25, wherein receiving the response includes receiving a verification of the set of credential data of the individual.

27. A process according to claim 25, wherein receiving the response includes receiving a notification that the transaction has been completed.

28. A process according to claim 25, wherein receiving the response triggers updating a transaction log maintained on the mobile electronic device.

29. A process according to claim 28, wherein receiving the response triggers setting of an upload flag to enqueue uploading of data reflecting the transaction.

30. A process according to claim 25, wherein the mobile electronic device includes a WORM memory, and the mobile device performs, on the WORM memory, an operation triggered by receiving the response.

31. A process according to claim 30, wherein the operation is storage of data related to the response.

32. A process according to claim 30, wherein the operation is rendering a portion of the WORM memory unreadable.

33. A process according to claim 1, wherein causing the device to communicate the set of credential data triggers storing, in a transaction log maintained on the mobile electronic device, a record having data related to the transaction.

34. A process for use by a relying party in authenticating an individual having a mobile electronic device to participate in a transaction with the relying party, the device storing a digitally signed document containing a set of credential data of the individual and requiring, as a condition to using the stored set of credential data for authentication purposes, entry into the device of authentication data authenticating a would-be user of the device as the individual, the process comprising:

receiving, in a system in communication with the device, the digitally signed

Petitioner Exhibit 1002-0857

document from the device, wherein receipt of the digitally signed document constitutes verification of entry into the device of the authentication data;

using the system to evaluate a credential in the set of credentials; and

storing data, associated with the transaction and the digitally signed document, in the system of the relying party in a transaction log.

35. A process according to claim 34, wherein the transaction includes a purchase.

36. A process according to claim 34, wherein the transaction includes granting an extension of credit.

37. A process according to claim 34, wherein the transaction includes providing access to money stored in a financial account.

38. A process according to claim 34, wherein the transaction includes providing access to a physical location.

39. A process according to claim 34, wherein the transaction includes providing access to a web page.

40. A process according to claim 34, wherein the transaction includes providing access to a computing resource.

41. A process according to claim 34, wherein the transaction includes providing access to data for downloading by the individual.

42. A process according to claim 34, wherein the transaction includes transmitting an HTTP cookie.

43. A process according to claim 34, wherein the mobile electronic device includes one of a smartphone and a personal digital assistant.

44. A process according to claim 34, wherein the mobile electronic device includes WORM memory.

45. A process according to claim 44, wherein the WORM memory includes a set of encryption data, the set having a private encryption key of the individual.

46. A process according to claim 44, wherein the WORM memory includes a set of encryption data, the set having a private signature key of the individual.

47. A process according to claim 46, wherein using the system to evaluate the credential includes validating a digital signature of the digitally signed document, using a public signature key of the individual that forms a key pair with the private signature key of the

Petitioner Exhibit 1002-0858

individual.

48. A process according to claim 34, wherein the set of credential data is derived from one or more of: a passport, a birth certificate, a Transportation Worker Identification Credential (TWIC), a Common Access Card (CAC), a smartcard, a driver's license, a pilot's certificate, an identification card, an organization membership card, an insurance card, a credit card, a debit card, a store discount card, a public transportation card, or a library card.

49. A process according to claim 34, wherein receiving the digitally signed document includes receiving the document wirelessly.

50. A process according to claim 34, wherein using the system to evaluate the credential includes validating a digital signature of the digitally signed document using a public signature key of the individual.

51. A process according to claim 34, wherein using the system to evaluate the credential includes comparing a digest derived from the credential with a stored digest.

52. A process according to claim 34, wherein using the system to evaluate the credential includes comparing the time the digitally signed document was received from the device with a timestamp in the document.

53. A process according to claim 52, wherein the timestamp is indicative of the time when credentials on the mobile electronic device were last updated.

54. A process according to claim 53, wherein the timestamp is indicative of the time when the mobile electronic device was last connected to a network in a session meeting pre-specified criteria.

55. A process according to claim 34, wherein using the system to evaluate the credential includes obtaining a certificate status response from the mobile electronic device.

56. A process according to claim 55, wherein obtaining the certificate status response comprises:

transmitting a first message including a cryptographic nonce to the mobile electronic device, the first message encrypted with a public encryption key of the individual; and

receiving a second message including the nonce and the certificate status response from the mobile electronic device.

Petitioner Exhibit 1002-0859

57. A process according to claim 34, wherein using the system to evaluate the credential includes communicating with a computer system, of a third party, that can validate the accuracy of the credential or verify that the credential is unexpired.

58. A process according to claim 57, wherein the third party is an issuer of the credential or an agent of the issuer.

59. A process according to claim 57, further comprising obtaining a certificate status response from the third party.

60. A process according to claim 57, further comprising obtaining a certificate revocation list from the third party.

61. A process according to claim 57, wherein communicating includes receiving, from the third party, data indicating that the credential has not been revoked.

62. A process according to claim 34, further comprising:

transmitting, to the mobile electronic device, a response to the communication of the set of credentials.

63. A process according to claim 62, wherein transmitting the response includes transmitting data indicating that a credential in the set of credentials is valid and unexpired.

64. A process according to claim 62, wherein transmitting the response includes transmitting a notification that the transaction has been completed.

65. A mobile electronic device, usable by an individual for authentication of transactions, the device comprising:

a storage module in which are stored:

(i) a digitally signed document containing a set of credentials of the individual, and

(ii) authentication data of the individual;

a data entry arrangement for entering data into the device;

a controller, coupled to the storage module and the data entry arrangement, programmed to require, as a condition to using the stored set of credentials for authentication purposes, entry of the authentication data into the device via the data entry arrangement, so as to authenticate a would-be user of the device as the individual; and

a communication port for receiving and transmitting the digitally signed document.

66. A device according to claim 65, wherein the set of credentials includes a plurality of

Petitioner Exhibit 1002-0860

credentials of the individual, so that the device can be used to authenticate distinct classes of transactions, each class of transactions being associated with a distinct one of the credentials.

67. A device according to claim 65, wherein the storage module includes non-volatile memory.

68. A device according to claim 65, wherein the storage module includes WORM memory.

69. A device according to claim 68, wherein the WORM memory includes the digitally signed document.

70. A device according to claim 68, wherein the WORM memory includes a set of encryption data, the set having a private encryption key of the individual.

71. A device according to claim 68, wherein the WORM memory includes a set of encryption data, the set having a private signature key of the individual.

72. A device according to claim 65, wherein the storage module includes both WORM memory and WMRM memory incorporated in flash memory.

73. A device according to claim 65, wherein the storage module includes an application, stored therein, and the device further comprises:

an access control module restricting use of the application until there has been entry into the device, via the data entry arrangement, of the authentication data, to authenticate the would-be user of the device as the individual.

74. A process for configuring an electronic device to be usable by an individual for authentication of transactions, the process comprising:

storing a digitally signed document in the electronic device, the digitally signed document including credential data derived from a set of credentials pertaining to the individual;

storing, in the electronic device, authentication data associated with the individual;

wherein the device includes an access control module that precludes access to the credential data without entry into the device of the authentication data.

75. A process according to claim 74, wherein the set of credentials includes a physical credential.

76. A process according to claim 75, wherein the physical credential is selected from the group consisting of: a passport, a birth certificate, a Transportation Worker Identification Credential (TWIC), a Common Access Card (CAC), a smartcard, a driver's license, a pilot's

Petitioner Exhibit 1002-0861

certificate, an identification card, an organization membership card, an insurance card, a credit card, a debit card, a store discount card, a public transportation card, and a library card.

77. A process according to claim 74, wherein the set of credentials includes a virtual credential.

78. A process according to claim 74, further comprising:

receiving the physical credential from the individual;

manually determining that the set of credentials pertains to the individual;

creating the digitally signed document; and

entrusting the device to the individual.

79. A process according to claim 74, further comprising obtaining biometric data of the individual and including the biometric data in the authentication data.

80. A process according to claim 74, wherein a digital signature in the digitally signed document is verifiable using a public signature key of the individual.

81. A process according to claim 74, wherein a digital signature in the digitally signed document is verifiable using a public signature key of a third party.

82. A process according to claim 74, wherein the electronic device includes WORM memory, and storing the digitally signed document in the electronic device includes storing the document in the WORM memory.

83. A process according to claim 74, further comprising storing a private encryption key of the individual in the electronic device.

84. A process according to claim 74, further comprising storing a private signature key of the individual in the electronic device.

85. A computer-implemented method of developing information pertinent to authentication of a set of credentials of a given individual, the set of credentials associated with a plurality of sets of credentials of other individuals, the method comprising:

for each of the individuals,

verifying such individual's credentials as being at the end of a chain of trust,

placing such individual's credentials in a digitally signed document, and

storing the digitally signed document in a credential database; and

automatically and repetitively checking, in a computer process, for revocation of any credentials in the credential database and storing data identifying credentials that have been

Petitioner Exhibit 1002-0862

revoked.

86. A method according to claim 85, wherein storing data identifying credentials that have been revoked includes updating the credential database.

87. A method according to claim 85, wherein storing data identifying credentials that have been revoked includes storing in a revocation database a listing of credentials that have been revoked.

88. A method according to claim 85, further comprising, for each of the individuals, storing the digitally signed document includes storing it in a token entrusted to such individual.

89. A method according to claim 85, wherein checking includes checking at least as often as once per day.

90. A method according to claim 85, wherein checking includes checking in conformity with a PKI standard.

91. A computer-implemented method of authenticating a given individual's set of credentials, each credential in the set having been authenticated as of a given time, the method comprising:

receiving the set of credentials over a communications network; and

in a computer process, comparing the set of credentials against a database listing of revoked credentials to identify a credential in the set that has been revoked since the given time.

92. A method according to claim 91, wherein receiving the set of credentials comprises receiving them from a federated data store.

93. A method according to claim 91, wherein receiving the set of credentials comprises uploading a digital document from a token in the possession of the given individual, such digitally signed document containing the individual's set of credentials.

94. A method according to claim 91, wherein identifying credentials of the individual that have been revoked implicitly determines that all other credentials of the given individual have not been revoked.

95. A method according to claim 91, wherein comparing is performed in a batch computer process.

96. A computer-implemented method of processing transactions between a relying party having a transaction system, and a set of individuals, each individual in the set of individuals

Petitioner Exhibit 1002-0863

having an electronic device capable of communication with the transaction system, the method comprising:

obtaining access to a first digitally signed document created in the transaction system of the relying party, the document containing one or more transaction records, each transaction record having data pertaining to a selected transaction between the relying party and a selected individual in the set of individuals; and

for each selected transaction,

obtaining access to a second digitally signed document created in the electronic device of the selected individual, the document containing a transaction record corresponding to the selected transaction; and

in a computer process, checking for consistency between the transaction record in the first digitally signed document and the transaction record in the second digitally signed document.

97. A method according to claim 96, further comprising validating a digital signature of the first digitally signed document, using a public signature key of the relying party.

98. A method according to claim 96, further comprising, validating a digital signature of the second digitally signed document of the selected individual, using a public signature key of the selected individual.

99. A method according to claim 96, further comprising, in the event that checking yields an inconsistency, communicating a warning to the relying party or the selected individual.

100. A method according to claim 96, wherein each transaction record contains data pertaining to at least one of a transaction time, a transaction date, a purchase amount, a loan number, a financial account number, a physical location, an address of a web page, an identifier of a computing resource, a file name, an HTTP cookie name, and a medical condition.

101. A method according to claim 96, wherein obtaining access to the first digitally signed document includes receiving the first digitally signed document over a computer data network.

102. A method according to claim 96, wherein obtaining access to the second digitally signed document includes receiving the second digitally signed document over a computer data network.

Petitioner Exhibit 1002-0864

103. A method according to claim 96, wherein checking is performed in a batch computer process.

104. A method according to claim 96, wherein checking is performed in a process substantially contemporaneously with the selected transaction.

105. A system enabling a second party to obtain data in a secure manner from a first party, the system comprising:

a receiving port for securely receiving the data, along with a digitally signed document associated with the first party and a reference to the second party;

a physical data storage medium for storing the received data and the digitally signed document in association with the second party;

a processor for validating that the sender of the received data is the first party using the digitally signed document, and for determining whether to securely forward data stored in the storage area to the second party according to a rule associated with the first party and the second party; and

a transmitting port for forwarding the data to a computer facility of the second party.

106. A system according to claim 105, wherein the storage area is readable only by the first party and the second party.

107. A system according to claim 105, wherein the storage area is associated with a URL.

108. A computerized method enabling a second party to obtain data in a secure manner from a first party, the method comprising:

receiving from the first party items including the data, a digitally signed document associated with the data and with the first party, and a reference to the second party;

verifying that the received data were sent by the first party, by using the digitally signed document;

storing the data in association with the digitally signed document and with the reference; and

making the stored data available to the second party using the reference, such that the second party may securely access the data.

109. A method according to claim 108, wherein the data have been encrypted using a public key of the second party.

110. A method according to claim 108, wherein the items are included in a message that has

Petitioner Exhibit 1002-0865

been encrypted using a public key associated with the receiver and receiving the items includes:

receiving the message from the first party, and

decrypting the message using a private key associated with the public key.

111. A method according to claim 108, wherein the reference includes at least one of a digital certificate, a telephone number, a postal address, and an electronic address.

112. A method according to claim 108, wherein making the stored data available comprises:

encrypting a second message, containing the data and the digitally signed document, using a public key of the second party; and

transmitting the encrypted second message to the second party.

113. A method according to claim 108, wherein the storage space is readable only by the first party and the second party.

114. A method according to claim 108, wherein receiving the data from the first party includes using a secure communications link.

115. A method according to claim 108, further comprising deciding whether to forward the data to the second party according to a set of computer-implemented rules associated with the first party and the second party.

116. A method according to claim 108, further comprising forwarding the data to the second party.

117. A method according to claim 116, wherein forwarding the data to the second party includes using a secure communications link.

118. A method according to claim 108, wherein receiving the items from the first party includes receiving the items through a communications gateway that is not dedicated to handling trusted data from a particular source.

119. A method according to claim 118, wherein the communications gateway also handles data other than trusted data.

120. A method according to claim 118, wherein verifying that the received data were sent by the first party is accomplished by the communications gateway.

121. A method according to claim 120, wherein verifying that the received data were sent by the first party includes accessing an authorized certificate store to retrieve a certificate of the first party.

Petitioner Exhibit 1002-0866

122. A method according to claim 121, wherein making the stored data available to the second party using the reference is accomplished by the communications gateway.

123. A method according to claim 120, wherein storing the data in association with the digitally signed document and with the reference is caused by the communications gateway.

124. A method according to claim 118, further comprising:

upon receiving the items from the first party, initiating communication with the second party to obtain authorization to cause storage of the data.

125. A method according to claim 124, wherein the second party has a mobile telephone, and making the stored data available to the second party includes sending a communication to the mobile telephone identifying the received data and seeking authorization to make the received data available to the second party, and, upon such authorization, making the received data available to the second party.

126. A method according to claim 125, wherein making the received data available to the second party includes making the data accessible to the mobile telephone for storage in memory thereof.

127. A method according to claim 126, wherein the memory of the mobile telephone is flash memory.

128. A method according to claim 126, wherein the data include information relating to a credential, and making the data accessible to the mobile telephone for storage in memory thereof includes making the data accessible for storage only in a portion of such memory configured as WORM memory.

129. A method according to claim 108, wherein the data include information relating to a credential, and making the stored data available to the second party includes making the data accessible for storage only in memory configured as WORM memory.

130. A method according to claim 129, wherein the WORM memory is implemented in flash memory.

131. A method according to claim 108, wherein the data are digital media content encrypted with a public key of the second party.

132. A computerized method for creating a virtual smartcard for an individual based on a physical credential applicable to the individual, the method comprising:

receiving, over a communications network, credential data derived from the physical

Petitioner Exhibit 1002-0867

credential;

receiving, over the communications network, authentication data pertinent to the individual;

using a computer process to establish a pair of cryptographic keys; and

creating a virtual smartcard for the individual by storing the credential data and the authentication data in association with the pair of cryptographic keys.

133. A method according to claim 132, wherein the physical credential is selected from the group consisting of a passport, a birth certificate, a Transportation Worker Identification Credential (TWIC), a smartcard, a driver's license, a pilot's certificate, an identification card, an organization membership card, an insurance card, a credit card, a debit card, a store discount card, a public transportation card, and a library card.

134. A method according to claim 132, wherein authentication data are selected from the group consisting of biometric data and a passcode.

135. A method of evaluating a primary credential issued by an agency, the method comprising:

using the primary credential to access from storage a summary certificate associated in the storage with the primary credential, the summary certificate containing a collection of secondary credentials considered by the agency in issuing the primary credential;

in a revocation computer process, collecting secondary credential revocation information by (i) identifying each of the secondary credentials that is the subject of a revocation, and, (ii) for each revoked credential, accessing data that characterize a basis for the revocation; and

in an evaluation computer process, applying a set of policy rules to the collected secondary credential revocation information to evaluate its effect on the primary credential.

136. A method according to claim 135, wherein the revocation computer process includes accessing a database of revoked credentials, the database established by automatic, computer-implemented, repetitive checking for revocation of secondary credentials of a plurality of individuals.

137. A method according to claim 135, wherein one of the secondary credentials that is the subject of revocation is another primary credential that has been previously revoked by operation of computer processes, so that processes herein may spawn a cascade of

Petitioner Exhibit 1002-0868

revocations when permitted by policy rules to do so.

138. A method according to claim 135, wherein accessing data that characterize a basis for the revocation include accessing data indicating that a chain of trust for a secondary credential has been broken.

139. A method according to claim 135, further comprising revoking the primary credential when the policy rules being applied so require.

140. A method according to claim 135, wherein the evaluation computer process leads to revocation of the primary credential, further comprising:

in a further revocation computer process, identifying a set of additional primary credentials, the set having at least one member, for which the primary credential serves as a secondary credential in a corresponding set of summary certificates; and

in a further evaluation computer process, subjecting the set of primary credentials to evaluation in a manner generally analogous to the evaluation computer process.

141. A computerized method for responding to a given individual's request for access, the method comprising:

receiving, over a first communications network, a first data set defining rights of the given individual to access;

receiving, over a second communications network, from a token possessed by the given individual, a digitally signed document including a second data set defining rights of the given individual relating to the access; and

in a computer process, comparing the first access rights data and the second access rights data to respond to the given individual's access rights.

142. A method according to claim 141, wherein receiving over the first communications network includes receiving data from a cellular telephone network.

143. A method according to claim 141, wherein receiving over the first communications network includes receiving data from the Internet.

144. A method according to claim 143, wherein receiving over the first communications network includes receiving data from a virtual private network.

145. A method according to claim 141, wherein receiving over the second communications network includes receiving data from a Bluetooth network.

146. A method according to claim 141, wherein the token is a smartphone.

Petitioner Exhibit 1002-0869

147. A method according to claim 141, further comprising validating a digital signature of the digitally signed document.

148. A method according to claim 147, wherein validating the digital signature includes receiving data from the token pertaining to a digital certificate, the digital certificate having a public signature key.

149. A method according to claim 148, wherein receiving data includes receiving a cached OCSP response.

150. A non-volatile memory device encoded with computer-readable data, such device including a first portion thereof configured as WORM memory in which are encoded credential data and a second portion thereof configured as WMRM memory.

151. A device according to claim 150, wherein the device is also encoded with computer-readable instructions, such instructions including program code defining a cryptographic engine.

152. A device according to claim 150, wherein the credential data relate to a plurality of credentials of an individual.

153. A device according to claim 150, such device being implemented in flash memory.

154. A method for efficiently authenticating an individual in connection with a transaction, at a physical transaction location, such location using a public key infrastructure and having a terminal for use in the transaction, the method comprising:

using data provided over a cellular telephone network to estimate a present location of a smartphone of the individual on which is stored credential data relating to a credential of the individual, such smartphone requiring the individual to authenticate himself to the smartphone as a condition of use of the credential data;

if the present location is determined to be within a specified range of the physical transaction location, sending data as to status of the credential to the terminal,

so that the individual will be able to present the credential for use in the transaction only by authenticating himself to the smartphone, and status information of the credential will be available to the terminal for use in connection with the transaction when the individual appears at the physical location.

155. A method according to claim 154, wherein using data provided over a cellular telephone network to estimate a present location includes using base station data.

Petitioner Exhibit 1002-0870

156. A method according to claim 154, wherein using data provided over a cellular telephone network to estimate a present location includes using GPS data from the smartphone.

157. A method for gating communication to a user's smartphone from a caller's smartphone based on a set of pre-specified criteria as to attributes of the caller, the method comprising:

receiving on the user's smartphone a control message from the caller's smartphone constituting a request to establish communication with the user's smartphone, such control message including a credential of the caller;

using a process running on the user's smartphone, determining validity of the credential, and if the credential is determined to be valid, evaluating the credential for conformity with the set of criteria;

if the credential is determined to be in conformity with the set of criteria, then allowing the communication to be established.

158. A method according to claim 157, wherein the set of criteria includes presence of the name of the caller on a white list.

159. A method according to claim 157, wherein the user has an age, and the set of criteria includes a requirement that the caller have an age that is within two years of the user's age.

160. A data gathering device for communicating with a mobile electronic device of an individual, the mobile electronic device being capable of decrypting messages according to an encryption key of the individual, the data gathering device comprising:

a sensor for gathering data;

a cryptographic module for encrypting gathered data using the encryption key; and

a transmitter for transmitting encrypted data to the mobile electronic device.

161. A device according to claim 160, wherein the transmitter is a Bluetooth transmitter.

162. A device according to claim 160, wherein the cryptographic module is a hardware security module.

163. A device according to claim 160, further comprising a smartcard, wherein the cryptographic module is embedded within the smartcard.

164. A device according to claim 160, further comprising:

a receiver for receiving encrypted data from the mobile electronic device; and

a display for displaying received data,

wherein the cryptographic module is further capable of decrypting received data according to

Petitioner Exhibit 1002-0871

the encryption key.

165. A device according to claim 164, wherein the display is a video display.

166. A device according to claim 164, wherein the display is an audio display.

167. A device according to claim 164, wherein the display is further capable of displaying gathered data.

168. A device according to claim 160, wherein the sensor gathers medical data, and the data gathering device is a medical device.

169. A method for securely obtaining, from a medical data gathering device, medical data pertinent to an individual, the method comprising:

receiving the medical data over a wireless network from a smartphone of the individual coupled to the medical data gathering device, wherein:

(i) the smartphone stores and forwards, over the wireless network, the data from the medical data gathering device; and

(ii) the medical data are encrypted with a public key of the individual.

170. A method according to claim 169, wherein the smartphone is wirelessly coupled to the medical data gathering device.

171. A method according to claim 169, wherein the smartphone includes flash memory in which the medical data are stored.

172. A method according to claim 169, wherein the smartphone includes a storage module in which is stored a digitally signed document containing a set of credentials of the individual.

173. A method according to claim 172, wherein the storage module also stores authentication data of the individual and the smartphone further includes a data entry arrangement for entering data into the device, a controller, coupled to the storage module and the data entry arrangement, programmed to require, as a condition to using the stored set of credentials for authentication purposes, entry of the authentication data into the device via the data entry arrangement, so as to authenticate a would-be user of the device as the individual.

174. A method according to claim 169, further comprising storing the data received over the wireless network in a database coupled to a server for access by authorized medical professionals.

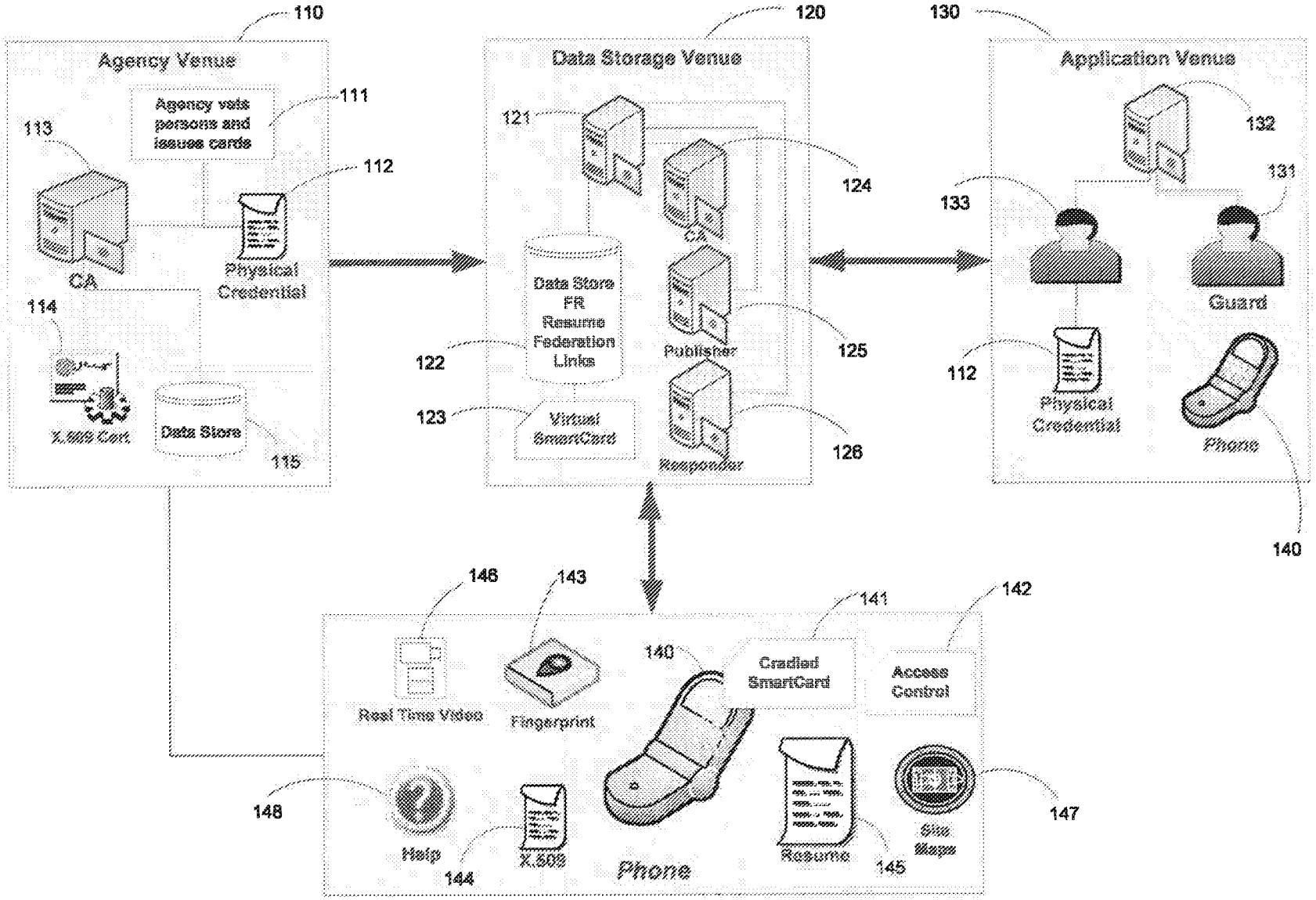
175. A method according to claim 174, further comprising decrypting and granting access to the medical data in response to a request by a person determined to be an authorized medical

Petitioner Exhibit 1002-0872

professional.

Petitioner Exhibit 1002-0873

FIG. 1



Petitioner Exhibit 1002-0874

FIG. 2A

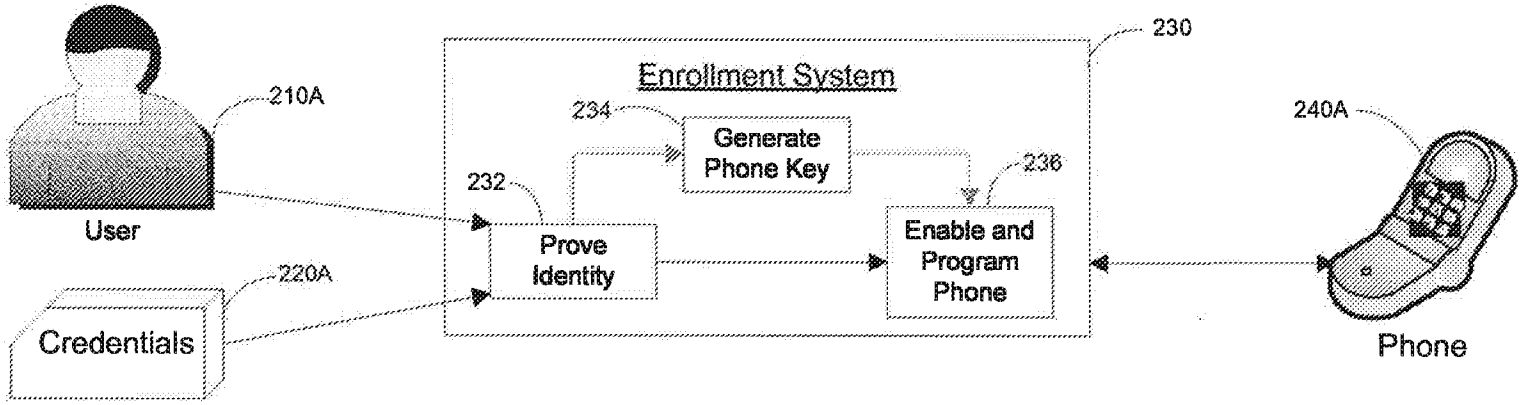
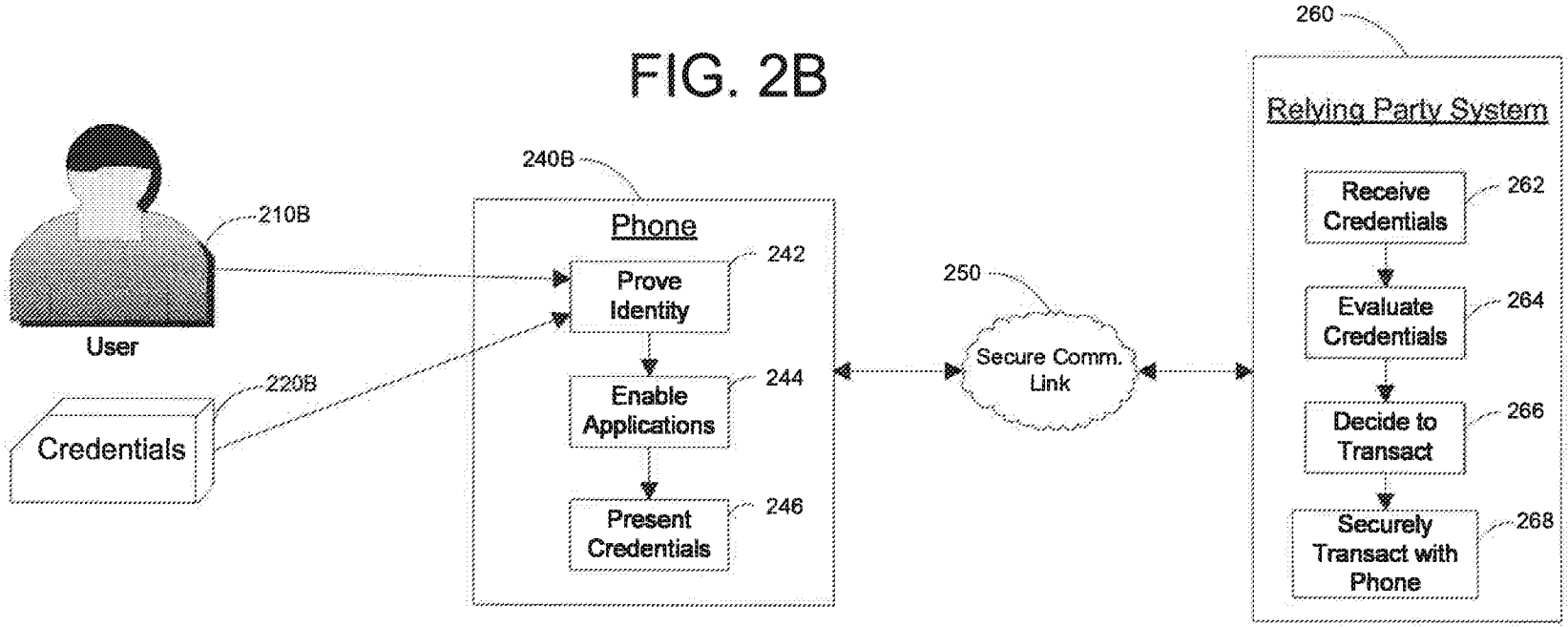
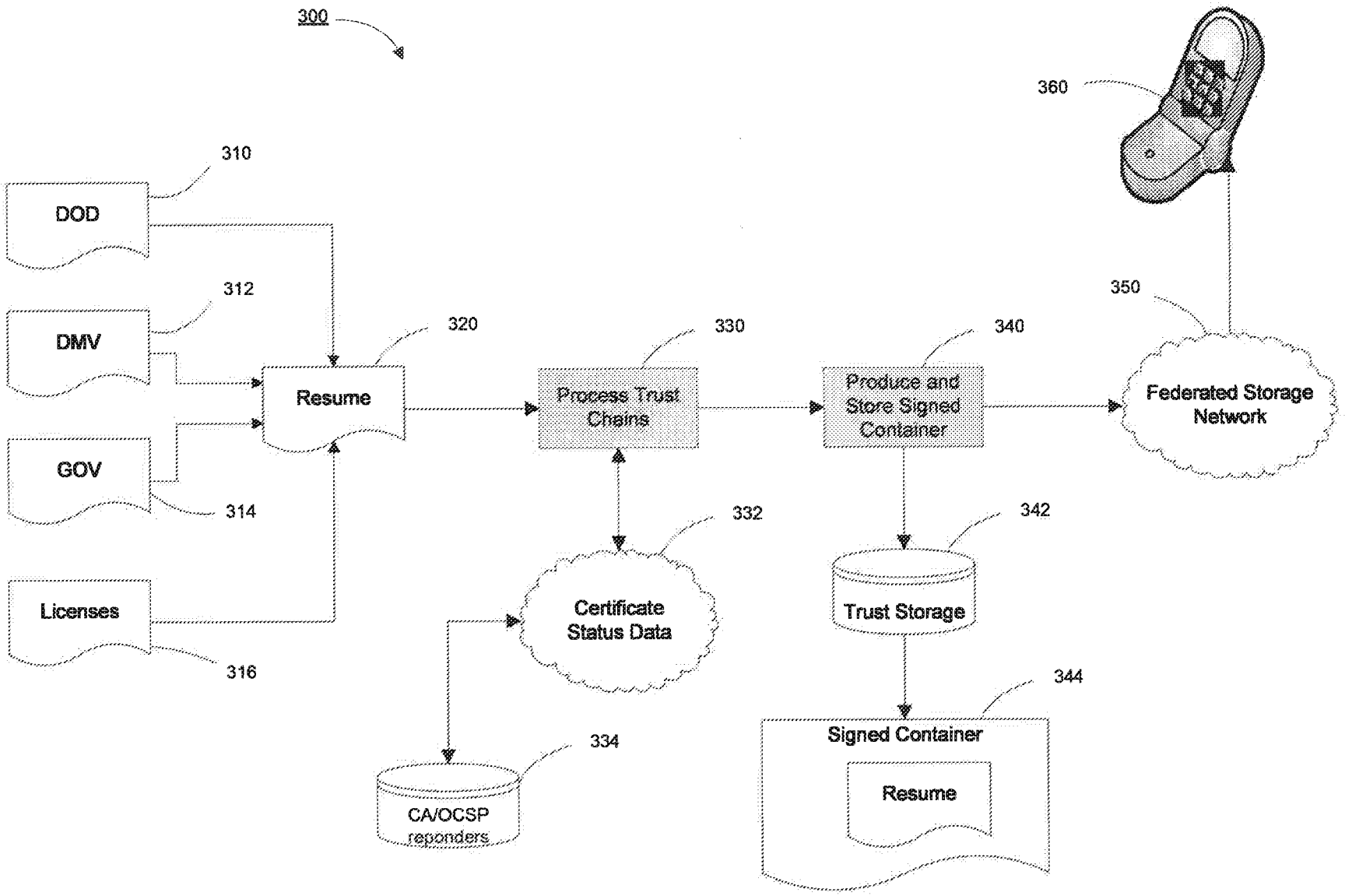


FIG. 2B



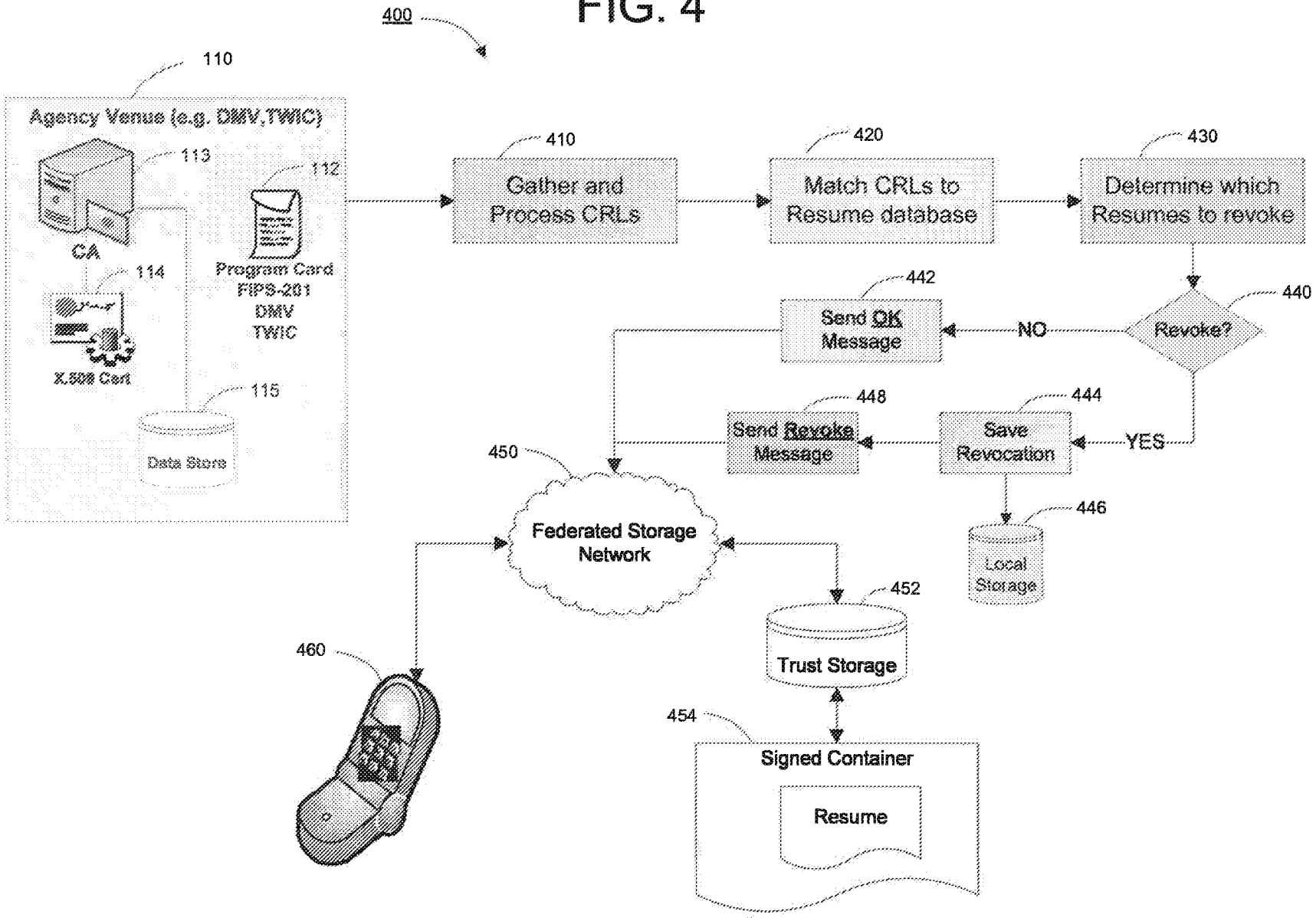
Petitioner Exhibit 1002-0875

FIG. 3



Petitioner Exhibit 1002-0876

FIG. 4



Petitioner Exhibit 1002-0877

FIG. 5 (Prior Art)

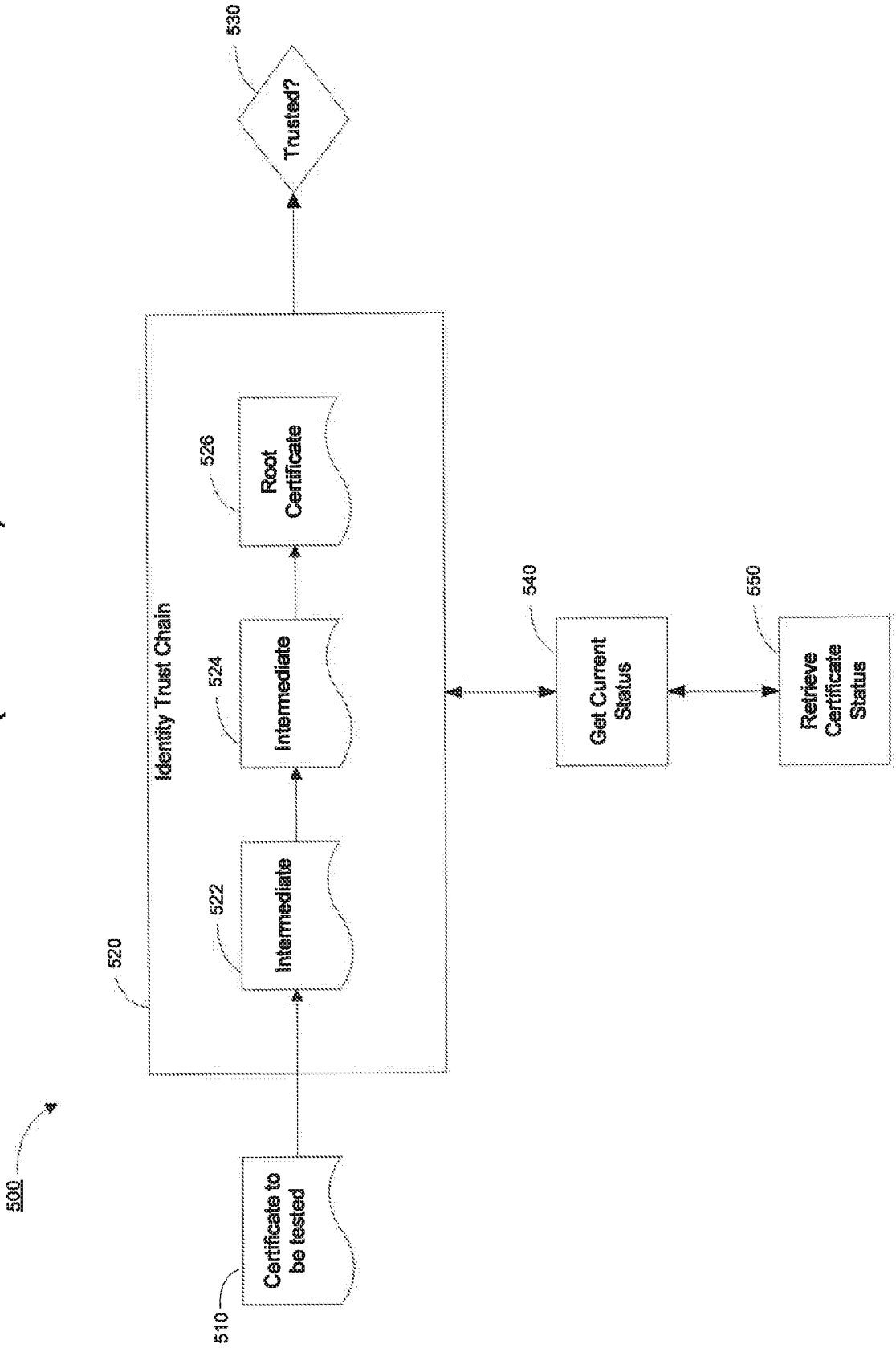


FIG. 6

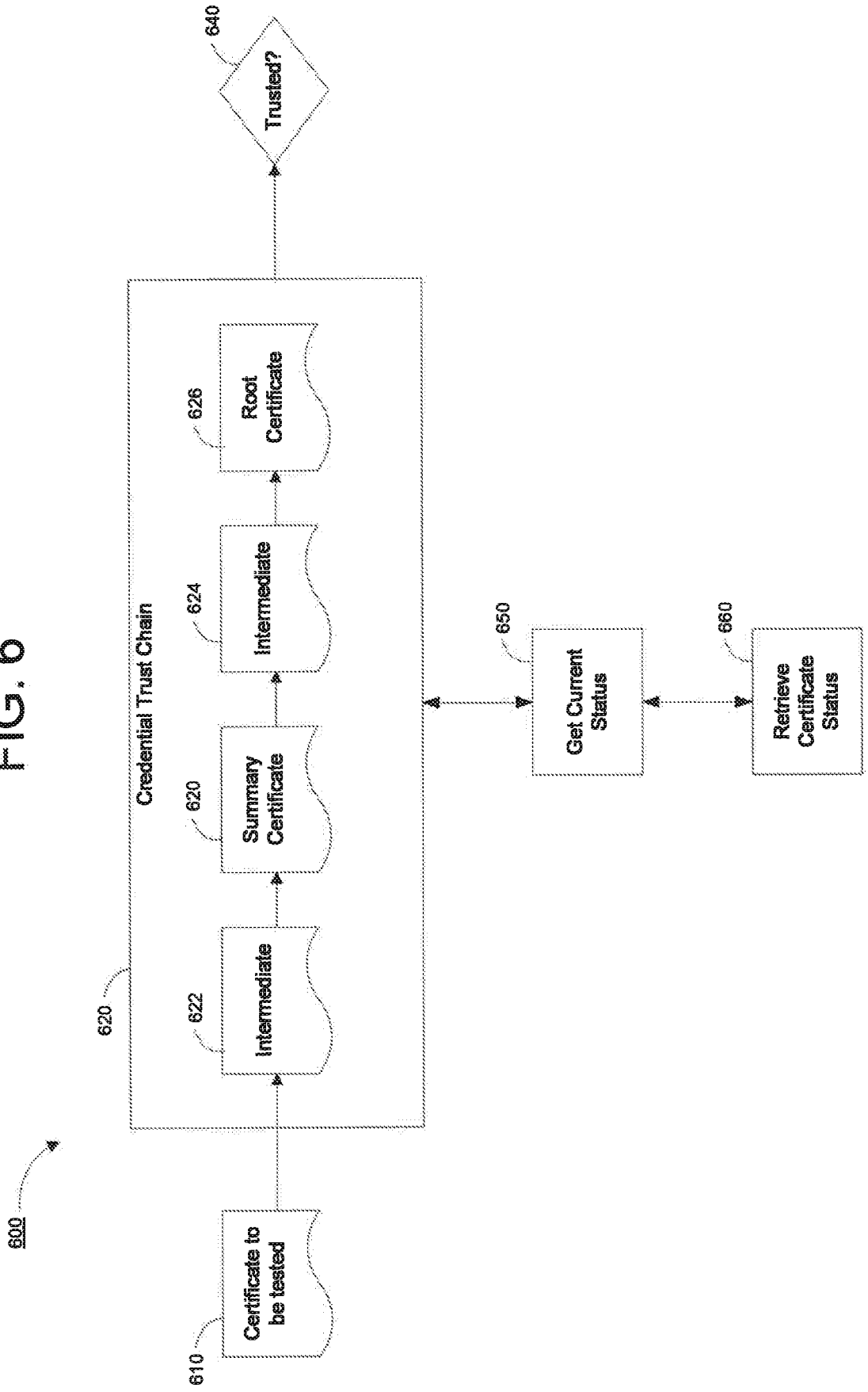

600
Certificate to be tested
610
Credential Trust Chain
620
Intermediate
622
Summary Certificate
620
Intermediate
624
Root Certificate
626
Trusted?
640
Get Current Status
650
Retrieve Certificate Status
660

FIG. 7

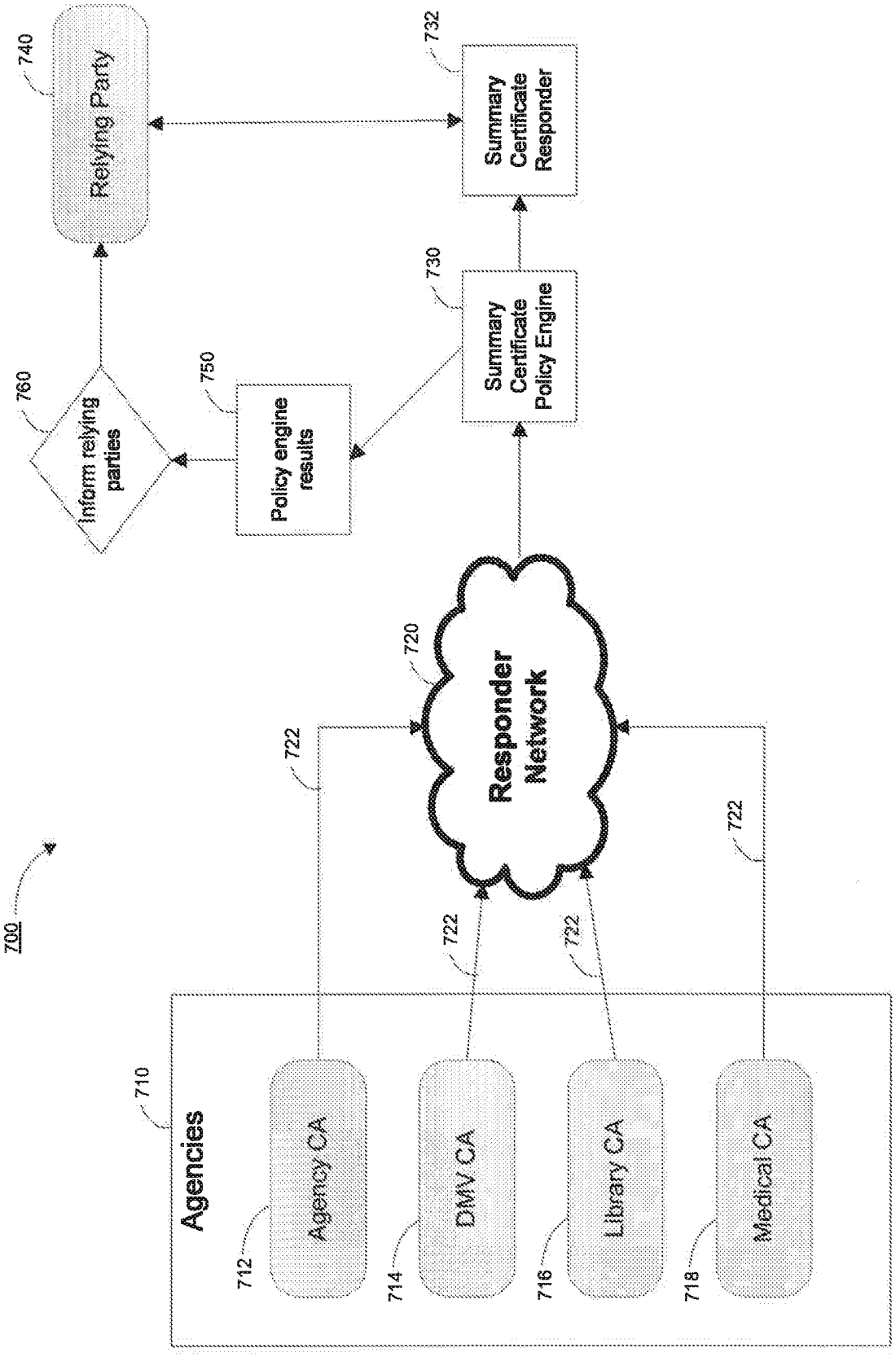
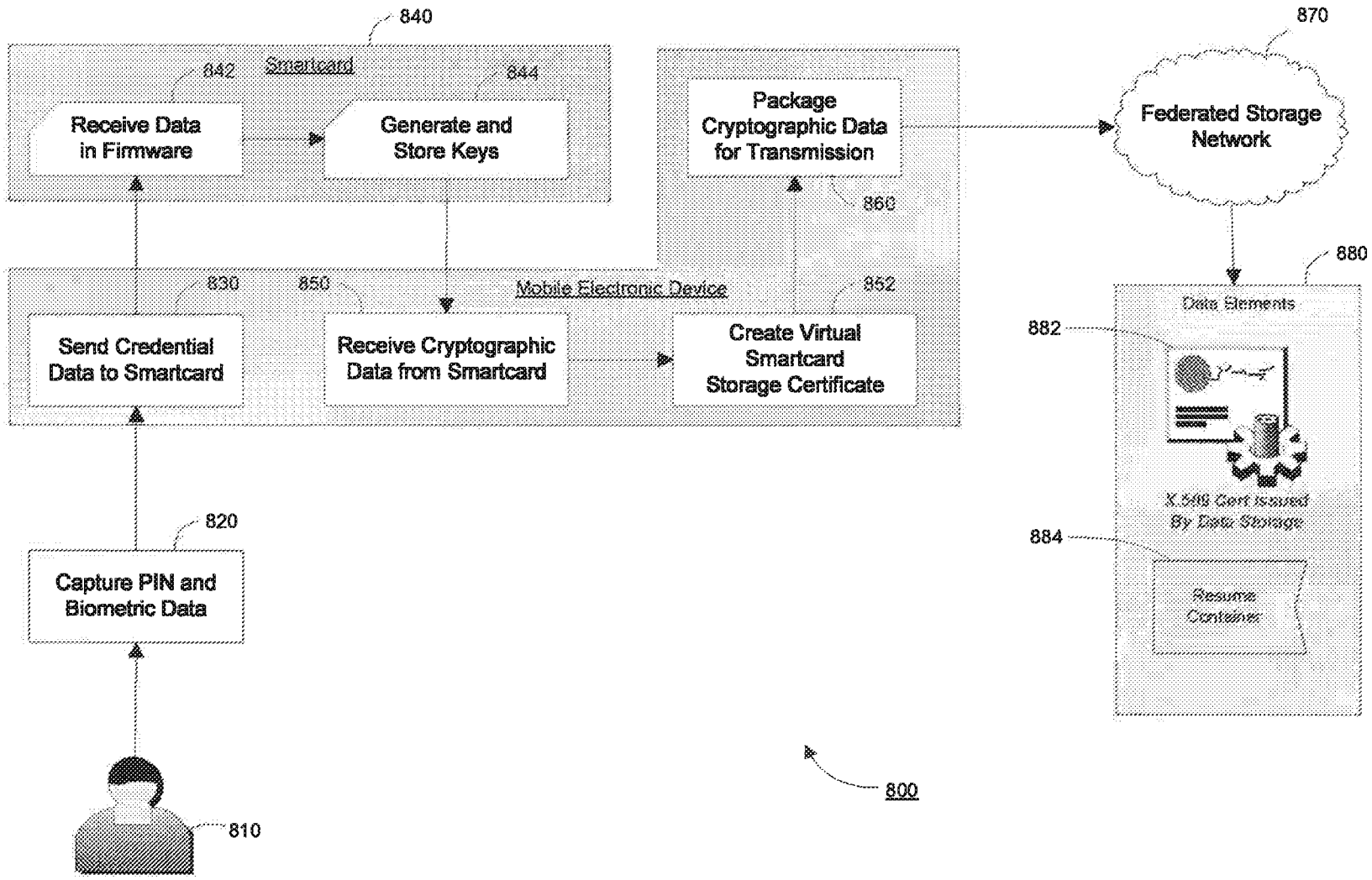

700
710
Agencies
712
Agency CA
714
DMV CA
716
Library CA
718
Medical CA
720
Responder Network
722
722
722
722
730
Summary Certificate Policy Engine
732
Summary Certificate Responder
740
Relying Party
750
Policy engine results
760
Inform relying parties

FIG. 8



Petitioner Exhibit 1002-0881

FIG. 9

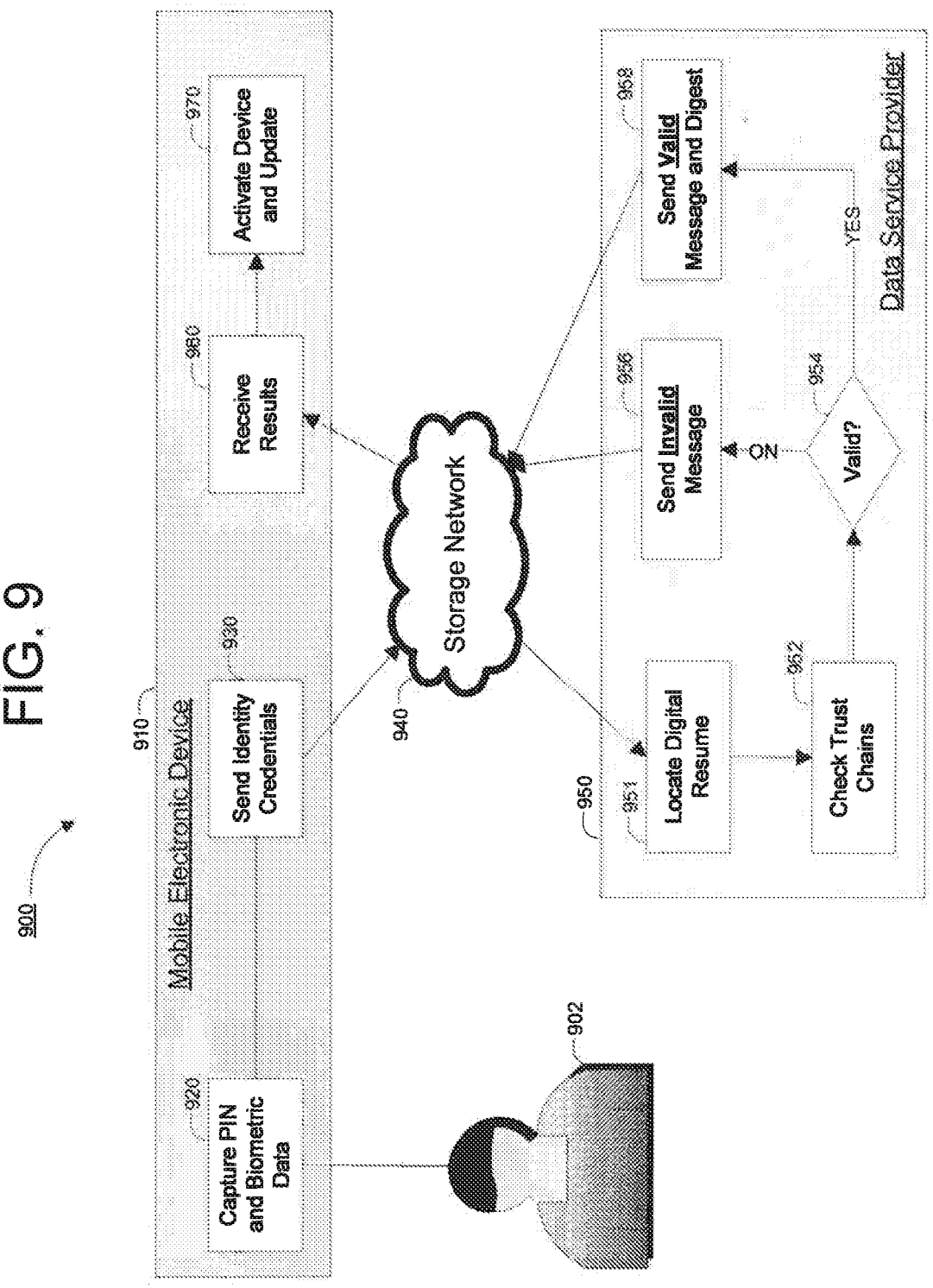
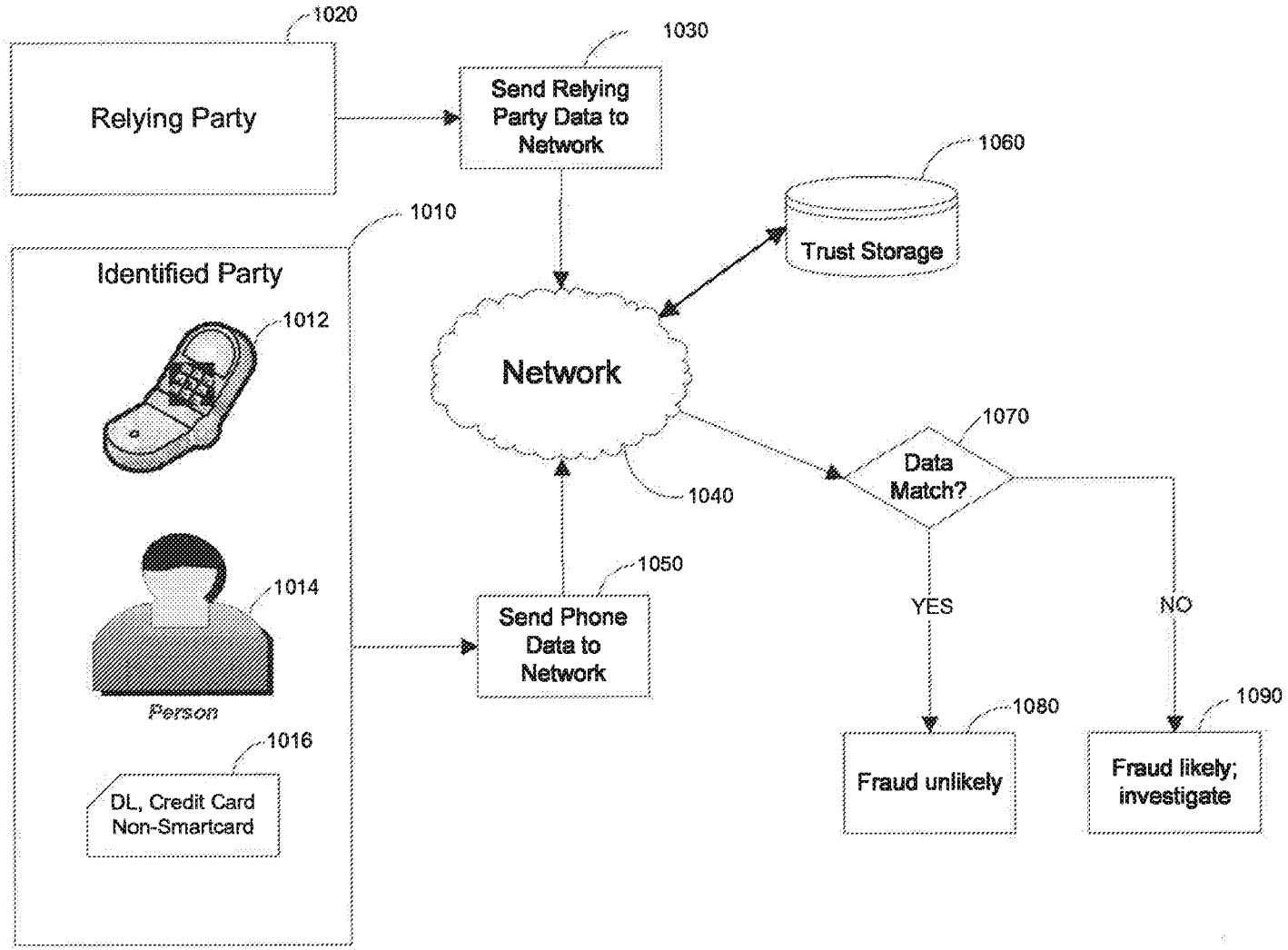
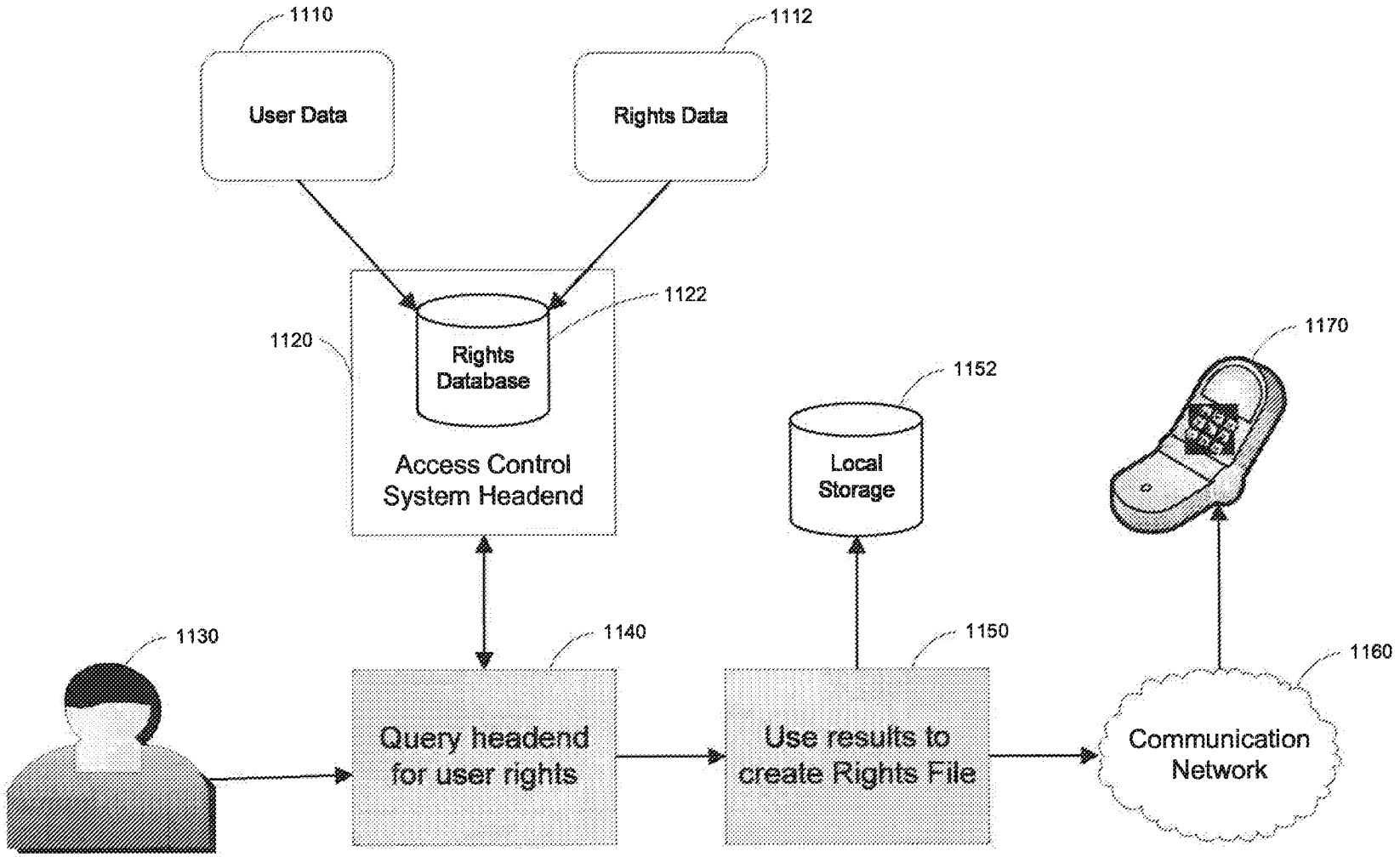

900
902
910
Mobile Electronic Device
920
Capture PIN and Biometric Data
930
Send Identity Credentials
940
Storage Network
950
Data Service Provider
951
Locate Digital Resume
952
Check Trust Chains
954
Valid?
YES
NO
956
Send Invalid Message
958
Send Valid Message and Digest
960
Receive Results
970
Activate Device and Update

FIG. 10



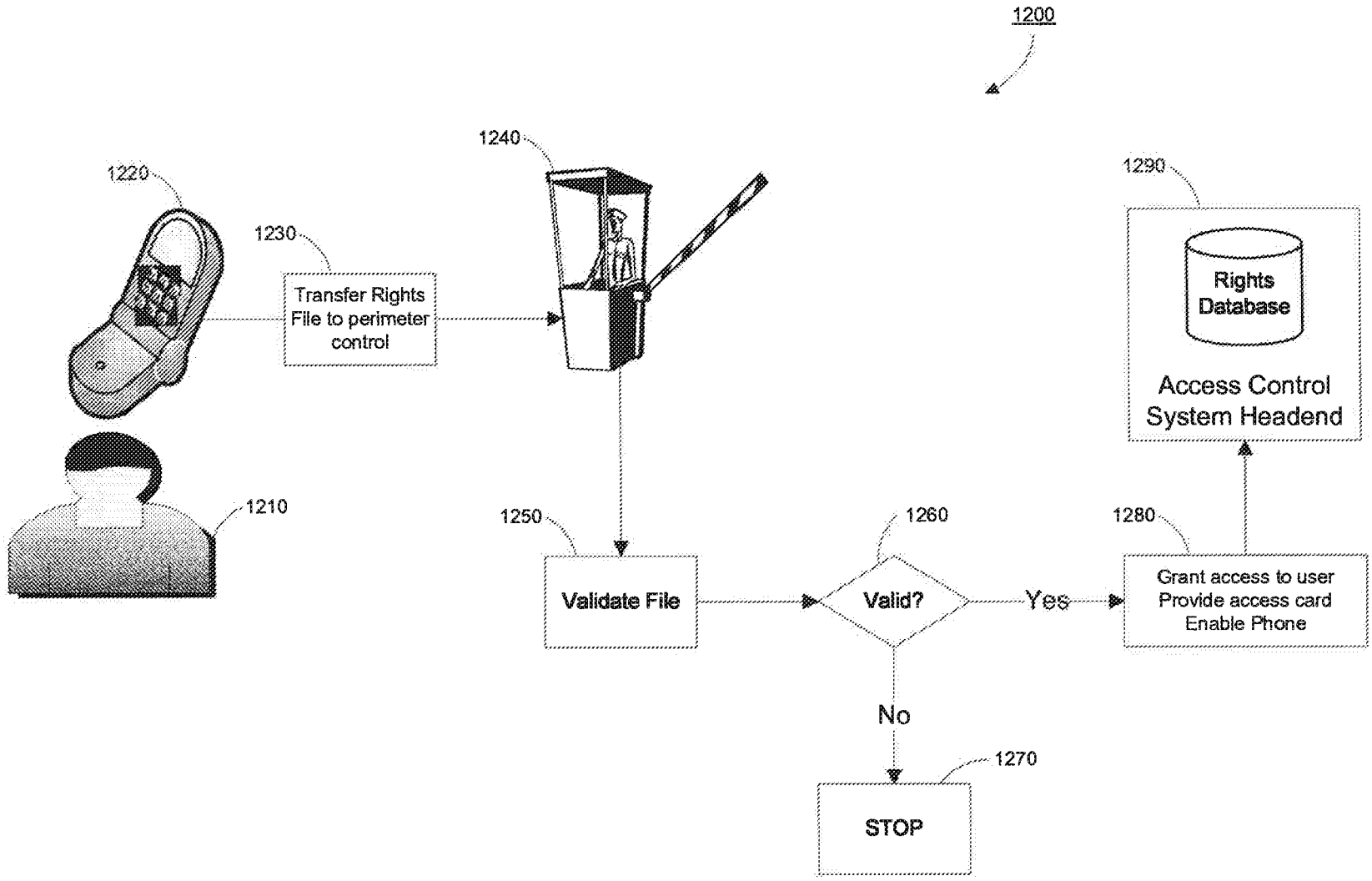
Petitioner Exhibit 1002-0883

FIG. 11



Petitioner Exhibit 1002-0884

FIG. 12



Petitioner Exhibit 1002-0885

FIG. 13

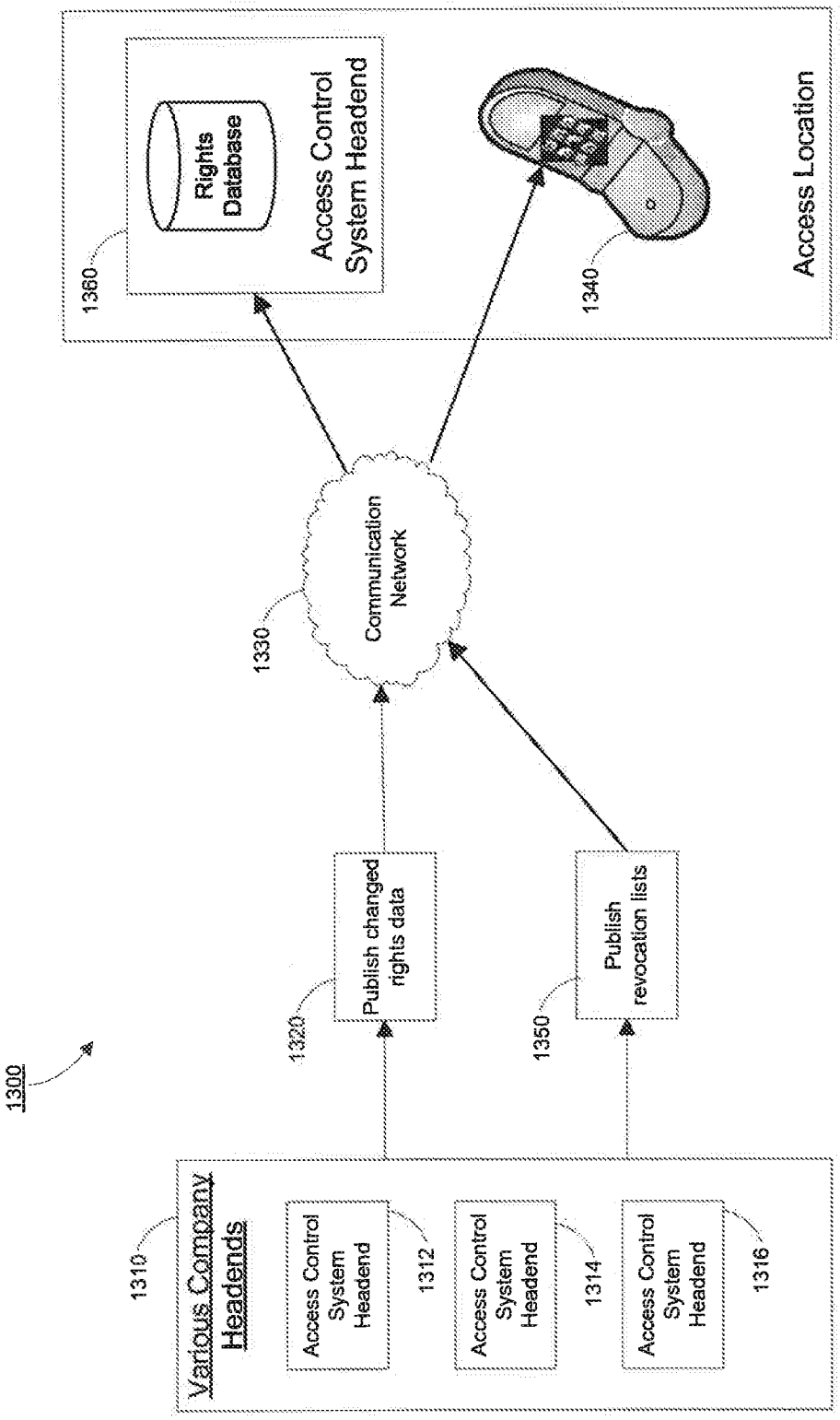
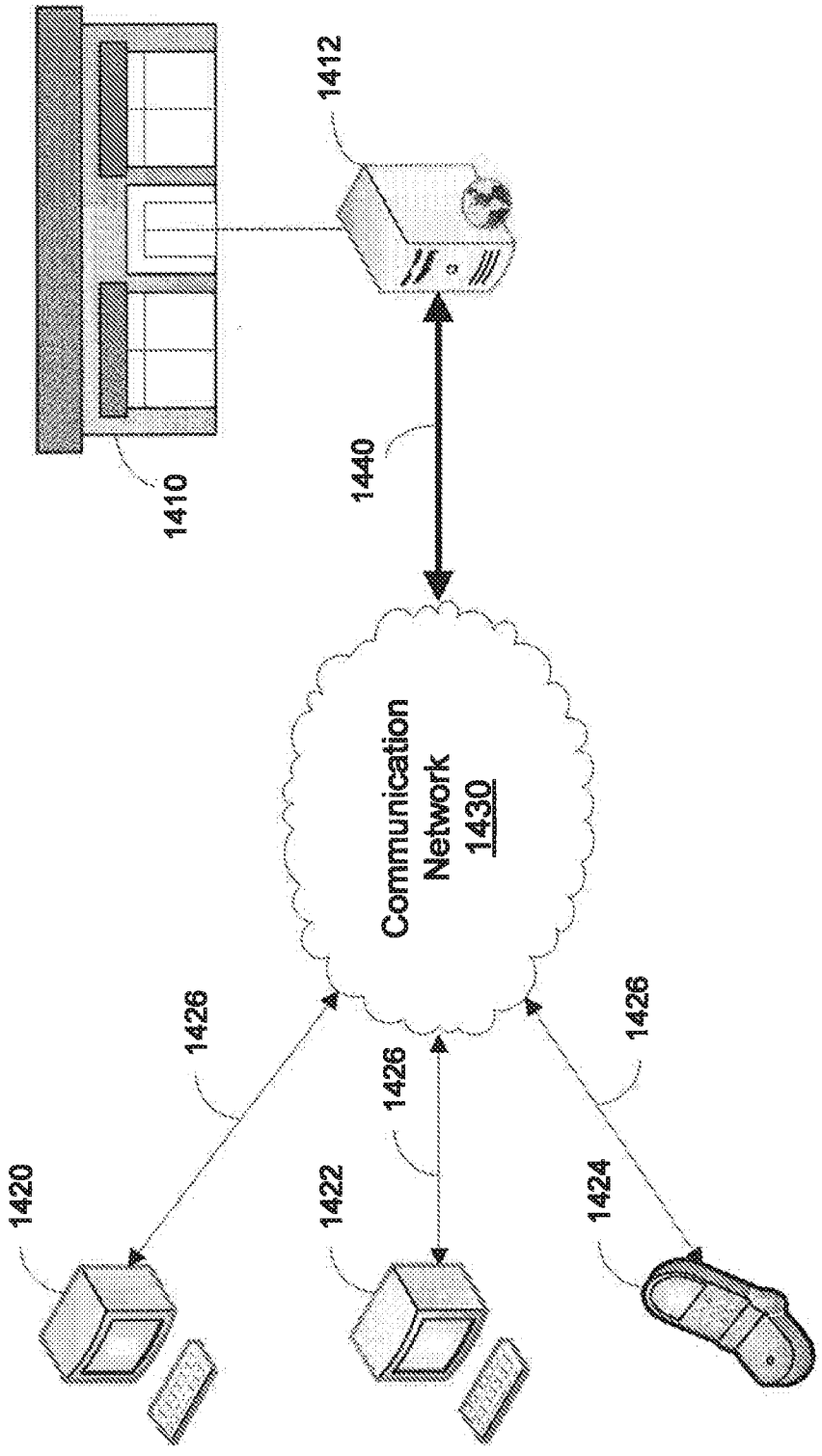

1300
Various Company Headends
1310
Access Control System Headend
1312
Access Control System Headend
1314
Access Control System Headend
1316
Publish changed rights data
1320
Publish revocation lists
1350
Communication Network
1330
Access Control System Headend
Rights Database
1360
1340
Access Location

FIG. 14 (Prior art)



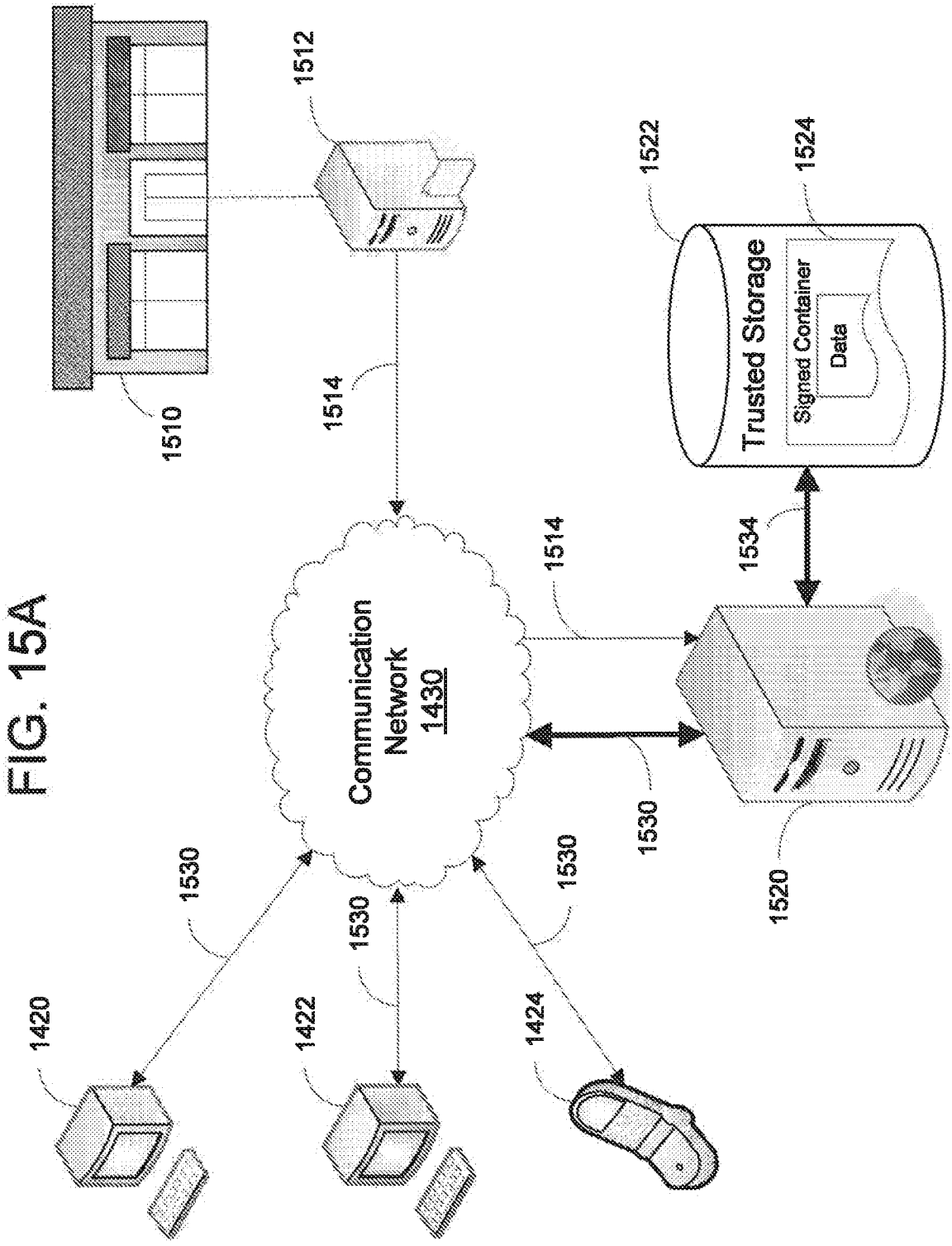

1512
1510
1514
1522
1524
Trusted Storage
Signed Container
Data
1534
1514
Communication Network 1430
1530
1520
1530
1530
1530
1420
1422
1424

FIG. 15A

FIG. 15B

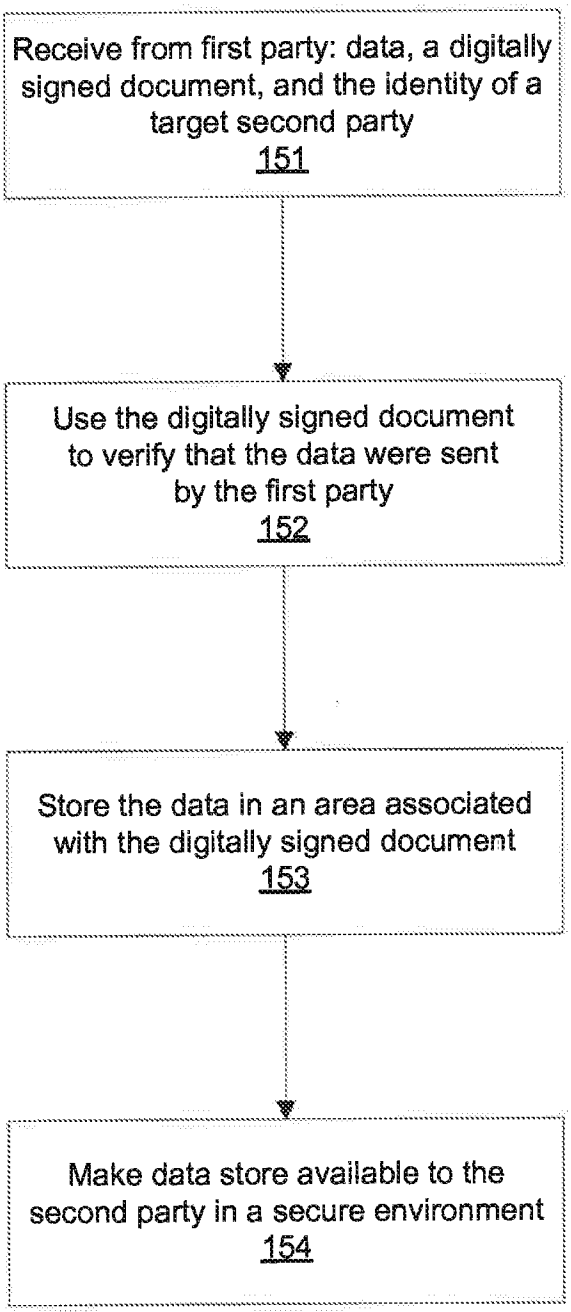
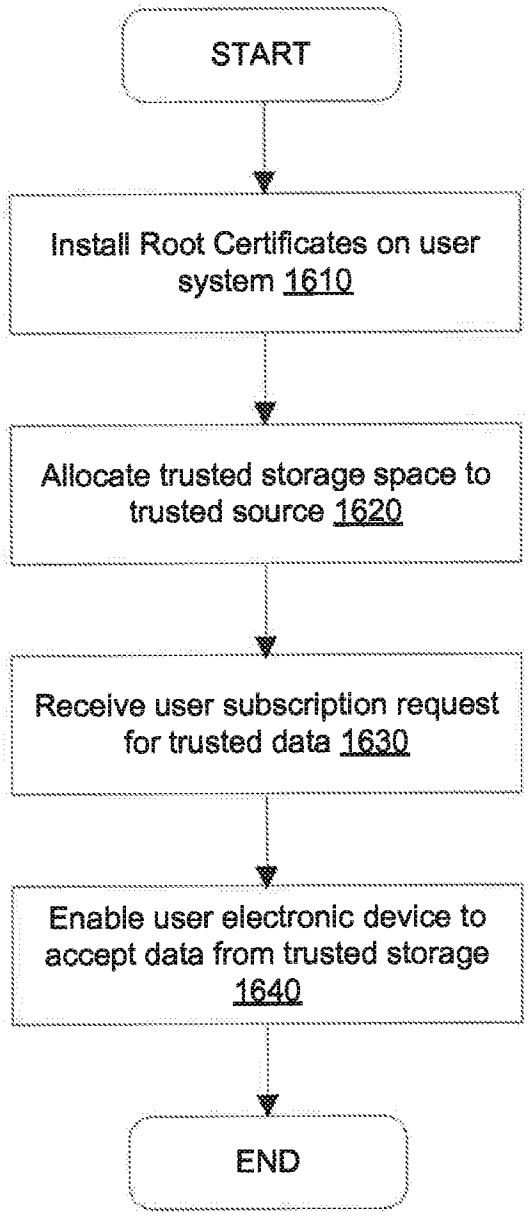
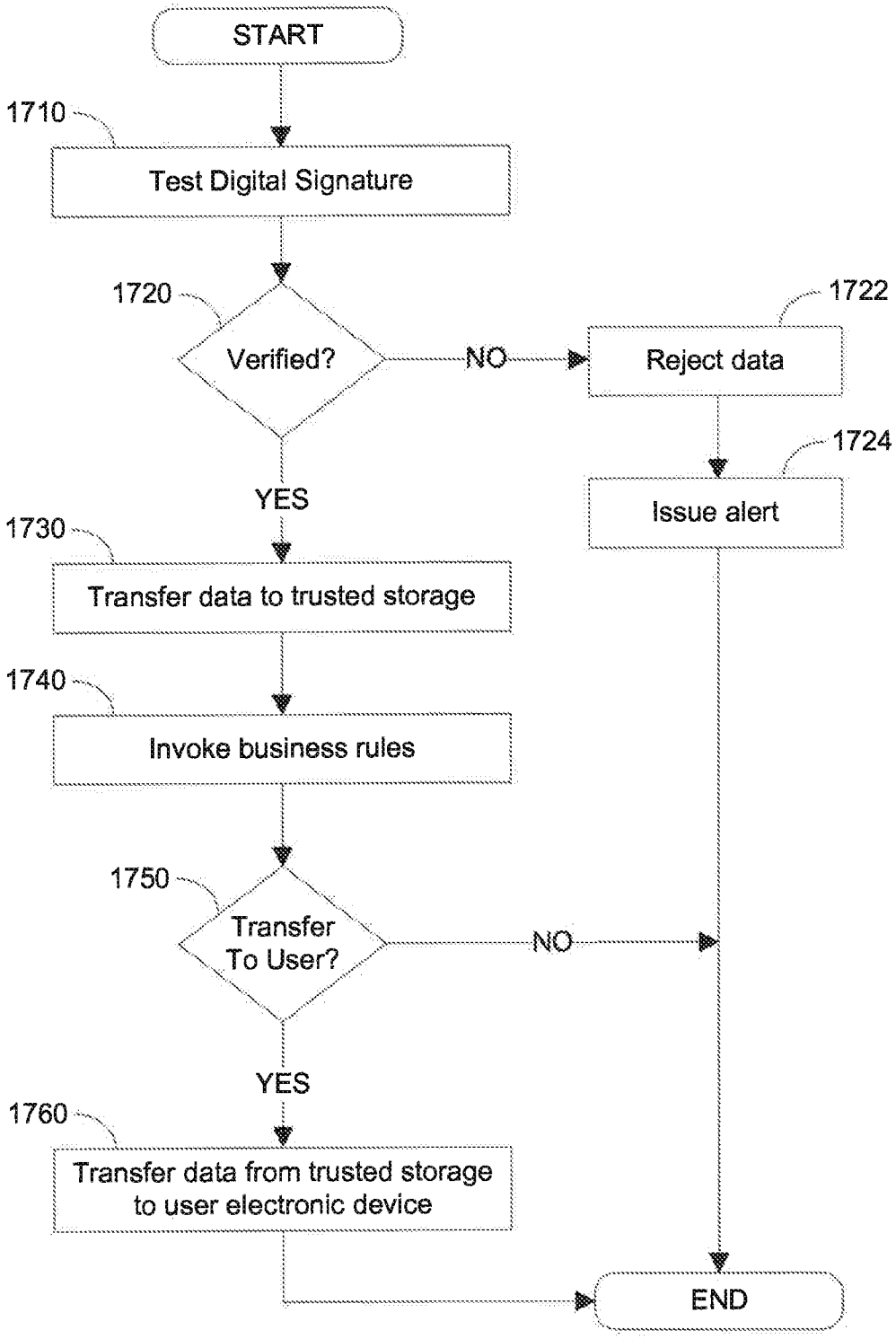

Receive from first party: data, a digitally signed document, and the identity of a target second party
151
Use the digitally signed document to verify that the data were sent by the first party
152
Store the data in an area associated with the digitally signed document
153
Make data store available to the second party in a secure environment
154

FIG. 16



Petitioner Exhibit 1002-0890

FIG. 17



Petitioner Exhibit 1002-0891

FIG. 18A (P1)

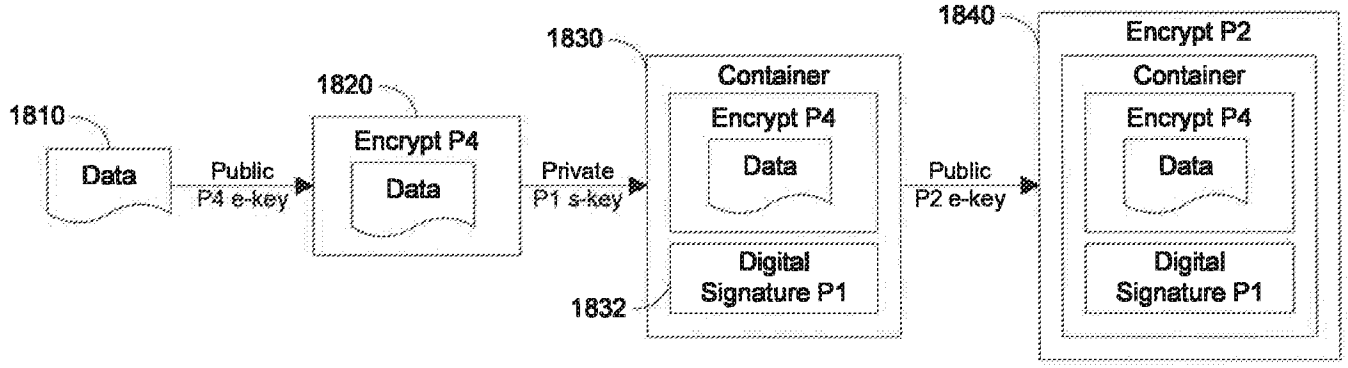
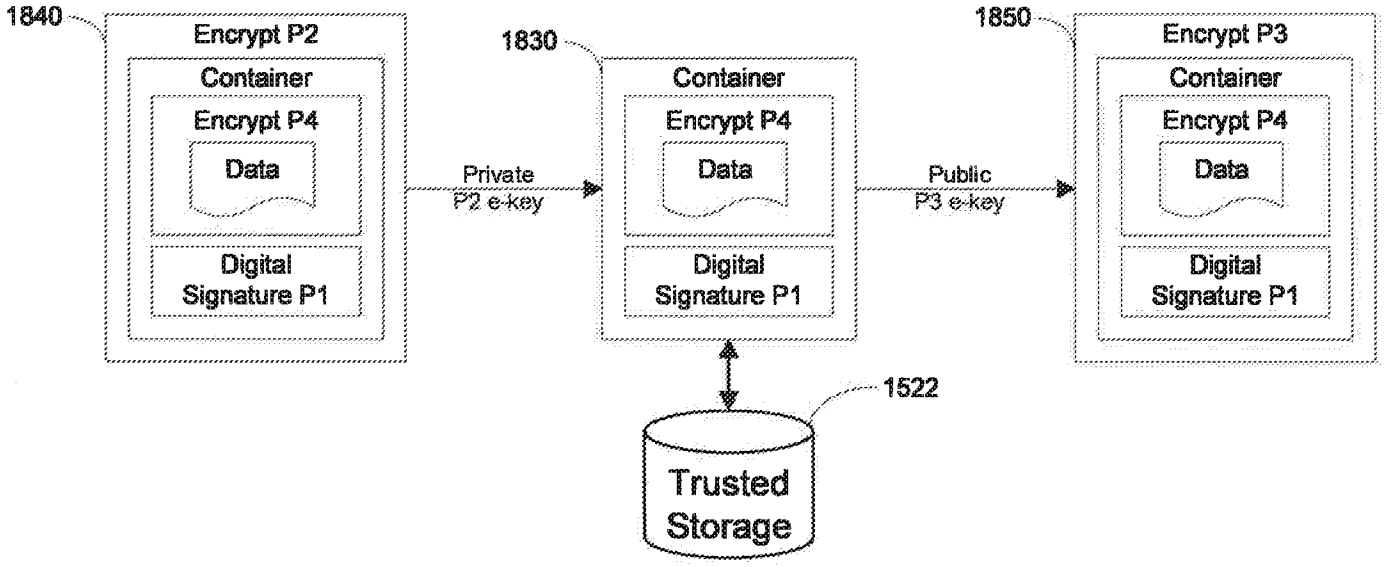


FIG. 18B (P2)



Petitioner Exhibit 1002-0892

FIG. 18C (P3)

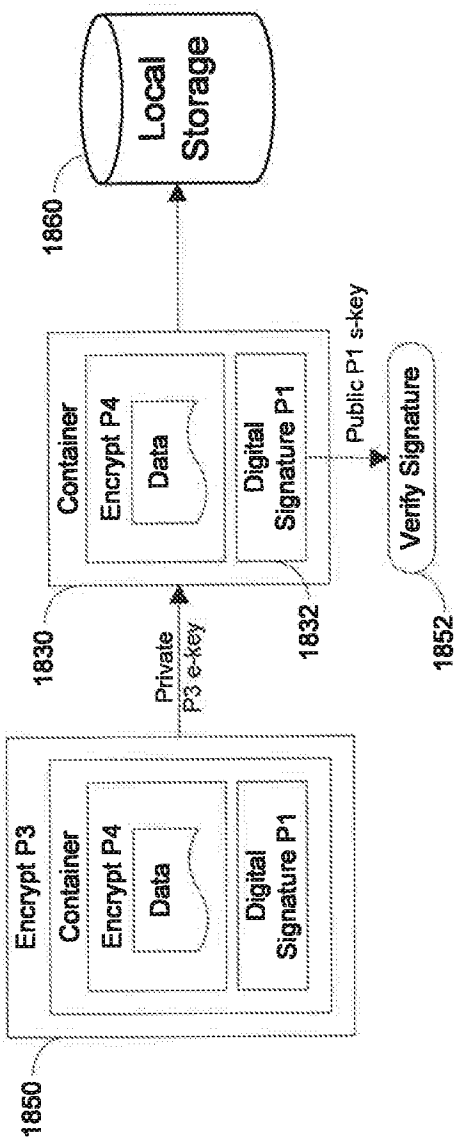


FIG. 18D (P4)

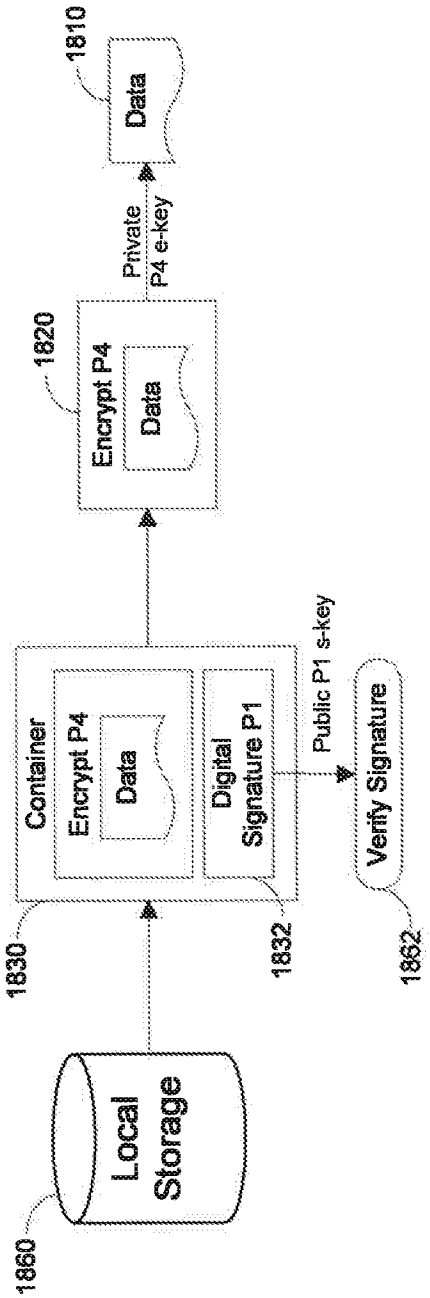
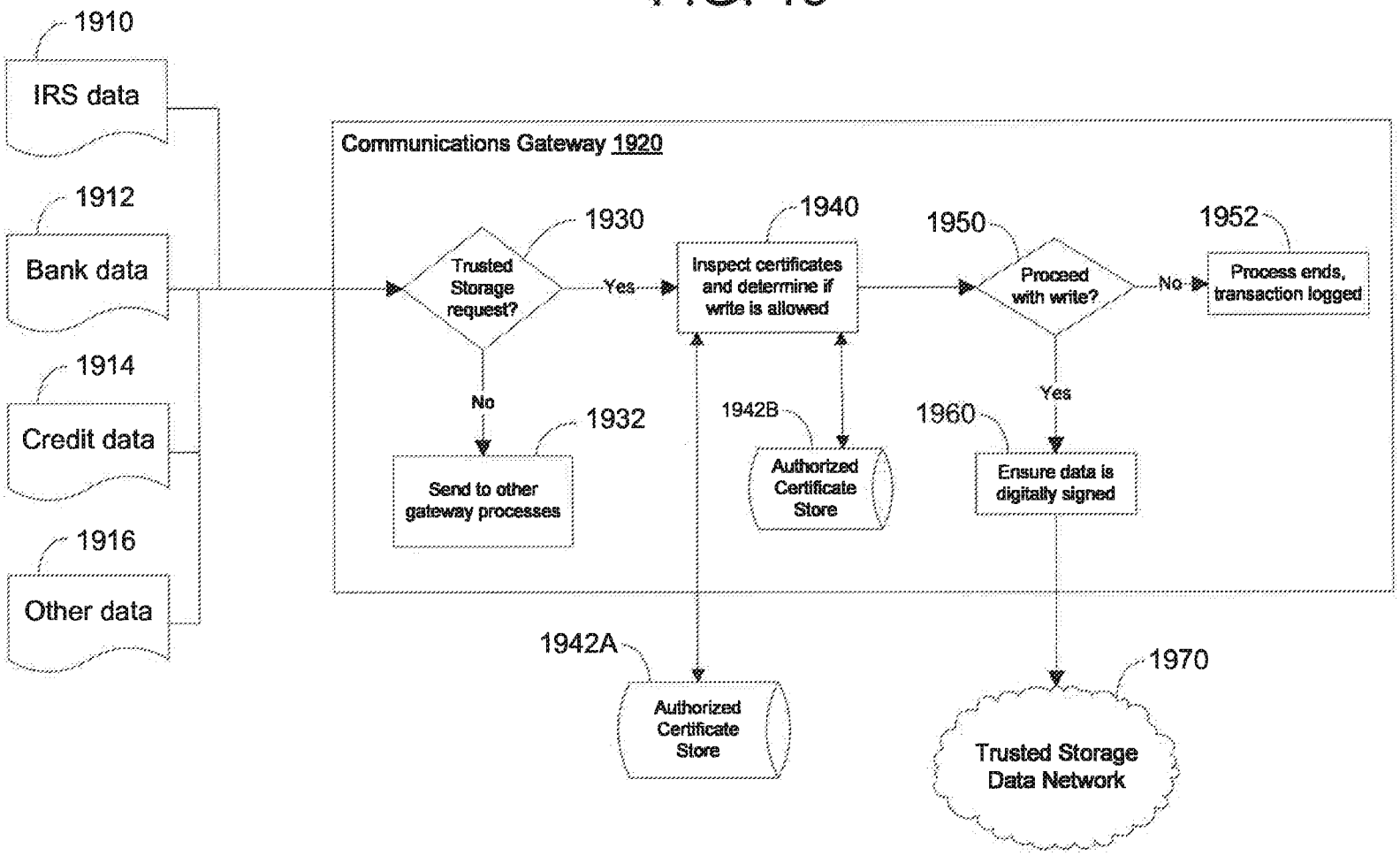


FIG. 19



Petitioner Exhibit 1002-0894

FIG. 20

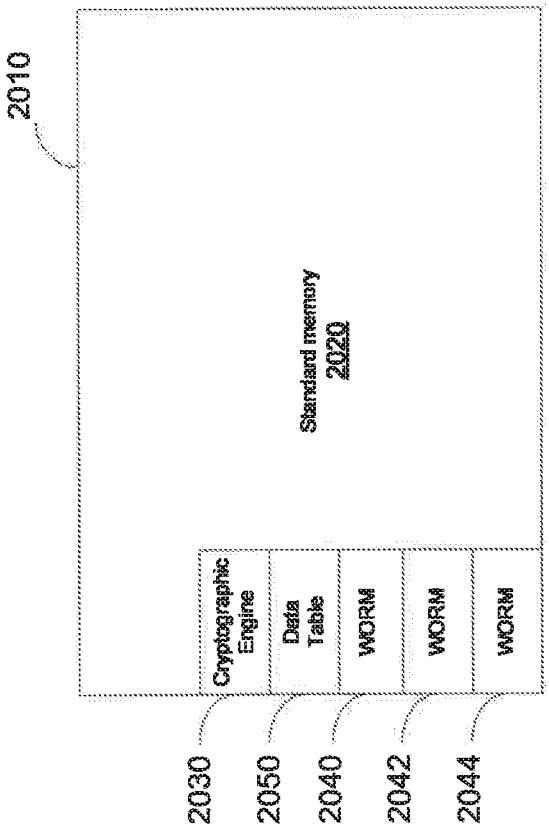

2010
Standard memory
2020
Cryptographic Engine
Data Table
WORM
WORM
WORM
2030
2050
2040
2042
2044

FIG. 21

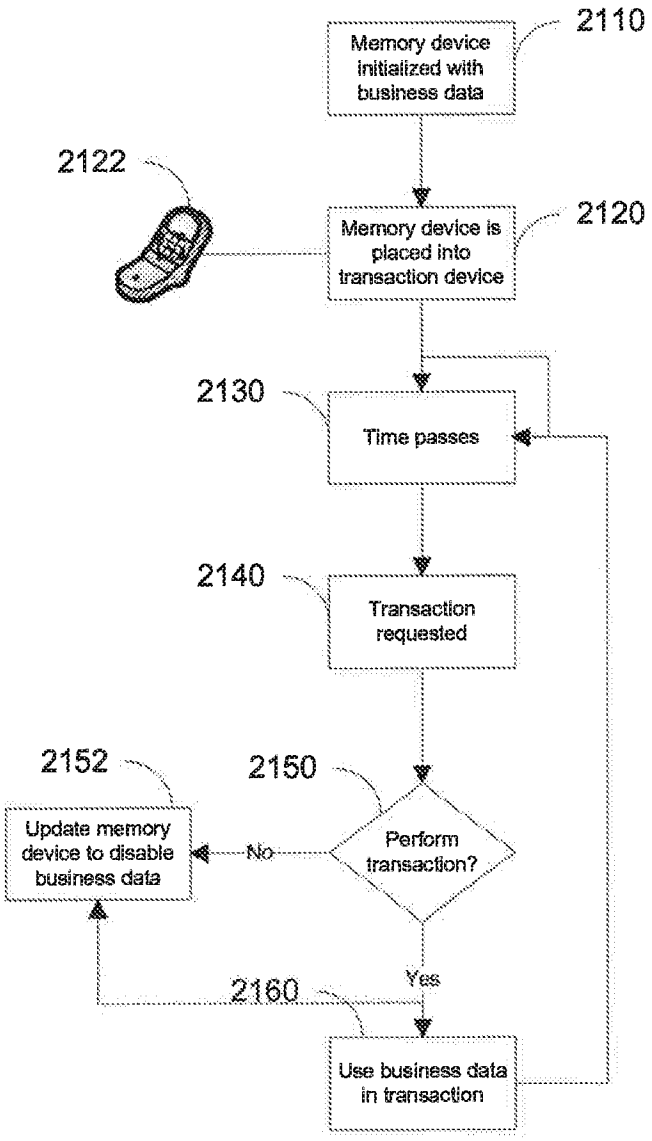

2110
Memory device initialized with business data
2122
2120
Memory device is placed into transaction device
2130
Time passes
2140
Transaction requested
2152
2150
Update memory device to disable business data
No
Perform transaction?
Yes
2160
Use business data in transaction

FIG. 22

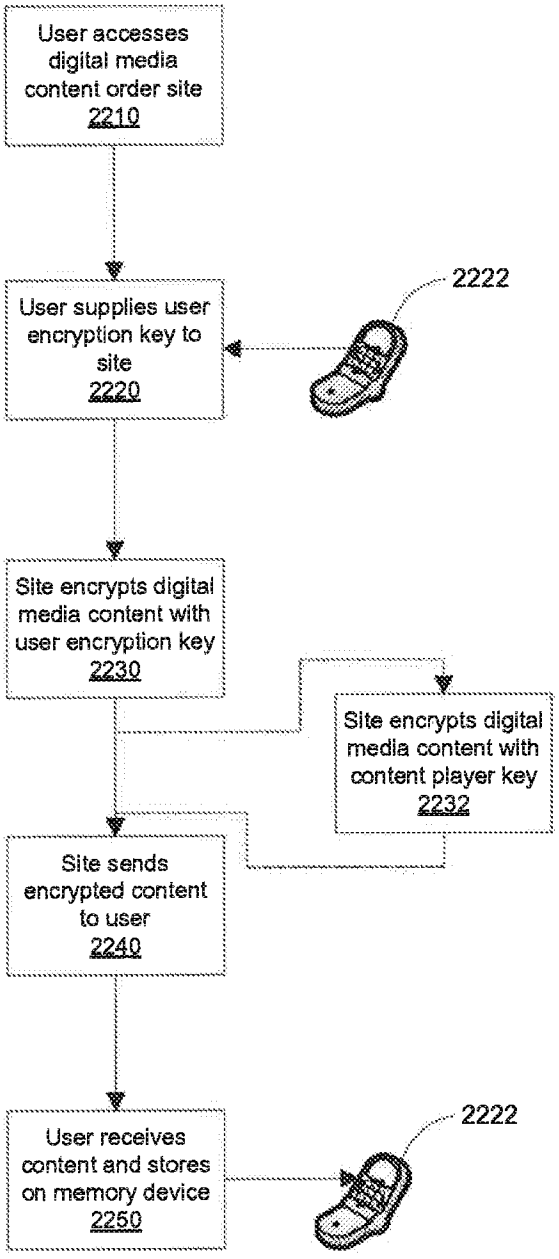
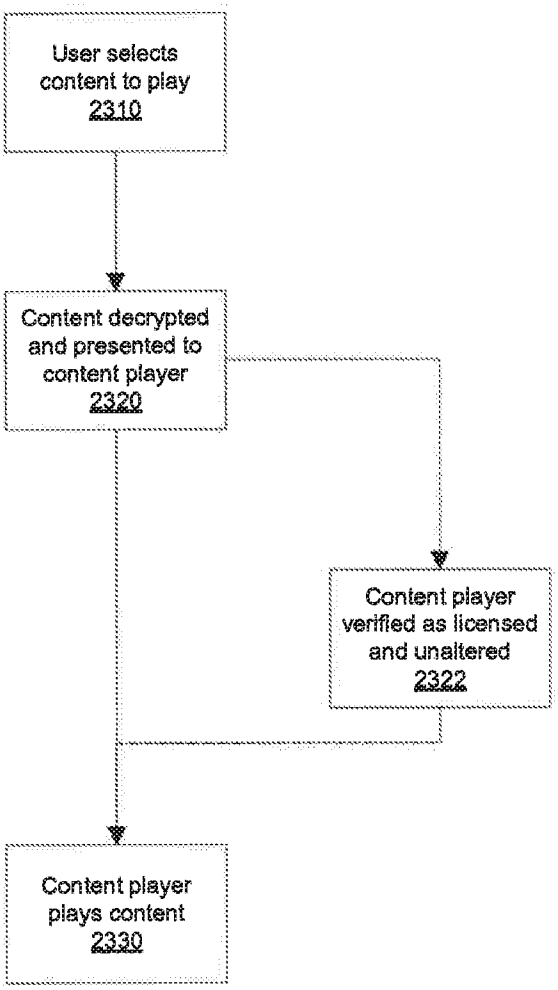
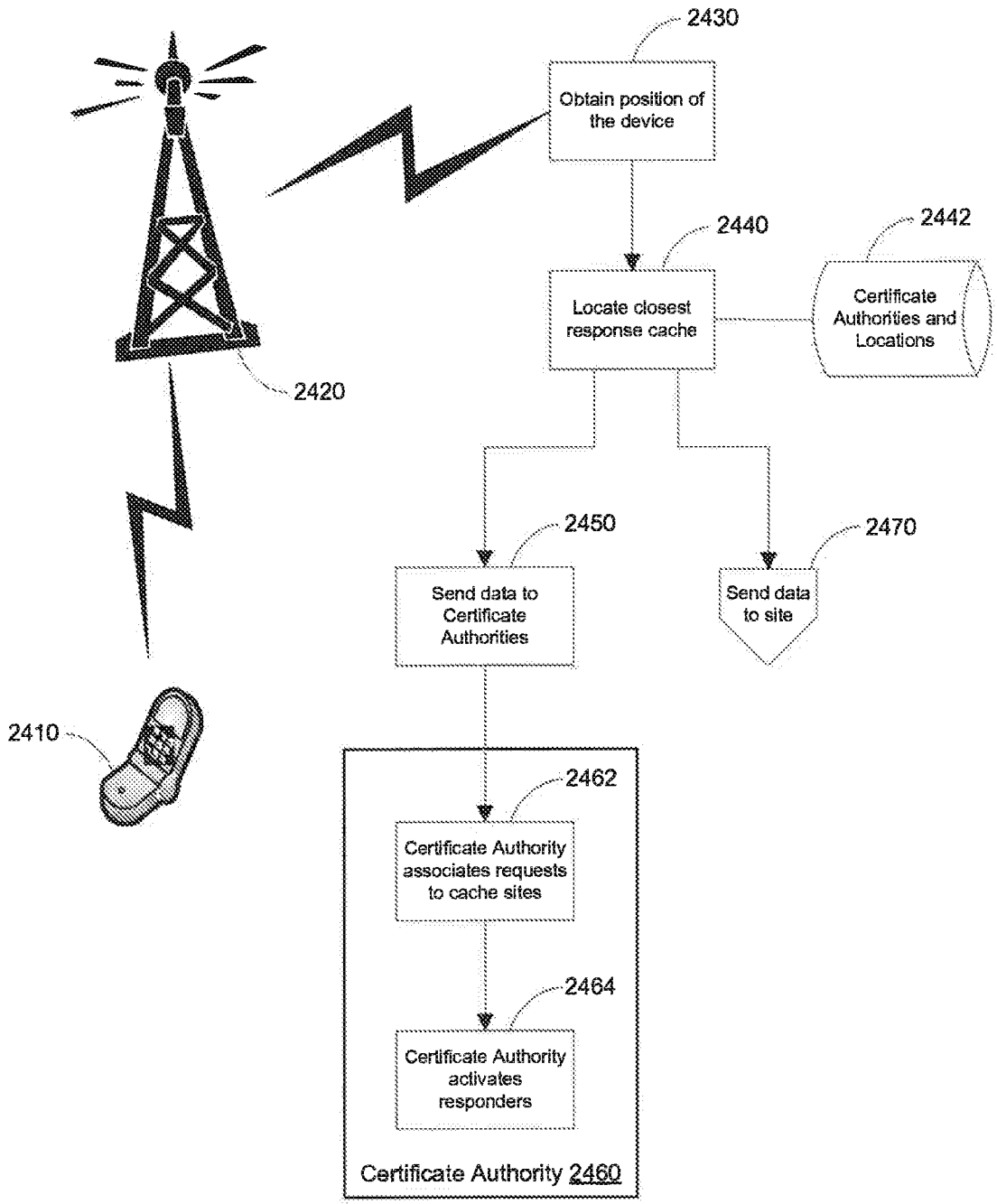

User accesses digital media content order site 2210
User supplies user encryption key to site 2220
2222
Site encrypts digital media content with user encryption key 2230
Site encrypts digital media content with content player key 2232
Site sends encrypted content to user 2240
User receives content and stores on memory device 2250
2222

FIG. 23



Petitioner Exhibit 1002-0898

FIG. 24


2430
Obtain position of the device
2440
Locate closest response cache
2442
Certificate Authorities and Locations
2420
2450
Send data to Certificate Authorities
2470
Send data to site
2410
2462
Certificate Authority associates requests to cache sites
2464
Certificate Authority activates responders
Certificate Authority 2460

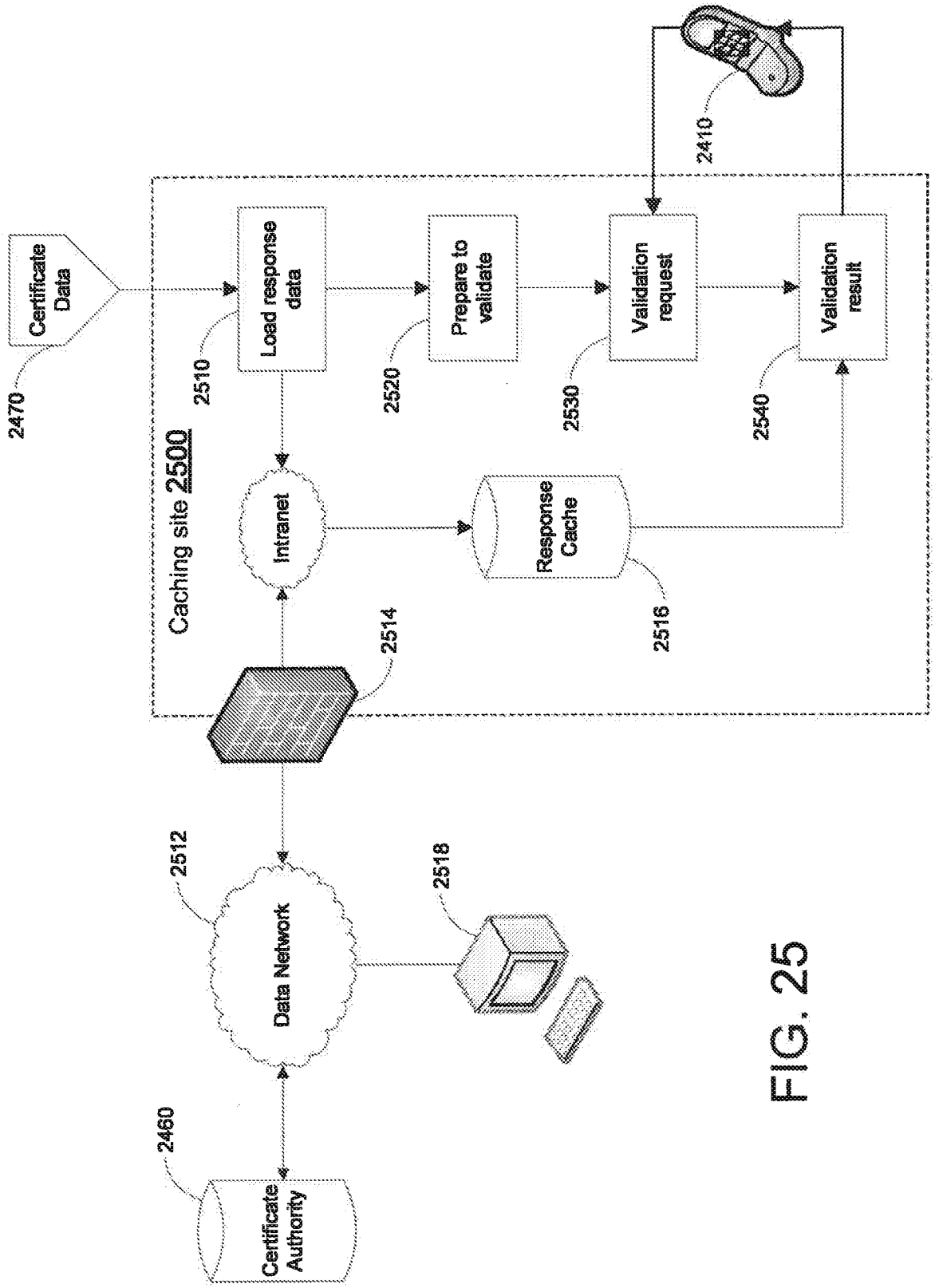

Certificate Data
2470
Caching site 2500
2510
Load response data
2520
Prepare to validate
2530
Validation request
2540
Validation result
2410
Intranet
Response Cache
2516
2514
2512
Data Network
2518
2460
Certificate Authority

FIG. 25

FIG. 26

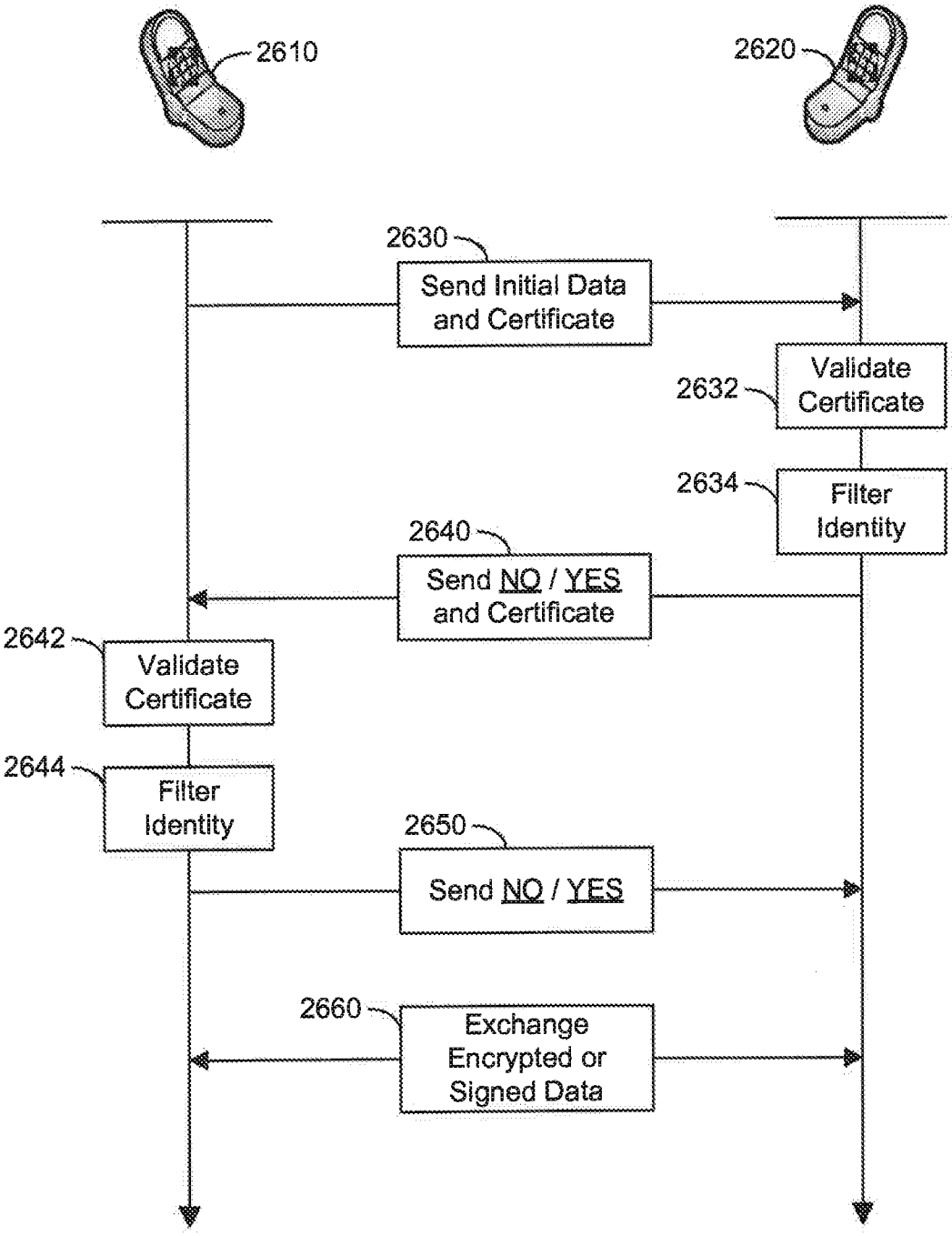

2610
2620
2630
Send Initial Data and Certificate
2632
Validate Certificate
2634
Filter Identity
2640
Send NO / YES and Certificate
2642
Validate Certificate
2644
Filter Identity
2650
Send NO / YES
2660
Exchange Encrypted or Signed Data

FIG. 27

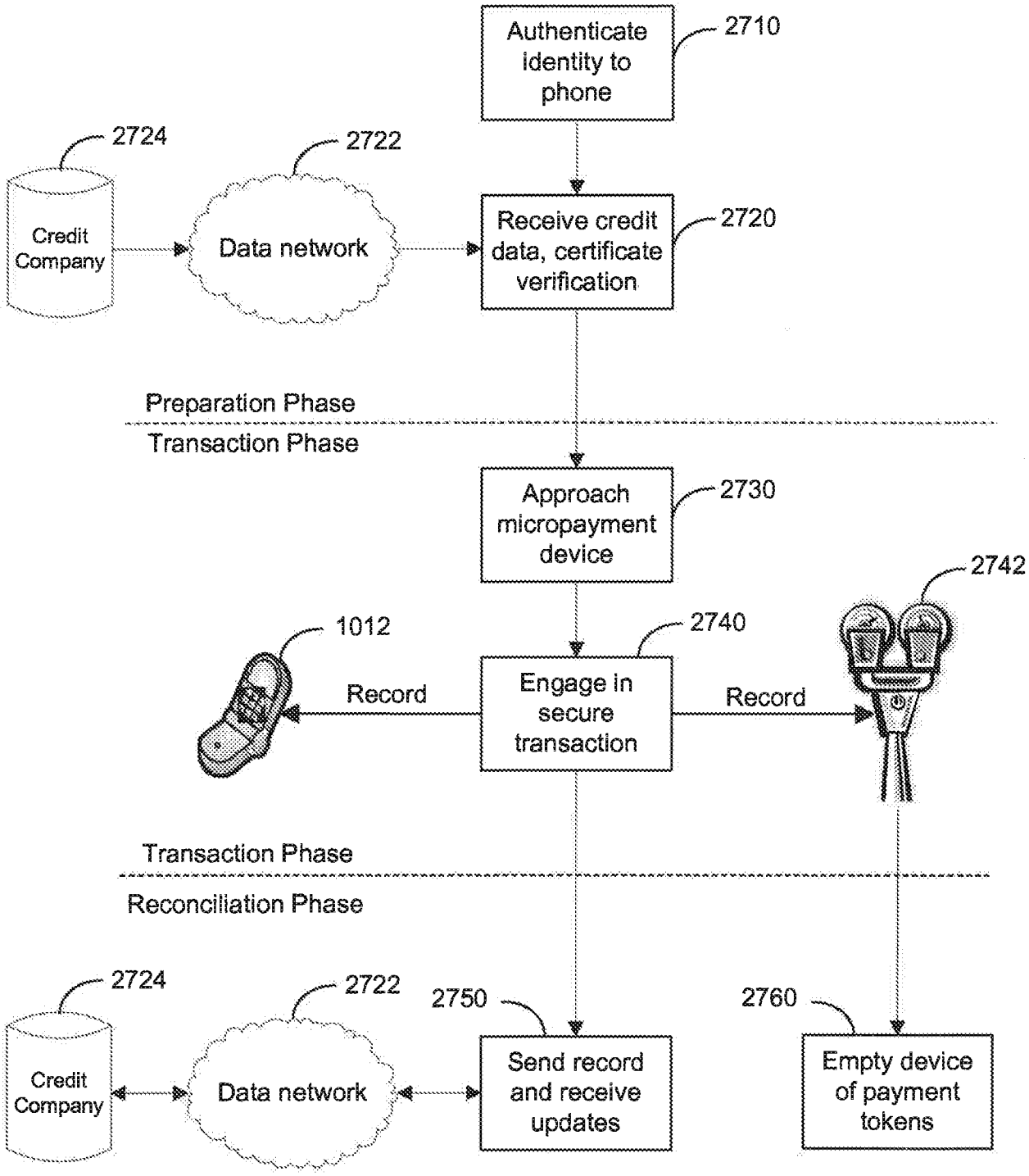

Authenticate identity to phone
2710
2724
2722
Credit Company
Data network
Receive credit data, certificate verification
2720
Preparation Phase
Transaction Phase
Approach micropayment device
2730
2742
1012
2740
Record
Engage in secure transaction
Record
Transaction Phase
Reconciliation Phase
2724
2722
2750
2760
Credit Company
Data network
Send record and receive updates
Empty device of payment tokens

FIG. 28

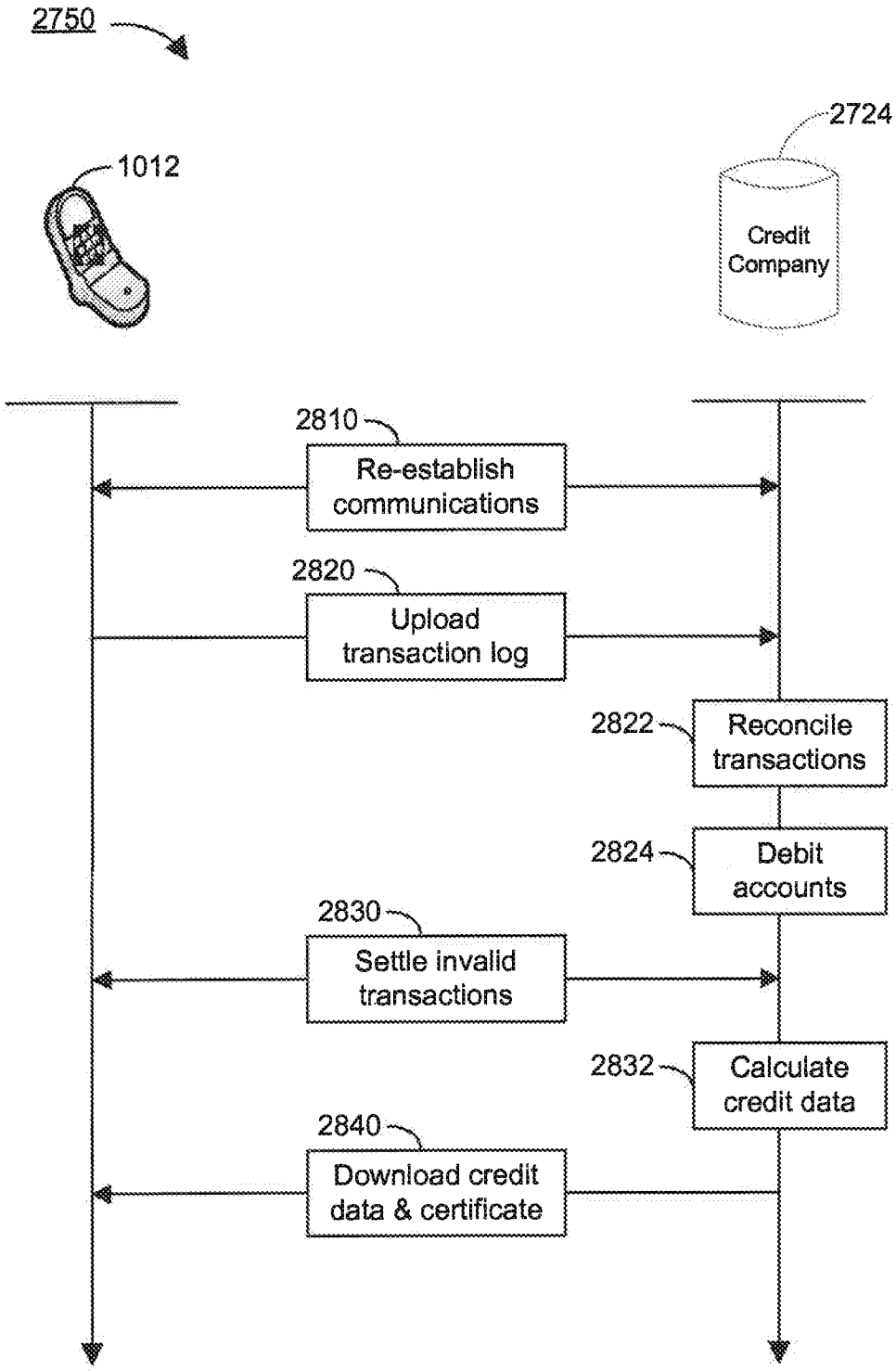

2750
2724
1012
Credit Company
2810
Re-establish communications
2820
Upload transaction log
2822
Reconcile transactions
2824
Debit accounts
2830
Settle invalid transactions
2832
Calculate credit data
2840
Download credit data & certificate

FIG. 29

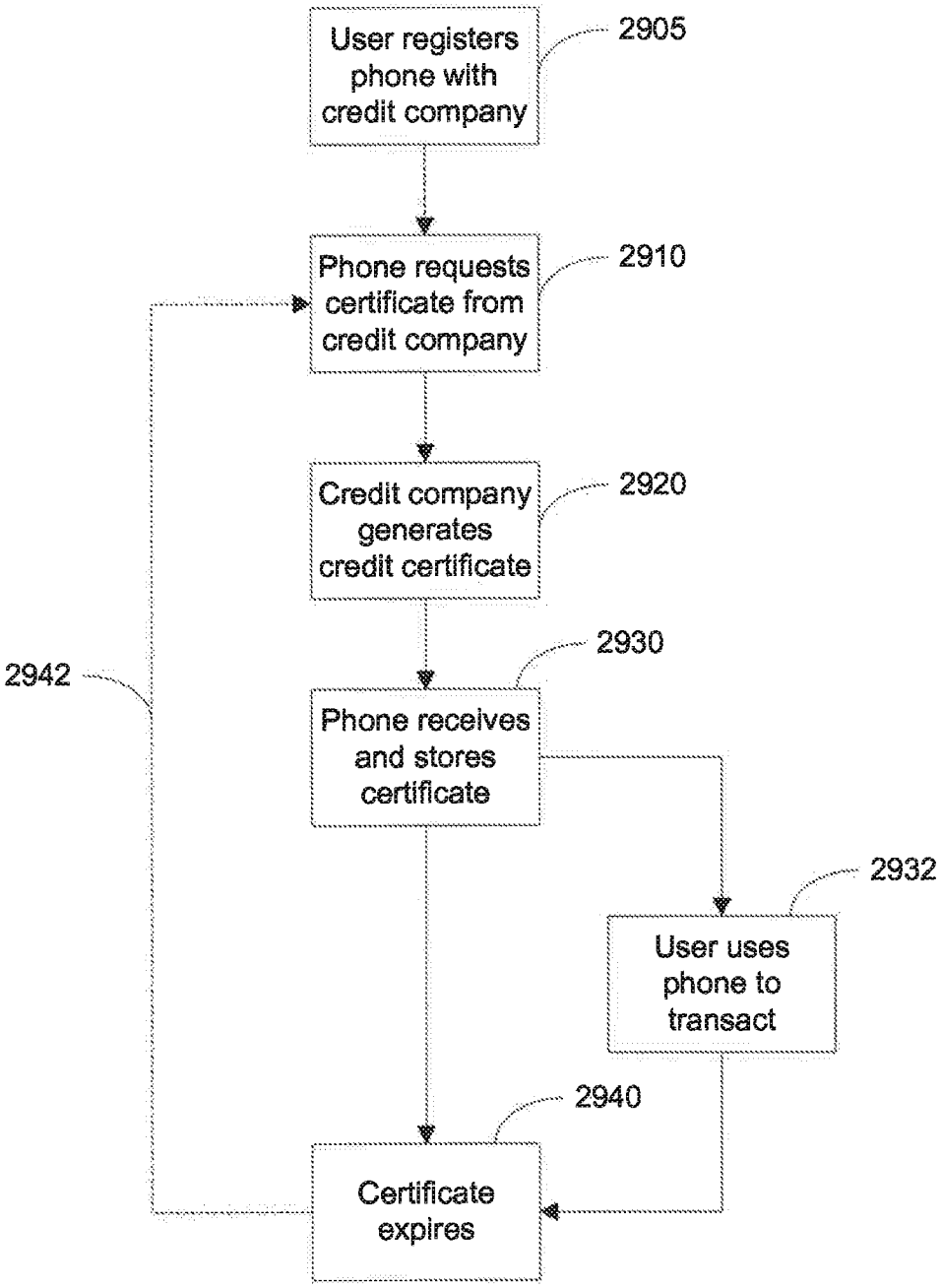
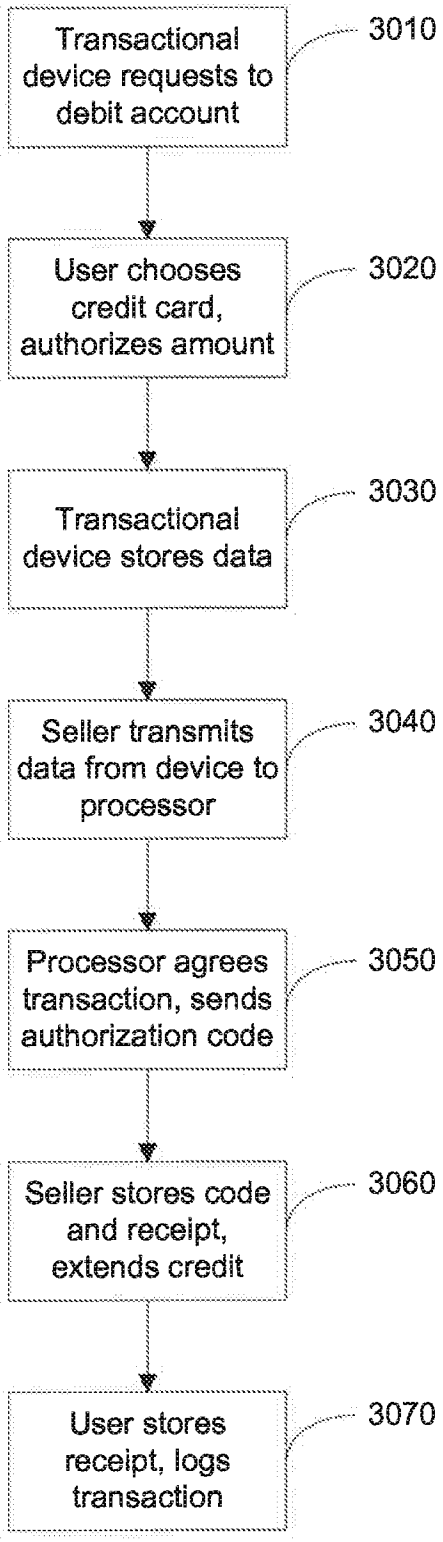
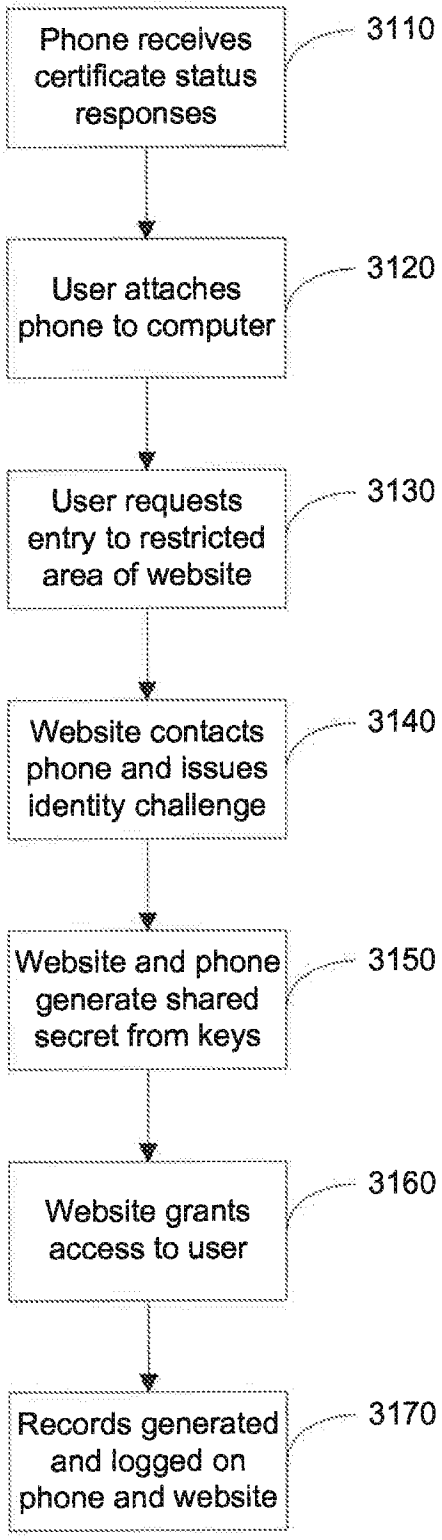

User registers phone with credit company
2905
Phone requests certificate from credit company
2910
Credit company generates credit certificate
2920
2930
2942
Phone receives and stores certificate
2932
User uses phone to transact
2940
Certificate expires

FIG. 30



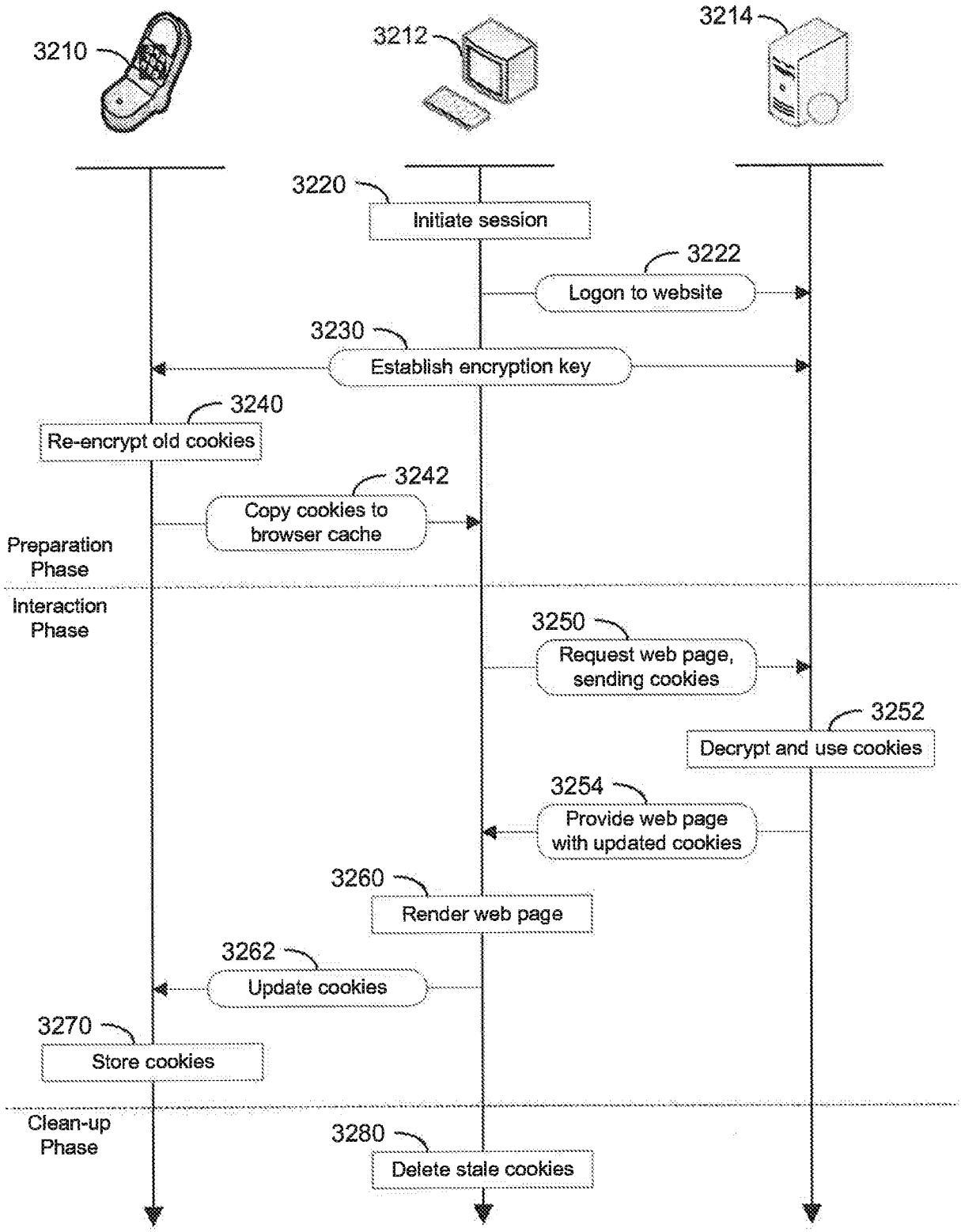
Petitioner Exhibit 1002-0905

FIG. 31



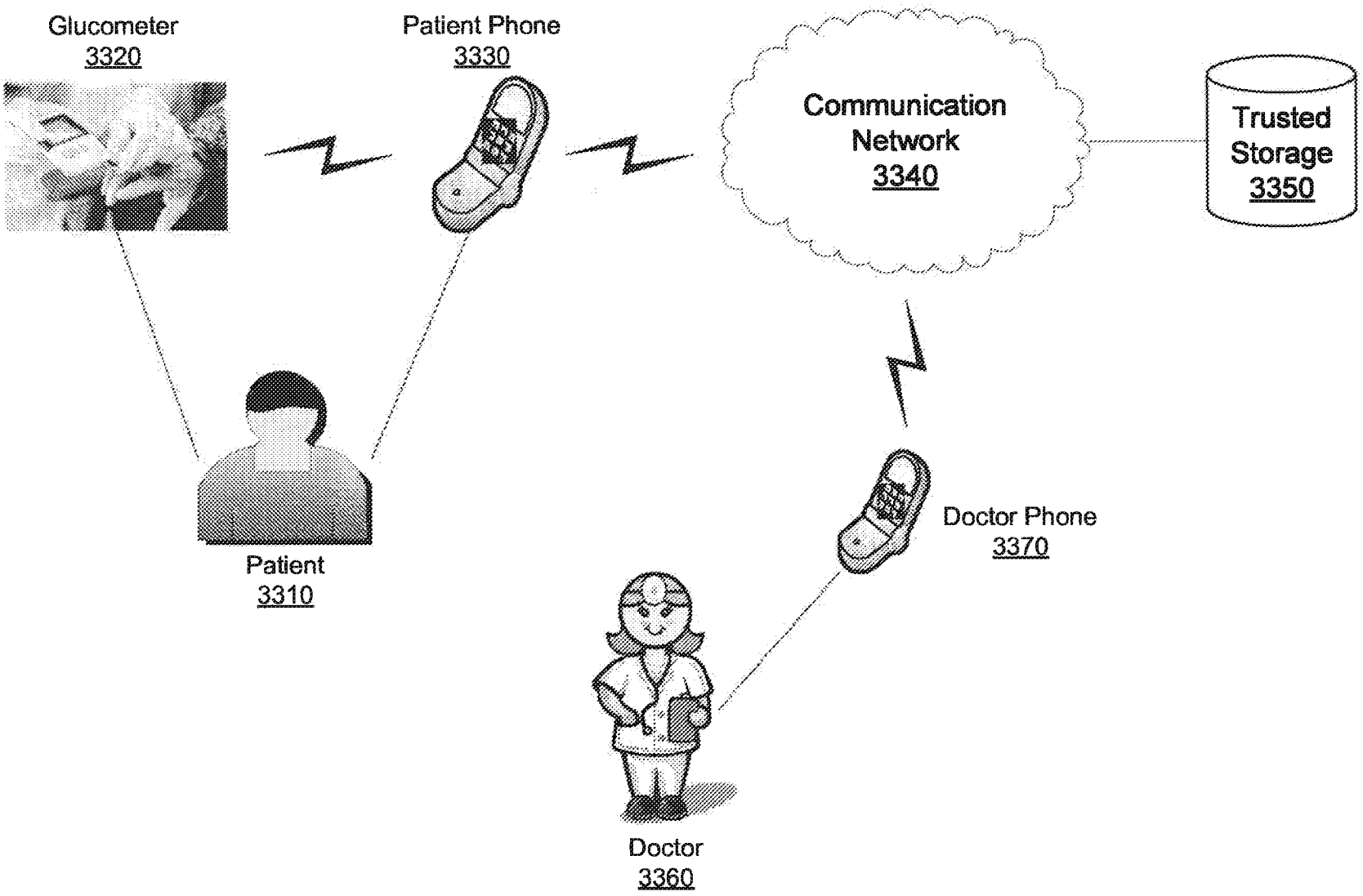
Petitioner Exhibit 1002-0906

FIG. 32



Petitioner Exhibit 1002-0907

FIG. 33



Petitioner Exhibit 1002-0908

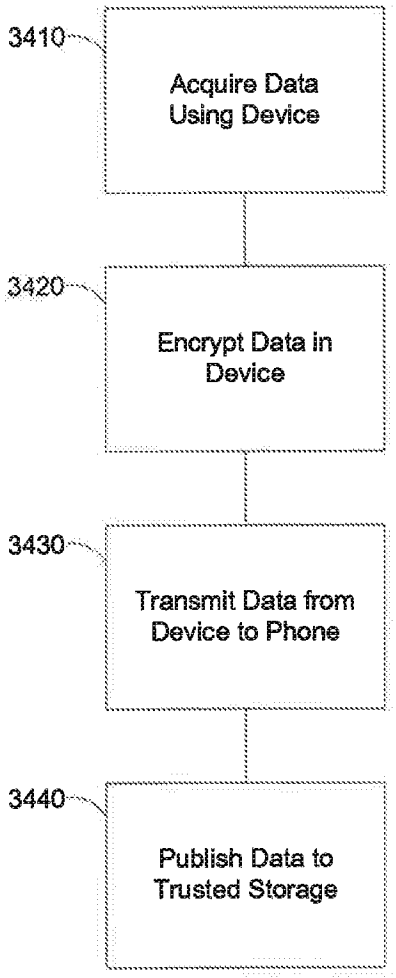

3410
Acquire Data Using Device
3420
Encrypt Data in Device
3430
Transmit Data from Device to Phone
3440
Publish Data to Trusted Storage

FIG. 34

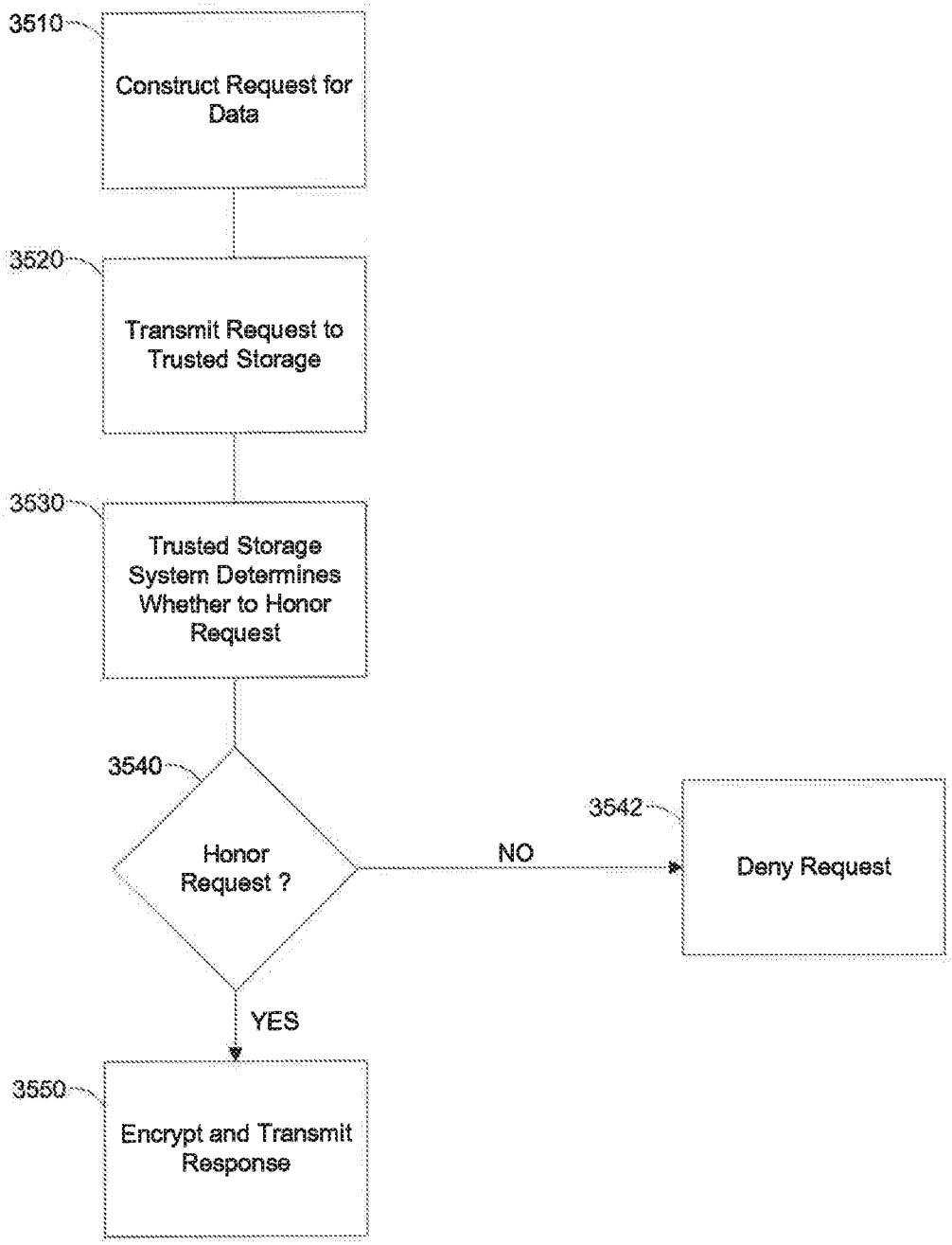

3510
Construct Request for Data
3520
Transmit Request to Trusted Storage
3530
Trusted Storage System Determines Whether to Honor Request
3540
Honor Request ?
NO
3542
Deny Request
YES
3550
Encrypt and Transmit Response

FIG. 35

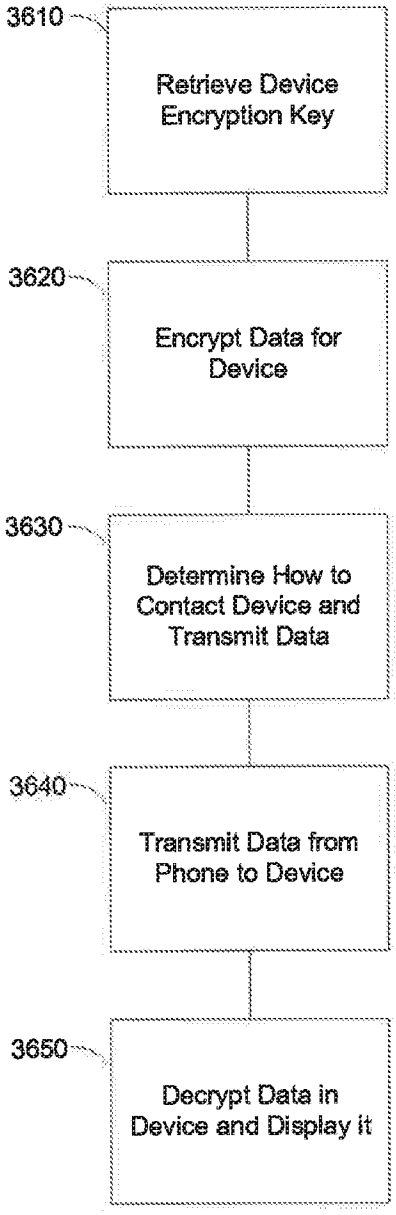

3610
Retrieve Device Encryption Key
3620
Encrypt Data for Device
3630
Determine How to Contact Device and Transmit Data
3640
Transmit Data from Phone to Device
3650
Decrypt Data in Device and Display it

FIG. 36

Espacenet

Bibliographic data: JPWO2013132995 (A1) — 2015-07-30

PAYMENT PROCESSING SYSTEM, PAYMENT TERMINAL, COMMUNICATION DEVICE, PAYMENT SERVER AND PAYMENT PROCESSING METHOD

Inventor(s): 永山 智彦

Applicant(s): ソニー株式会社

Classification: - international: *G06Q20/26; G06Q20/40; G07F7/08; G07G1/12; G07G1/14*
- cooperative: G06Q20/02 (US); G06Q20/204 (EP, CN, US); G06Q20/322 (EP, CN, US); G06Q20/327 (EP, US); G06Q20/3278 (EP, CN, US); G06Q20/382 (EP, US); H04L67/10 (US)

Application number: JP20140503739 20130218 Global Dossier

Priority number(s): JP20120050273 20120307 ; WO2013JP53827 20130218

Also published as: CN104145284 (A) EP2824629 (A1) EP2824629 (A4) JP5935871 (B2) US11017382 (B2) more

Abstract not available for JPWO2013132995 (A1)
Abstract of corresponding document: EP2824629 (A1)

Provided is a payment processing system for executing payment processing by transmitting and receiving payment data between a payment terminal and a payment server via a communication device, the payment terminal not including a dedicated network device for communication with the payment server, the payment data including at least payment amount information and service information to which a payment is to be executed. The payment terminal includes a payment data generation section configured to generate first payment data in which the payment amount information is encrypted, and a terminal communication unit configured to transmit the generated first payment data to the communication device by short range communication

Petitioner Exhibit 1002-0912

(19)日本国特許庁(JP)

再公表特許(A1)

(11)国際公開番号
WO2013/132995

発行日　平成27年7月30日(2015.7.30)

(43)国際公開日　平成25年9月12日(2013.9.12)

(51)Int.Cl.		F I		テーマコード（参考）
G06Q 20/40	(2012.01)	G06Q 20/40	110	3E044
G06Q 20/26	(2012.01)	G06Q 20/26		3E142
G07G 1/12	(2006.01)	G07G 1/12	321L	5L055
G07G 1/14	(2006.01)	G07G 1/14		
G07F 7/08	(2006.01)	G07F 7/08	R	

審査請求 有　予備審査請求 未請求　（全 37 頁）　最終頁に続く

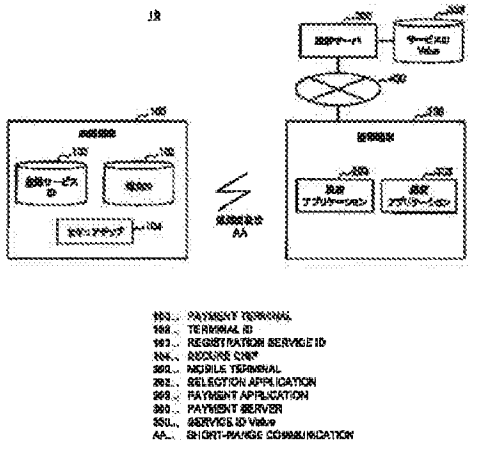
出願番号　特願2014-503739 (P2014-503739)
(21)国際出願番号　PCT/JP2013/053827
(22)国際出願日　平成25年2月18日(2013.2.18)
(31)優先権主張番号　特願2012-50273 (P2012-50273)
(32)優先日　平成24年3月7日(2012.3.7)
(33)優先権主張国　日本国(JP)

(71)出願人　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100095957
弁理士　亀谷　美明
(74)代理人　100096389
弁理士　金本　哲男
(74)代理人　100101557
弁理士　萩原　康司
(74)代理人　100128587
弁理士　松本　一騎
(72)発明者　永山　智彦
東京都港区港南１丁目７番１号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】決済処理システム、決済端末、通信装置、決済サーバ、及び決済処理方法

(57)【要約】
専用のネットワークデバイスを有していない決済端末と決済サーバの間で通信装置を経由した決済処理システムにおいて、決済端末は、決済金額情報を暗号化した第１決済データを生成し、生成された第１決済データを、近距離通信により通信装置へ送信する。通信装置は、決済端末から受信した第１決済データに基づく第２決済データを、ネットワークを介して決済サーバへ送信する。決済サーバは、通信装置から受信した第２決済データを復号化して、決済処理を実行し、決済後に暗号化された残高情報を少なくとも含む第３決済データを、ネットワークを介して通信装置へ送信する。そして、通信装置は、決済サーバから受信した第３決済データに基づく第４決済データを、近距離通信により決済端末へ送信する。



Petitioner Exhibit 1002-0913

【特許請求の範囲】
【請求項１】
決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末と前記決済サーバの間で、通信装置を経由して少なくとも決済金額情報と決済対象のサービス情報とを含む決済データを送受信して、決済処理を実行する決済処理システムであって、
前記決済端末は、
前記決済金額情報を暗号化した第１決済データを生成する決済データ生成部と、
生成された前記第１決済データを、近距離通信により前記通信装置へ送信する端末通信部と、
を備え、
前記通信装置は、
前記近距離通信により前記決済端末から前記第１決済データを受信する第１装置通信部と、
前記決済端末から受信した前記第１決済データに基づく第２決済データを、ネットワークを介して前記決済サーバへ送信する第２装置通信部と、
を備え、
前記決済サーバは、
前記ネットワークを介して前記通信装置から前記第２決済データを受信するサーバ通信部と、
前記通信装置から受信した前記第２決済データを復号化して、決済処理を実行する決済処理部と、
を備え、
前記サーバ通信部は、決済後に暗号化された残高情報を少なくとも含む第３決済データを、前記ネットワークを介して前記通信装置へ送信し、
前記第１装置通信部は、前記第２装置通信部により前記決済サーバから受信した決済後の前記第３決済データに基づく第４決済データを、前記近距離通信により前記決済端末へ送信する、
決済処理システム。
【請求項２】
前記通信装置は、前記第１装置通信部により受信した前記第１決済データを用いて、前記決済サーバへ送信する前記第２決済データを生成する装置データ処理部を更に備え、
前記第２装置通信部は、前記装置データ処理部により生成された前記第２決済データを前記決済サーバへ送信する、
請求項１に記載の決済処理システム。
【請求項３】
前記決済端末から前記通信装置へ送信される前記第１決済データには、決済可能な複数のサービスのリスト情報が暗号化されずに含まれ、
前記装置データ処理部は、前記リスト情報を、前記決済サーバによる決済対象の一のサービス情報に置換することで、前記第２決済データを生成する、
請求項２に記載の決済処理システム。
【請求項４】
前記装置データ処理部は、生成する前記第２決済データに、前記決済サーバで処理される装置付加情報を暗号化せずに付加し、
前記決済サーバは、前記通信装置から受信した前記第２決済データに基づく決済処理の際に、前記装置付加情報に対応する処理を行う、
請求項２に記載の決済処理システム。
【請求項５】
前記通信装置は、前記第２装置通信部により受信した決済後の前記第３決済データを用いて、前記決済端末へ送信する前記第４決済データを生成する装置データ処理部を備

Petitioner Exhibit 1002-0014

前記第１装置通信部は、前記装置データ処理部により生成された前記第４決済データを前記決済端末へ送信する、
請求項１に記載の決済処理システム。
【請求項６】
前記装置データ処理部は、生成する前記第４決済データに、前記決済端末で処理される装置付加情報を暗号化せずに付加し、
前記決済端末は、前記通信装置から受信した前記第４決済データの前記装置付加情報に対応する処理を行う、
請求項５に記載の決済処理システム。
【請求項７】
前記決済サーバから前記通信装置へ送信される前記第３決済データには、前記通信装置で処理されるサーバ付加情報が暗号化せずに含まれ、
前記通信装置は、前記決済サーバから受信した前記第３決済データの前記サーバ付加情報に対応する処理を行う、
請求項１に記載の決済処理システム。
【請求項８】
前記決済端末から前記通信装置へ送信される前記第１決済データには、前記通信装置で処理される端末付加情報が暗号化せずに含まれ、
前記通信装置は、前記決済端末から受信した前記第１決済データの前記端末付加情報に対応する処理を行う、
請求項１に記載の決済処理システム。
【請求項９】
決済可能なサービスのバリューを記憶するバリュー記憶部が、前記決済サーバに接続され、
前記決済処理部は、前記通信装置から受信した前記第２決済データに含まれる前記サービス情報に対応する、前記バリュー記憶部に記憶されたサービスの前記バリューに対して決済処理を行う、
請求項１に記載の決済処理システム。
【請求項１０】
決済可能なサービスのバリューを記憶するバリュー記憶部が、前記通信装置に設けられ、
前記決済処理部は、前記通信装置から受信した前記第２決済データに含まれる前記サービス情報に対応する、前記バリュー記憶部に記憶されたサービスの前記バリューに対して決済処理を行う、
請求項１に記載の決済処理システム。
【請求項１１】
決済可能なサービスのバリューを記憶するバリュー記憶部が、前記通信装置と近距離通信する外部装置に設けられ、
前記決済処理部は、前記通信装置から受信した前記第２決済データに含まれる前記サービス情報に対応する、前記バリュー記憶部に記憶されたサービスの前記バリューに対して決済処理を行う、
請求項１に記載の決済処理システム。
【請求項１２】
決済処理を実行する決済処理システムにおいて、通信装置を経由して決済サーバとの間で、少なくとも決済金額情報と決済対象のサービス情報とを含む決済データの送受信を行う、前記決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末であって、
前記決済金額情報を暗号化した第１決済データを生成する決済データ生成部と、
生成された前記第１決済データを、近距離通信により前記通信装置へ送信する

Petitioner Exhibit 1002-0915

を備え、
前記端末通信部は、前記第１決済データに基づく第２決済データを前記通信装置から受信した前記決済サーバが前記第２決済データを復号化して決済処理した後に、暗号化された残高情報を少なくとも含む第３決済データに基づく第４決済データを前記近距離通信により前記通信装置から受信する、
決済端末。
【請求項１３】
決済処理を実行する決済処理システムにおいて、決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末と前記決済サーバとの間で、少なくとも決済金額情報と決済対象のサービス情報とを含む決済データの送受信を行う通信装置であって、
前記決済端末において前記決済金額情報を暗号化して生成された第１決済データを、近距離通信により前記決済端末から受信する第１装置通信部と、
前記決済端末から受信した前記第１決済データに基づく第２決済データを、ネットワークを介して前記決済サーバへ送信する第２装置通信部と、
を備え、
前記第２装置通信部は、送信した前記第２決済データを前記決済サーバが復号化して決済処理した後に、暗号化された残高情報を少なくとも含む第３決済データを、前記ネットワークを介して前記決済サーバから受信し、
前記第１装置通信部は、前記決済サーバから受信した前記第３決済データに基づく第４決済データを、前記近距離通信により前記決済端末へ送信する、
通信装置。
【請求項１４】
決済処理を実行する決済処理システムにおいて、決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末との間で、通信装置を経由して少なくとも決済金額情報と決済対象のサービス情報とを含む決済データの送受信を行う決済サーバであって、
前記決済端末において前記決済金額情報を暗号化して生成された第１決済データに基づく第２決済データを、ネットワークを介して前記通信装置から受信するサーバ通信部と、
前記通信装置から受信した前記第２決済データを復号化して、決済処理を実行する決済処理部と、
を備え、
前記サーバ通信部は、決済後に暗号化された残高情報を少なくとも含む第３決済データを、前記ネットワークを介して前記通信装置へ送信する、
決済サーバ。
【請求項１５】
決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末と前記決済サーバの間で、通信装置を経由して少なくとも決済金額情報と決済対象のサービス情報とを含む決済データを送受信して、決済処理を実行する決済処理方法であって、
前記決済端末が、前記決済金額情報を暗号化した第１決済データを生成することと、
前記決済端末が、生成された前記第１決済データを、近距離通信により前記通信装置へ送信することと、
前記通信装置が、前記近距離通信により前記決済端末から受信した前記第１決済データに基づく第２決済データを、ネットワークを介して前記決済サーバへ送信することと、
前記決済サーバが、前記ネットワークを介して前記通信装置から受信した前記第２決済データを復号化して、決済処理を実行することと、
前記決済サーバが、決済後に暗号化された残高情報を少なくとも含む第３決済データを、前記ネットワークを介して前記通信装置へ送信することと、
前記通信装置が、前記決済サーバから受信した前記第３決済データに基づく第４決済データを、前記近距離通信により前記決済端末へ送信することと、

Petitioner Exhibit 1002-0916

【請求項１６】
決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末と前記決済サーバの間で、通信装置を経由して少なくとも決済金額情報と決済対象のサービス情報とを含む決済データを送受信して、決済処理を実行する決済処理方法であって、
前記通信装置が、前記決済端末において前記決済金額情報を暗号化して生成された第１決済データを、近距離通信により前記決済端末から受信することと、
前記通信装置が、前記決済端末から受信した前記第１決済データに基づく第２決済データを、ネットワークを介して前記決済サーバへ送信することと、
前記通信装置が、送信した前記第２決済データを前記決済サーバが復号化して決済処理した後に、暗号化された残高情報を少なくとも含む第３決済データを、前記ネットワークを介して前記決済サーバから受信することと、
前記通信装置が、前記決済サーバから受信した前記第３決済データに基づく第４決済データを、前記近距離通信により前記決済端末へ送信することと、
を含む決済処理方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、決済処理システム、決済端末、通信装置、決済サーバ、及び決済処理方法に関する。
【背景技術】
【０００２】
近年、購入者がサービスに対する対価として現金の代わりに電子マネーで決済ができる電子マネーシステムが普及している。この電子マネーシステムでは、例えば、サービスを提供する店舗の決済端末と、電子マネーシステムの事業者の決済サーバとの間で決済データを送受信することで、決済処理が行われる。
【０００３】
下記の特許文献１には、買物の支払、サービス代価の支払、自動販売機の支払、タクシー運賃の支払などのオフライン取引の決済について開示されている。具体的には、決済の際に、現金、クレジットカードまたはポイントカードなどを持参することなく携帯端末を決済用近距離無線通信機器にかざすだけの簡単な操作でポイントの利用と決済が出来る決済方法が開示されている。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２０１１－１４１８５３号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかし、特許文献１の技術では、取引データの改ざん等を防止する観点から、クライアント端末に、決済サーバと通信を行う専用のネットワークデバイスを設けている。このようなネットワークデバイスを設けるとクライアント端末の構成が複雑になり、またコストも高くなる。
【０００６】
そこで、本開示は、決済サーバと通信を行う専用のネットワークデバイスを有しない決済端末を利用して、安全かつ汎用的な決済方法を提案する。
【課題を解決するための手段】
【０００７】
本開示によれば、決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末と前記決済サーバの間で、通信装置を経由して少なくとも決済金額情報と決済対

Petitioner Exhibit 1002-0917

象のサービス情報とを含む決済データを送受信して、決済処理を実行する決済処理システムであって、前記決済端末は、前記決済金額情報を暗号化した第１決済データを生成する決済データ生成部と、生成された前記第１決済データを、近距離通信により前記通信装置へ送信する端末通信部と、を備え、前記通信装置は、前記近距離通信により前記決済端末から前記第１決済データを受信する第１装置通信部と、前記決済端末から受信した前記第１決済データに基づく第２決済データを、ネットワークを介して前記決済サーバへ送信する第２装置通信部と、を備え、前記決済サーバは、前記ネットワークを介して前記通信装置から前記第２決済データを受信するサーバ通信部と、前記通信装置から受信した前記第２決済データを復号化して、決済処理を実行する決済処理部と、を備え、前記サーバ通信部は、決済後に暗号化された残高情報を少なくとも含む第３決済データを、前記ネットワークを介して前記通信装置へ送信し、前記第１装置通信部は、前記第２装置通信部により前記決済サーバから受信した決済後の前記第３決済データに基づく第４決済データを、前記近距離通信により前記決済端末へ送信する、決済処理システムが提供される。

【０００８】

かかる構成によれば、前記決済端末は、前記決済金額情報を暗号化した第１決済データを生成し、生成された前記第１決済データを、近距離通信により前記通信装置へ送信する。前記通信装置は、前記近距離通信により前記決済端末から受信した前記第１決済データに基づく第２決済データを、ネットワークを介して前記決済サーバへ送信する。前記決済サーバは、前記ネットワークを介して前記通信装置から受信した前記第２決済データを復号化して、決済処理を実行し、決済後に暗号化された残高情報を少なくとも含む第３決済データを、前記ネットワークを介して前記通信装置へ送信する。そして、前記通信装置は、前記決済サーバから受信した前記第３決済データに基づく第４決済データを、前記近距離通信により前記決済端末へ送信する。これにより、決済端末にネットワークデバイスを設けなくても、通信装置を経由して決済端末と決済サーバとの間で決済データの送受信ができる。また、暗号化された決済データが送受信されるので、暗号化された情報の改ざんを防止できる。従って、決済サーバと通信を行う専用のネットワークデバイスを有しない決済端末を利用して、安全かつ汎用的な決済方法を実現できる。

【０００９】

また、本開示によれば、決済処理を実行する決済処理システムにおいて、決済処理を実行する決済処理システムにおいて、通信装置を経由して決済サーバとの間で、少なくとも決済金額情報と決済対象のサービス情報とを含む決済データの送受信を行う、前記決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末であって、前記決済金額情報を暗号化した第１決済データを生成する決済データ生成部と、生成された前記第１決済データを、近距離通信により前記通信装置へ送信する端末通信部と、を備え、前記端末通信部は、前記第１決済データに基づく第２決済データを前記通信装置から受信した前記決済サーバが前記第２決済データを復号化して決済処理した後に、暗号化された残高情報を少なくとも含む第３決済データに基づく第４決済データを前記近距離通信により前記通信装置から受信する、決済端末が提供される。

【００１０】

また、本開示によれば、決済処理を実行する決済処理システムにおいて、決済処理を実行する決済処理システムにおいて、決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末と前記決済サーバとの間で、少なくとも決済金額情報と決済対象のサービス情報とを含む決済データの送受信を行う通信装置であって、前記決済端末において前記決済金額情報を暗号化して生成された第１決済データを、近距離通信により前記決済端末から受信する第１装置通信部と、前記決済端末から受信した前記第１決済データに基づく第２決済データを、ネットワークを介して前記決済サーバへ送信する第２装置通信部と、を備え、前記第２装置通信部は、送信した前記第２決済データを前記決済サーバが復号化して決済処理した後に、暗号化された残高情報を少なくとも含む第３決済データを、前記ネットワークを介して前記決済サーバから受信し、前記第１装置通信部は

Petitioner Exhibit 1002-0018

により前記決済端末へ送信する、通信装置が提供される。

【００１１】

また、本開示によれば、決済処理を実行する決済処理システムにおいて、決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末との間で、通信装置を経由して少なくとも決済金額情報と決済対象のサービス情報とを含む決済データの送受信を行う決済サーバであって、前記決済端末において前記決済金額情報を暗号化して生成された第１決済データに基づく第２決済データを、ネットワークを介して前記通信装置から受信するサーバ通信部と、前記通信装置から受信した前記第２決済データを復号化して、決済処理を実行する決済処理部と、を備え、前記サーバ通信部は、決済後に暗号化された残高情報を少なくとも含む第３決済データを、前記ネットワークを介して前記通信装置へ送信する、決済サーバが提供される。

【００１２】

また、本開示によれば、決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末と前記決済サーバの間で、通信装置を経由して少なくとも決済金額情報と決済対象のサービス情報とを含む決済データを送受信して、決済処理を実行する決済処理方法であって、前記決済端末が、前記決済金額情報を暗号化した第１決済データを生成することと、前記決済端末が、生成された前記第１決済データを、近距離通信により前記通信装置へ送信することと、前記通信装置が、前記近距離通信により前記決済端末から受信した前記第１決済データに基づく第２決済データを、ネットワークを介して前記決済サーバへ送信することと、前記決済サーバが、前記ネットワークを介して前記通信装置から受信した前記第２決済データを復号化して、決済処理を実行することと、前記決済サーバが、決済後に暗号化された残高情報を少なくとも含む第３決済データを、前記ネットワークを介して前記通信装置へ送信することと、前記通信装置が、前記決済サーバから受信した前記第３決済データに基づく第４決済データを、前記近距離通信により前記決済端末へ送信することと、を含む決済処理方法が提供される。

【００１３】

また、本開示によれば、決済サーバと通信を行う専用のネットワークデバイスを有していない決済端末と前記決済サーバの間で、通信装置を経由して少なくとも決済金額情報と決済対象のサービス情報とを含む決済データを送受信して、決済処理を実行する決済処理方法であって、前記通信装置が、前記決済端末において前記決済金額情報を暗号化して生成された第１決済データを、近距離通信により前記決済端末から受信することと、前記通信装置が、前記決済端末から受信した前記第１決済データに基づく第２決済データを、ネットワークを介して前記決済サーバへ送信することと、前記通信装置が、送信した前記第２決済データを前記決済サーバが復号化して決済処理した後に、暗号化された残高情報を少なくとも含む第３決済データを、前記ネットワークを介して前記決済サーバから受信することと、前記通信装置が、前記決済サーバから受信した前記第３決済データに基づく第４決済データを、前記近距離通信により前記決済端末へ送信することと、を含む決済処理方法が提供される。

【発明の効果】

【００１４】

以上説明したように本開示によれば、決済サーバと通信を行う専用のネットワークデバイスを有しない決済端末を利用して、安全かつ汎用的な決済方法を実現可能である。

【図面の簡単な説明】

【００１５】

【図１】本開示の第１の実施形態に係る決済処理システムの概要を説明するための図である。

【図２】第１の実施形態に係る決済端末の機能構成の一例を示すブロック図である。

【図３】第１の実施形態に係る決済データ生成部により生成される決済データＤａの一例を示す図である。

Petitioner Exhibit 1002-0919

【図５】第１の実施形態に係る決済データ処理部により処理される決済データＤｂの一例を示す図である。
【図６】第１の実施形態に係る決済サーバから受信する決済データＤｃの一例を示す図である。
【図７】第１の実施形態に係る決済データ処理部により処理される決済データＤｄの一例を示す図である。
【図８】第１の実施形態に係る決済サーバの機能構成の一例を示すブロック図である。
【図９】第１の実施形態に係る決済処理システムによる決済処理の流れを示すフローチャートである。
【図１０】第１の実施形態に係る決済処理システムにおける認証関係を説明するための模式図である。
【図１１】本開示の第２の実施形態に係る決済処理システムの概要を説明するための図である。
【図１２】本開示の第３の実施形態に係る決済処理システムの概要を説明するための図である。
【図１３】第１～第３の実施形態に係る携帯端末のハードウェア構成の一例を示すブロック図である。
【図１４】第１の実施形態に係る携帯端末サーバデータの一例を示す図である。
【図１５】第１の実施形態の変形例に係る携帯端末サーバデータの一例を示す図である。
【発明を実施するための形態】
【００１６】
以下に添付図面を参照しながら、本開示の好適な実施の形態について詳細に説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複説明を省略する。
【００１７】
なお、説明は以下の順序で行うものとする。
１．第１の実施形態
１－１．決済処理システムの概要
１－２．決済端末の構成例
１－３．携帯端末の構成例
１－４．決済サーバの構成例
１－５．決済処理システムによる決済処理の流れ
１－６．決済処理システムにおける認証関係
１－７．まとめ
２．第２の実施形態
３．第３の実施形態
４．ハードウェア構成例
【００１８】
＜１．第１の実施形態＞
（１－１．決済処理システムの概要）
図１を参照しながら、本開示の第１の実施形態に係る決済処理システム１０の概要について説明する。図１は、本開示の第１の実施形態に係る決済処理システム１０の概要を説明するための図である。
【００１９】
決済処理システム１０は、図１に示すように、決済端末１００と、通信装置の一例である携帯端末２００と、決済サーバ３００と、ネットワーク４００と、を有する。この決済処理システム１０は、例えば、サービスを提供する店舗の決済端末１００と、電子マネーシステムの事業者の決済サーバ３００との間で、携帯端末２００を経由して決済データを送受信することで、決済処理を行うものである。

Petitioner Exhibit 1002-0920

決済端末１００は、サービスを提供する店舗に設置された端末であり、例えばＰＯＳ（Point Of Sales）装置である。決済端末１００は、決済端末１００の端末ＩＤ１０２と、電子マネー事業者から取得した登録サービスＩＤ１０３と、を記憶している。決済端末１００は、決済処理される決済金額を受け付ける機能と、決済処理後にレシートを出力する機能と、を有する。また、決済端末１００は、セキュリティ処理を実行するセキュアチップ１０４を有する。

【００２１】

また、決済端末１００は、例えばリーダ／ライタ（不図示）を有し、携帯端末２００と近距離通信（非接触通信とも呼ばれる）を行う。例えば、決済端末１００は、携帯端末２００とＮＦＣ（Near Field Communication）による通信を行い、データを送受信する。決済端末１００は、決済処理に供される暗号化された決済データを、携帯端末２００を経由して決済サーバ３００に送信する。

【００２２】

携帯端末２００は、サービスが提供される購入者が利用する端末であり、例えばスマートフォンや携帯電話である。携帯端末２００は、近距離通信により、決済端末１００との間で決済データの送受信を行う。また、携帯端末２００は、無線通信によりネットワーク４００を介して、決済サーバ３００との間で決済データの送受信を行う。携帯端末２００には、決済処理におけるサービスを選択する選択アプリケーション２０２と、サービス毎の決済アプリケーション２０３と、がインストールされている。

【００２３】

決済サーバ３００は、例えば電子マネーシステムを管理する事業者側のサーバである。決済サーバ３００は、携帯端末２００を経由して決済端末１００から受信した決済データを復号化し、復号化した決済データに基づいて決済処理を行う。決済サーバ３００には、決済対象のサービスＩＤのバリュー３５０を記憶するバリュー記憶部の一例であるデータベースが接続されており、決済サーバ３００は、決済データのサービスＩＤに対応するバリューに対して決済処理を行う。

【００２４】

ネットワーク４００は、携帯端末２００と決済サーバ３００を接続する無線、または有線の伝送路である。ネットワーク４００は、例えば、インターネット、電話回線網、衛星通信網などの公衆回線網や、Ｅｔｈｅｒｎｅｔ（登録商標）を含む各種のＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）、ＷＡＮ（Ｗｉｄｅ Ａｒｅａ Ｎｅｔｗｏｒｋ）などを含んでもよい。また、ネットワーク４００は、ＩＰ－ＶＰＮ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ－Ｖｉｒｔｕａｌ Ｐｒｉｖａｔｅ Ｎｅｔｗｏｒｋ）などの専用回線網を含んでもよい。なお、決済端末１００と携帯端末２００の間の通信路と、携帯端末２００と決済サーバ３００の間の通信路は、予め暗号化されている。

【００２５】

（１－２．決済端末の構成例）

図２を参照しながら、第１の実施形態に係る決済端末１００の機能構成の一例について説明する。図２は、第１の実施形態に係る決済端末１００の機能構成の一例を示すブロック図である。

【００２６】

決済端末１００は、決済処理システムにおいて携帯端末２００を経由して決済サーバ３００との間で決済データの送受信を行って、決済処理を行う。図２に示すように、決済端末１００は、制御部１１０と、記憶部１１２と、入力部１１４と、表示部１１６と、端末通信部の一例である近距離通信部１１８と、を有する。

【００２７】

制御部１１０は、決済端末１００の各ブロックと信号をやり取りして各種演算を行い、決済端末１００の動作全体を制御する。例えば、制御部１１０は、決済データを生成して送信する処理を行う。制御部１１０は、例えばＣＰＵ、ＲＯＭ、ＲＡＭ、[illegible]

Petitioner Exhibit 1002-0921

【００２８】
決済データ生成部１２０は、図３に示す決済データを生成する。決済データは、決済金額や、決済端末１００の端末ＩＤ等の決済情報を含む。なお、決済データは、決済サーバ３００に直接送信されるのではなく、近距離通信部１１８により携帯端末２００に送信される。

【００２９】
図３は、第１の実施形態に係る決済データ生成部１２０により生成される決済データＤａの一例を示す図である。決済データＤａは、決済端末ＩＤと、サーバＩＤと、決済実行ＩＤと、決済金額と、携帯端末ＩＤと、携帯端末サーバデータと、決済端末による署名値と、サービスＩＤリストと、端末付加情報の一例である付加情報Ｉ１とを含む。

【００３０】
端末ＩＤは、決済端末１００のＩＤを示す。サーバＩＤは、決済サーバ３００のＩＤを示す。決済実行ＩＤは、決済後に出力されるレシートの番号に利用される。決済金額は、入力部１１４で受け付けた決済金額である。携帯端末ＩＤは、携帯端末２００のＩＤを示す。携帯端末サーバデータは、決済処理に用いられるものであり、図１４に示すように、携帯端末ＩＤと、ユーザＩＤと、サーバによる署名値と、を含む。ユーザＩＤは、決済処理に用いられる携帯端末２００のユーザのＩＤを示す。図１４は、第１の実施形態に係る携帯端末サーバデータの一例を示す図である。

【００３１】
図３に戻って、決済データＤａの説明を続ける。決済端末による署名値は、決済データを受信した決済サーバ３００が決済端末１００の認証に用いるものである。サービスＩＤリストは、決済端末１００が処理可能（決済可能）な複数のサービスＩＤの一覧を示す。付加情報Ｉ１は、携帯端末２００で処理される情報である。例えば、付加情報Ｉ１は、決済端末１００が設置された店舗の特売に関する情報（来週の特売予定、現在の特売等）である。また、付加情報Ｉ１は、決済データを送信する携帯端末２００のユーザに応じて付加されても良い。

【００３２】
決済データＤａのうち端末ＩＤ及び決済金額は、決済端末１００（セキュアチップ１０４）により署名されると共に、予めサーバ３００から取得したサーバ鍵で暗号化される。一方で、サービスＩＤリストは、暗号化されていない。なお、暗号化された決済金額と同じ決済金額の情報が、携帯端末２００でユーザに表示させるために、暗号化されずに決済データＤａに含まれている。決済サーバ３００で決済に供される決済金額は、暗号化された決済金額である。

【００３３】
署名検証部１２２は、携帯端末２００から受信した決済後の決済データに付された決済サーバ３００の認証を検証する。これにより、決済端末１００は、送信した決済データに対応した決済が実行されたかを確認できる。

【００３４】
記憶部１１２は、制御部１１０が実行する制御プログラムや、制御部１１０が決済処理に用いるデータを記憶する。例えば、記憶部１１２は、決済端末１００の端末ＩＤや、電子マネー事業者から取得した登録サービスＩＤを記憶する。また、記憶部１１２は、決済データＤａの付加情報Ｉ１に関する情報や、決済サーバ３００から取得したサーバ鍵を記憶する。

【００３５】
入力部１１４は、決済端末１００の利用者の操作を受け付け、入力信号を制御部１１０に出力する。入力部１１４は、決済端末１００の利用者の操作による各種の情報を受け付ける。例えば、入力部１１４は、決済金額を受け付ける。入力部１１４は、例えば、キーボード、マウス等で構成されうるが、タッチパネルで構成されても良い。

【００３６】

Petitioner Exhibit 1002-0922

決済処理に関する設定画面（例えば、決済金額を受け付ける画面）を表示する。表示部１１６は、例えばＴＦＴ（Thin Film Transistor）等のＬＣＤやＯＥＬＤ（Organic Electro-Luminescence Display）である。

【００３７】

近距離通信部１１８は、通信アンテナを有し、携帯端末２００と近距離通信（ＮＦＣ通信）を行う。近距離通信部１１８は、近距離通信により、携帯端末２００との間で決済データの送受信を行う。例えば、近距離通信部１１８は、決済データ生成部１２０により生成された決済データ（図３に示す決済データＤａ）を携帯端末２００へ送信する。

【００３８】

上述した構成を有する決済端末１００は、決済金額情報を暗号化した決済データＤａを生成し、生成された決済データＤａを近距離通信により携帯端末２００へ送信する。そして、決済端末１００は、送信した決済データを決済サーバ３００が復号化して決済処理した後に、暗号化された残高情報を少なくとも含む決済データを近距離通信により携帯端末２００から受信する。これにより、決済端末１００にネットワークデバイスを設けなくても、携帯端末２００を経由して決済端末１００と決済サーバ３００との間で決済データの送受信ができる。また、暗号化された決済データが送受信されるので、携帯端末２００において、暗号化された情報（例えば、端末ＩＤや決済金額）の改ざんを防止できる。

【００３９】

（１－３．携帯端末の構成例）

図４を参照しながら、第１の実施形態に係る携帯端末２００の機能構成の一例について説明する。図４は、第１の実施形態に係る携帯端末２００の機能構成の一例を示すブロック図である。

【００４０】

携帯端末２００は、決済処理システム１０において決済端末１００と決済サーバ３００の間の決済データの送受信を中継する装置である。携帯端末２００は、図４に示すように、制御部２１０と、記憶部２１２と、入力部２１４と、表示部２１６と、第１装置通信部の一例である近距離通信部２１８と、第２装置通信部の一例である無線通信部２２０と、を有する。

【００４１】

制御部２１０は、携帯端末２００の各ブロックと信号をやり取りして各種演算を行い、携帯端末２００の動作全体を制御する。例えば、制御部２１０は、決済端末１００及び決済サーバ３００との間で決済データを送受信する処理を行う。制御部２１０は、装置データ処理部の一例である決済データ処理部２２２を有する。

【００４２】

決済データ処理部２２２は、決済端末１００から受信した決済データＤａを処理する。決済データ処理部２２２は、決済データＤａに含まれる付加情報Ｉ１に対応した処理を実行する。例えば、決済データ処理部２２２は、付加情報Ｉ１に基づいて、表示部２１６に表示させるための処理を行う。

【００４３】

また、決済データ処理部２２２は、図３に示す決済データＤａを用いて、図５に示す決済サーバ３００へ送信する決済データＤｂを生成する。すなわち、決済データ処理部２２２は、決済データＤａに別の付加情報（装置付加情報の一例）を加えた決済データＤｂを生成する。

【００４４】

図５は、第１の実施形態に係る決済データ処理部２２２により処理される決済データＤｂの一例を示す図である。決済データＤｂは、決済データＤａと同様にサーバ鍵で暗号された、決済端末ＩＤと、サーバＩＤと、決済実行ＩＤと、決済金額と、携帯端末ＩＤと、携帯端末サーバデータと、決済端末による署名値と、を含む。さらに、決済データＤｂは、サービスＩＤと、付加情報Ｉ２と、を含む。

Petitioner Exhibit 1002-0923

サービスＩＤは、決済データＤａのサービスＩＤリストの中で携帯端末２００のユーザが選択したサービスＩＤである。すなわち、決済データ処理部２２２は、サービスＩＤリストを決済対象のサービスＩＤに置換する。付加情報Ｉ２は、ユーザに関する情報であり、例えば、決済サービスの会員ＩＤや、Facebook等のソーシャルユーティリティサイトのＩＤ等である。付加情報Ｉ２は、ここでは暗号化されていない。ただし、付加情報Ｉ２も暗号化されることとしても良い。そして、決済サーバ３００は、決済データＤｂの付加情報Ｉ２に対応する処理を行う。

【００４６】

なお、上記では、決済データ処理部２２２は、決済データＤｂに付加情報Ｉ２を付加することとしたが、付加情報Ｉ２を付加しなくても良い。また、決済データＤａにおいてサービスＩＤリストの代わりにサービスＩＤが含まれている場合には、サービスＩＤリストをサービスＩＤに置換する処理が不要となる。

【００４７】

また、決済データ処理部２２２は、決済サーバ３００から受信した図６に示す決済データＤｃ（決済サーバ３００における決済データＤａに基づく決済処理後のデータ）を用いて、決済端末１００へ送信する図７に示す決済データＤｄを生成する。すなわち、決済データ処理部２２２は、決済データＤｃに別の付加情報（装置付加情報の一例）を加えた決済データＤｄを生成する。なお、付加情報は、ここでは暗号化されない。しかし、これに限定されず、付加情報も暗号化されても良い。

【００４８】

図６は、第１の実施形態に係る決済サーバ３００から受信する決済データＤｃの一例を示す図である。決済データＤｃは、決済サーバ３００で生成されている。決済データＤｃは、決済端末鍵で暗号化された、決済端末ＩＤと、サーバＩＤと、決済実行ＩＤと、決済金額と、携帯端末ＩＤと、残高と、サーバによる署名値と、を含む。また、決済データＤｃは、付加情報Ｉ３を含む。

【００４９】

決済データＤｃの決済端末ＩＤと、サーバＩＤと、決済実行ＩＤと、決済金額と、携帯端末ＩＤは、図５に示す決済データＤｂと同じである。残高は、携帯端末２００のユーザの利用可能な金額である。付加情報Ｉ３は、携帯端末で処理される情報であり、例えば、決済端末１００の登録情報（決済端末１００の位置情報）を反映した決済端末１００周辺の広告情報、観光情報、ポイント情報等である。そして、携帯端末２００（決済データ処理部２２２）は、決済データＤｃの付加情報Ｉ３に対応する処理を行う。なお、決済データＤｃの端末ＩＤ、決済金額、サービスＩＤ、サーバＩＤ、及び残高は、決済サーバ３００により署名されると共に、決済端末１００の端末鍵で暗号化されている。一方で、付加情報Ｉ３は、ここでは暗号化されていない。しかし、付加情報Ｉ３も暗号化されても良い。

【００５０】

決済データ処理部２２２は、付加情報Ｉ３に、決済データＤｂの携帯端末サーバデータを追加しても良い。そして、決済データＩ３に追加された携帯端末サーバデータを、次の処理で用いても良い。なお、かかる場合には、携帯端末サーバデータに、図１５に示すように、実行カウンタが追加される。これにより、決済端末１００からの電文再利用が可能というセキュリティ上の問題を解決しうる。図１５は、第１の実施形態の変形例に係る携帯端末サーバデータの一例を示す図である。

【００５１】

図７は、第１の実施形態に係る決済データ処理部２２２により処理される決済データＤｄの一例を示す図である。決済データＤｄは、決済データＤｃと同様に決済端末鍵で暗号化された、決済端末ＩＤと、サーバＩＤと、決済実行ＩＤと、決済金額と、携帯端末ＩＤと、残高と、サーバによる署名値と、を含む。さらに、決済データＤｄは、付加情報Ｉ４を含む。

Petitioner Exhibit 1002-0924

決済データＤｄの決済端末ＩＤと、サーバＩＤと、決済実行ＩＤと、決済金額と、携帯端末ＩＤと、残高と、サーバによる署名値は、決済データＤｃと同じである。付加情報Ｉ４は、ここでは暗号化されておらず、決済端末１００で処理される情報である。ただし、付加情報Ｉ４も暗号化されることとしても良い。例えば、付加情報Ｉ４は、決済端末１００からのレシートの受け取りの有無や、ポイントサービスのポイントを付与するサービスの指定に関する情報等である。そして、決済端末１００は、決済データＤｄの付加情報Ｉ４に対応した処理を行う。

【００５３】

記憶部２１２は、制御部２１０が実行する制御プログラムや、制御部２１０が処理する各種のデータを記憶する。例えば、記憶部２１２は、決済データＤｂの付加情報Ｉ２に関する情報や、決済データＤｄの付加情報Ｉ４に関する情報を記憶する。また、記憶部２１２は、携帯端末２００が対応できるサービスＩＤに関する情報を記憶する。記憶部２１２は、例えばフラッシュメモリ等で構成される。

【００５４】

入力部２１４は、携帯端末２００の利用者の操作を受け付け、入力信号を制御部２１０に出力する。入力部２１４は、携帯端末２００のユーザの操作による各種の情報を受け付ける。入力部２１４は、例えばキー、ボタン、スイッチ等で構成されうるが、タッチパネルで構成されても良い。

【００５５】

表示部２１６は、表示画面に各種の画像や情報を表示する。表示部２１６は、例えば、決済端末１００から受信した決済データＤａに含まれる付加情報Ｉ１（ここでは、決済端末１００が設置された店舗の特売に関する情報）に対応した情報を表示する。これにより、携帯端末２００のユーザは、表示部２１６の表示を見ることで、店舗に関する情報を取得できる。また、ユーザは、付加情報Ｉ１に付加された個別情報も知ることができ、ユーザのプライバシーを保護できる。

【００５６】

近距離通信部２１８は、決済端末１００の近距離通信部１１８と近距離通信（ＮＦＣ通信）を行う。近距離通信部２１８は、近距離通信により、携帯端末２００との間で決済データの送受信を行う。近距離通信部２１８は、決済端末１００から決済データＤａを受信する。また、近距離通信部２１８は、決済データ処理部２２２により生成された決済後の決済データＤｄ（図６参照）を決済端末１００へ送信する。

【００５７】

無線通信部２２０は、ネットワーク４００を介して決済サーバ３００と無線通信を行う。無線通信部２２０は、決済サーバ３００に決済データ処理部２２２により生成された決済データＤｂ（図５）を送信し、決済サーバ３００から図６に示す決済後の決済データＤｃを受信する。無線通信部２２０は、例えばネットワークインタフェースカードやモデム等を有し、インターネットやＬＡＮ（Local Area Network）等のネットワークを介して、決済サーバ３００との間で通信処理を行う。無線通信部２２０は、無線ＬＡＮモージュル、又はＷＷＡＮ（Wireless Wide Area Network）モージュルを有していても良い。

【００５８】

上述した構成を有する携帯端末２００は、決済端末１００において生成された決済データＤａを、近距離通信により決済端末１００から受信し、受信した決済データＤａに基づく決済データＤｂを、ネットワーク４００を介して決済サーバ３００へ送信する。また、携帯端末２００は、送信した決済データＤａを決済サーバ３００が復号化して決済処理した後に、暗号化された残高情報を少なくとも含む決済データＤｃを、ネットワーク４００を介して決済サーバ３００から受信する。そして、携帯端末２００は、受信した決済データＤｃに基づく決済データＤｄを、近距離通信により決済端末１００へ送信する。これにより、決済端末１００にネットワークデバイスを設けなくても、携帯端末２００を経由して決済端末１００と決済サーバ３００との間で決済データの送受信[illegible]

Petitioner Exhibit 1002-0925

例えば、端末ＩＤや決済金額）の改ざんを防止できる。

【００５９】

（１－４．決済サーバの構成例）

図８を参照しながら、第１の実施形態に係る決済サーバ３００の機能構成の一例について説明する。図８は、第１の実施形態に係る決済サーバ３００の機能構成の一例を示すブロック図である。

【００６０】

決済サーバ３００は、決済端末１００から携帯端末２００を経由して受信した決済データを復号化して、決済処理を行う。また、決済サーバ３００は、決済後の決済データを、携帯端末２００を経由して決済端末１００に送信する。図８に示すように、決済サーバ３００は、制御部３１０と、記憶部３１２と、入力部３１４と、表示部３１６と、サーバ通信部の一例である無線通信部３１８と、を有する。

【００６１】

制御部３１０は、決済サーバ３００の各ブロックと信号をやり取りして各種演算を行い、決済サーバ３００の動作全体を制御する。例えば、制御部３１０は、受信した決済データに基づいて、決済処理を行う。制御部３１０は、署名検証部３２０と、決済処理部３２２と、決済データ処理部３２４と、を有する。

【００６２】

署名検証部３２０は、携帯端末２００から受信した決済データＤｂの端末ＩＤにより、決済端末１００の認証を検証する。具体的には、署名検証部３２０は、サーバ鍵で決済データＤｂ中の暗号化されたデータを復号化し、決済端末１００による署名値を検証し、決済端末ＩＤを確認する。これにより、決済サーバ３００は、決済端末１００がサービス登録された装置であることを確認する。

【００６３】

決済処理部３２２は、復号化された決済データＤｂを用いて、決済処理を実行する。すなわち、決済処理部３２２は、決済データＤｂのサービスＩＤに対応するバリュー（すなわち、図１に示す決済サーバ３００に接続されたデータベースに記憶されたバリュー３５０）に対して、決済データＤｂの決済金額（暗号化されていた決済金額）の決済を実行する。これにより、バリューを携帯端末２００に登録する必要がなくなり、多様なバリューに対して決済処理を実行できる。

【００６４】

決済データ処理部３２４は、携帯端末２００から受信した決済データＤｂを処理する。決済データ処理部３２４は、決済データＤｂに含まれる付加情報１２（決済サービスの会員ＩＤ等）に対応した処理を実行する。例えば、決済データ処理部３２４は、付加情報１２を参照して、決済処理と会員ＩＤとを包括的に管理しうる。また、決済データ処理部３２４は、会員ＩＤを参照してサービスポイントの取得等の処理を行なっても良い。

【００６５】

また、決済データ処理部３２４は、決済処理部３２２による決済処理後に、決済データＤｂに基づいて、上述した図６に示す決済データＤｃを生成する。すなわち、決済データ処理部３２４は、端末ＩＤと、決済金額と、サービスＩＤと、サーバＩＤと、残高と、付加情報１３と、を含む決済データＤｃを生成する。決済データＤｃの端末ＩＤ、決済金額、サービスＩＤ、サーバＩＤ、残高は、決済サーバ３００により署名されると共に、予め決済端末１００から取得した決済端末１００の端末鍵で暗号化される。一方で、付加情報１３は、暗号化されていない。

【００６６】

記憶部３１２は、制御部３１０が実行する制御プログラムや、制御部３１０が処理する各種のデータを記憶する。例えば、記憶部３１２は、決済データＤｃの決済サーバ３００のサーバＩＤを記憶する。また、記憶部３１２は、決済データＤｃの付加情報１３に関する情報を記憶する。

Petitioner Exhibit 1002-0926

入力部３１４は、決済サーバ３００の利用者の操作を受け付け、入力信号を制御部３１０に出力する。入力部３１４は、例えば、キーボード、マウス等で構成されうるが、タッチパネルで構成されても良い。

【００６８】

表示部３１６は、表示画面に各種の画像や情報を表示する。表示部３１６は、例えば、携帯端末２００から受信した決済データＤｂに関する情報を表示する。

【００６９】

無線通信部３１８は、ネットワーク４００を介して携帯端末２００と無線通信を行い、決済データの送受信を行う。具体的には、無線通信部３１８は、携帯端末２００から図５に示す決済データＤｂを受信し、決済処理後に携帯端末２００に図６に示す決済データＤｃを送信する。

【００７０】

上述した構成を有する決済サーバ３００は、決済端末１００において生成された決済データＤａに基づく決済データＤｂを、ネットワーク４００を介して携帯端末２００から受信し、受信した決済データＤｂを復号化して、決済処理を実行する。また、決済サーバ３００は、決済後に暗号化された残高情報を少なくとも含む決済データＤｄを、ネットワーク４００を介して携帯端末２００へ送信する。これにより、決済端末１００にネットワークデバイスを設けなくても、携帯端末２００を経由して決済端末１００と決済サーバ３００との間で決済データの送受信ができる。また、暗号化された決済データが送受信されるので、携帯端末２００において、暗号化された情報（例えば、端末ＩＤや決済金額）の改ざんを防止できる。

【００７１】

（１－５．決済処理システムによる決済処理の流れ）

図９を参照しながら、第１の実施形態に係る決済処理システム１０による決済処理の流れについて説明する。図９は、第１の実施形態に係る決済処理システム１０による決済処理の流れを示すフローチャートである。

【００７２】

本決済処理は、決済端末１００、携帯端末２００、決済サーバ３００の制御部１１０、２１０、３１０が、記憶部１１２、２１２、３１２に記憶されたプログラムを実行することにより、実現される。

【００７３】

図９に示すフローチャートは、決済端末１００の入力部１１４が、例えば店舗の店員によって入力された決済金額を受け付けるところから開始される（ステップＳ１０２）。次に、決済端末１００の決済データ生成部１２０は、図３に示す決済データＤａを生成する（ステップＳ１０４）。

【００７４】

ここで、決済データＤａは、図３に示すように、決済端末１００の端末ＩＤと、入力部１１４が受け付けた決済金額と、決済端末１００が処理可能なサービスＩＤリストと、付加情報Ｉ１と、を含む。なお、決済データＤａの決済金額、及び端末ＩＤのデータは、決済端末１００により署名されると共に、記憶部１１２に記憶されたサーバ鍵で暗号化される。

【００７５】

次に、ユーザが携帯端末２００を決済端末１００にかざすと、近距離通信部１１８は、決済データ生成部１２０により生成された決済データＤａを携帯端末２００に送信する（ステップＳ１０６）。

【００７６】

携帯端末２００の近距離通信部２１８は、決済端末１００から送信された決済データＤａを受信する。次に、表示部２１６は、受信した決済データＤａに基づいて、サービスリスト及び決済金額を表示する（ステップＳ１０８）。なお、表示部

Petitioner Exhibit 1002-0927

スＩＤのリストである。携帯端末２００のユーザは、表示されたサービスリストの中から、所望のサービスを選択できる。また、携帯端末２００は、決済データＤａの付加情報Ｉ１に対応する処理を行なっても良い。

【００７７】

次に、決済データ処理部２２２は、選択画面においてユーザにより選択されたサービスに対応する、図５に示す決済データＤｂを生成する（ステップＳ１１０）。決済データ処理部２２２は、決済データＤａのサービスＩＤリストを、ユーザが選択したサービスＩＤに置き換えると共に、付加情報Ｉ２を付加することで、決済データＤｂを生成する。

【００７８】

次に、無線通信部２２０は、決済データ処理部２２２により生成された決済データＤｂを、ネットワーク４００を介して決済サーバ３００に送信する（ステップＳ１１２）。このように、本決済処理においては、決済端末１００が生成した決済データが、携帯端末２００を経由して決済サーバ３００へ送信される。

【００７９】

決済サーバ３００の無線通信部３１８は、携帯端末２００から送信された決済データＤｂを受信する。次に、署名検証部３２０は、受信した決済データＤｂに付された決済端末１００の署名を検証する（ステップＳ１１４）。これにより、決済サーバ３００は、決済端末１００がサービス登録された装置であることを確認する。

【００８０】

次に、決済処理部３２２は、ユーザが選択したサービスＩＤ（決済データＤｂのサービスＩＤ）に対応するバリューに対して、決済処理を実行する（ステップＳ１１６）。すなわち、決済処理部３１６は、サービスＩＤに対応するデータベースに格納されたバリューに対して、決済処理を実行する。この際、決済処理部３２２は、決済データＤｂ中の携帯端末サーバデータ（図１４参照）を用いて、ユーザ毎のデータベースによる決済も可能である。また、決済サーバ３００は、決済データＤｂの付加情報Ｉ２に対応する処理を行なっても良い。

【００８１】

次に、決済データ処理部３２４は、決済データＤｂに基づいて、図６に示す決済データＤｃを生成する（ステップＳ１１８）。決済データＤｃは、決済端末１００の装置ＩＤと、決済金額と、サービスＩＤと、サーバ３００のサーバＩＤと、残高と、付加情報Ｉ３と、を含む。すなわち、決済データ処理部３２４は、決済データＤｂに、決済サーバ３００のサーバＩＤと、残高と、付加情報Ｉ３と、を付加することで、決済データＤｃを生成する。なお、決済データＤｃの装置ＩＤ、決済金額、サービスＩＤ、サーバサーバＩＤ、及び残高は、決済サーバ３００により署名されると共に、記憶部３１２に記憶された決済端末１００の端末鍵で暗号化される。

【００８２】

次に、無線通信部３１８は、決済データ処理部３２４により生成された決済データＤｃを携帯端末２００に送信する（ステップＳ１２０）。このように、本決済処理においては、決済サーバ３００が生成した決済データＤｃが決済端末１００に直接送信されるのではなく、携帯端末２００を経由して送信される。

【００８３】

携帯端末２００は、決済サーバ３００から送信された決済データＤｃを無線通信部２２０により受信する。携帯端末２００は、決済データＤｃの付加情報Ｉ３に対応する処理を行なっても良い。次に、決済データ処理部２２２は、受信した決済データＤｃに基づいて、図７に示す決済データＤｄを生成する（ステップＳ１２２）。決済データ処理部２２２は、決済データＤｃに付加情報Ｉ４を付与することで、決済データＤｄを生成する。

【００８４】

次に、近距離通信部２１８は、決済データ処理部２１６により生成された決済データＤｄを決済端末１００に送信する（ステップＳ１２４）。

Petitioner Exhibit 1002-0928

決済端末１００の近距離通信部１１８は、携帯端末２００から送信された決済データＤｄを受信する。次に、署名検証部１２２は、受信した決済データＤｄに付されたサーバ３００の署名を検証する（ステップＳ１２６）。これにより、決済端末１００は、決済処理が実行されたことを確認する。

【００８６】

次に、表示部１１６は、決済が完了したことを示す情報を表示する（ステップＳ１２８）。この際、決済端末１００は、決済に関するレシートを出力しても良い。また、決済端末１００は、決済データＤｄの付加情報Ｉ４に対応する処理を行なっても良い。

【００８７】

なお、携帯端末２００の表示部２１６も、決済が完了したことを示す情報を表示する（ステップＳ１３０）。これにより、携帯端末２００のユーザも決済が完了したことを把握できる。以上により、決済処理システム１０による決済処理が完了する。

【００８８】

（１－６．決済処理システムにおける認証関係）

図１０を参照しながら、第１の実施形態に係る決済処理システム１０における認証関係について説明する。図１０は、第１の実施形態に係る決済処理システム１０における認証関係を説明するための模式図である。

【００８９】

上述したように、決済端末１００と携帯端末２００は近距離通信を行うので、携帯端末２００は、決済端末１００の近傍に位置する。このように携帯端末２００が決済端末１００の近くに位置することで、決済端末１００のサービス提供者側は、携帯端末２００を物理的に認証できる。

【００９０】

また、携帯端末２００は、決済サーバ３００に対して携帯端末２００のＩＤ等の情報を送信することで、決済サーバ３００は、ＩＤ情報等に基づいて認証できる。なお、携帯端末２００のＩＤ等の情報は、別のセキュリティが確保されている通信路で決済サーバ３００に送信される。これにより、決済サーバ３００の事業者側は、携帯端末２００のユーザが支払者であるか否かを確認できる。

【００９１】

決済端末１００と決済サーバ３００との間の認証関係については、まず、決済端末１００が、携帯端末２００を経由して端末ＩＤを含む決済データを決済サーバ３００に送信することで、決済サーバ３００は、端末ＩＤを照合することで、サービスの提供が認められている端末であるか否かを確認できる。一方で、決済サーバ３００が、決済後に携帯端末２００を経由してサーバＩＤを含む決済データを送信することで、決済端末１００は、決済結果の提供身元が正しいか否かを確認できる。

【００９２】

このように、決済処理システム１０によれば、携帯端末２００を経由して決済端末１００と決済サーバ３００との間で決済データを送受信しても、互いに認証ができるので、安全な決済方法を実現できる。

【００９３】

（１－７．まとめ）

上述したように、第１の実施形態に係る決済処理システム１０において、決済端末１００は、決済金額情報を暗号化した決済データＤａを生成し、生成された決済データＤａを近距離通信により携帯端末２００へ送信する。次に、携帯端末２００は、近距離通信により決済端末１００から受信した決済データＤａに基づく決済データＤｂを、ネットワーク４００を介して決済サーバ３００へ送信する。次に、決済サーバ３００は、ネットワーク４００を介して携帯端末２００から受信した決済データＤｂを復号化して、決済処理を実行し、決済後に暗号化された残高情報を少なくとも含む決済データＤｃを、ネットワーク４００を介して携帯端末２００へ送信する。そして、携帯端末２００は、近距離通信により決済端末１

Petitioner Exhibit 1002-0929