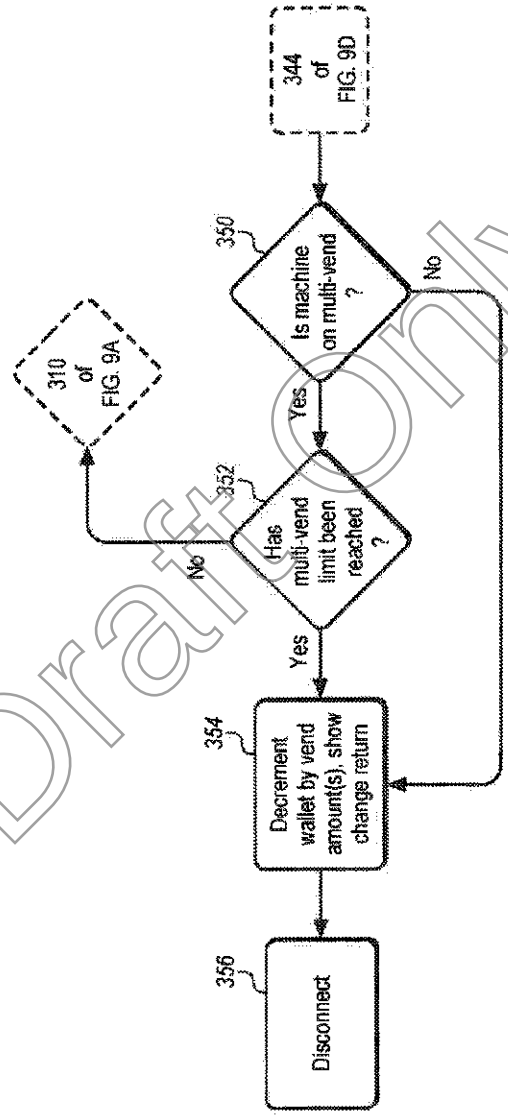


Figure 9E

Draft Only

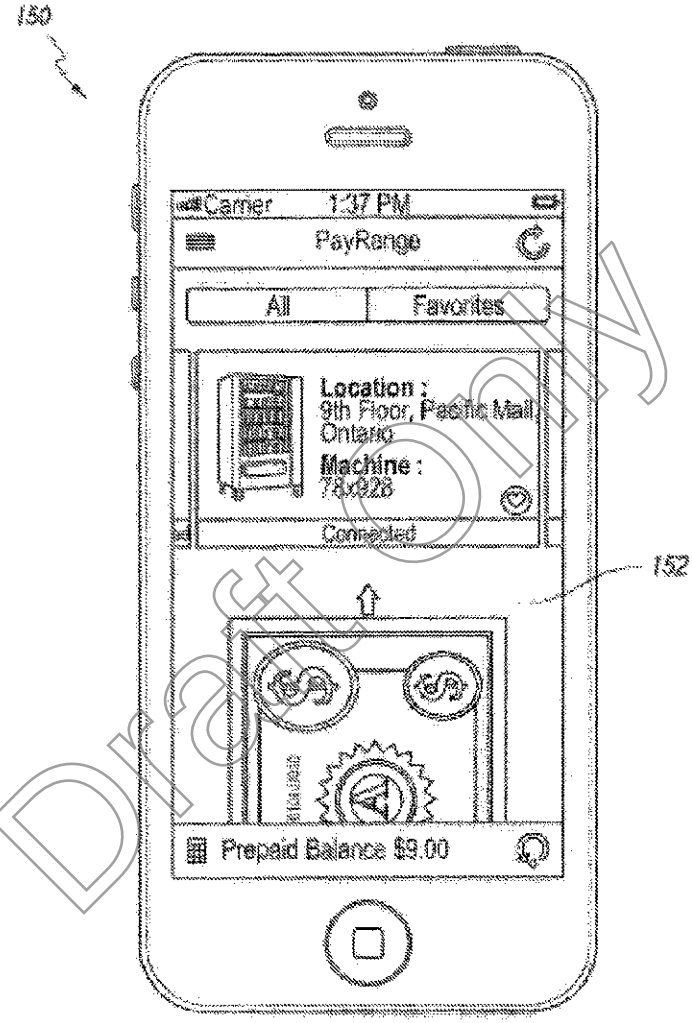


Figure 10A

Draft Only

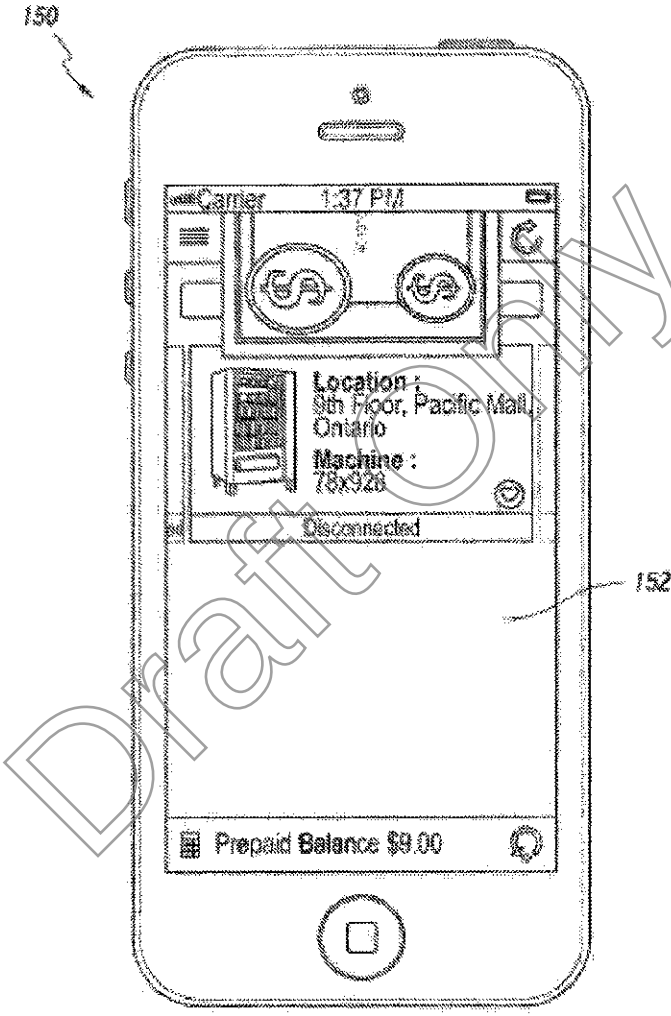


Figure 10B

Draft Only

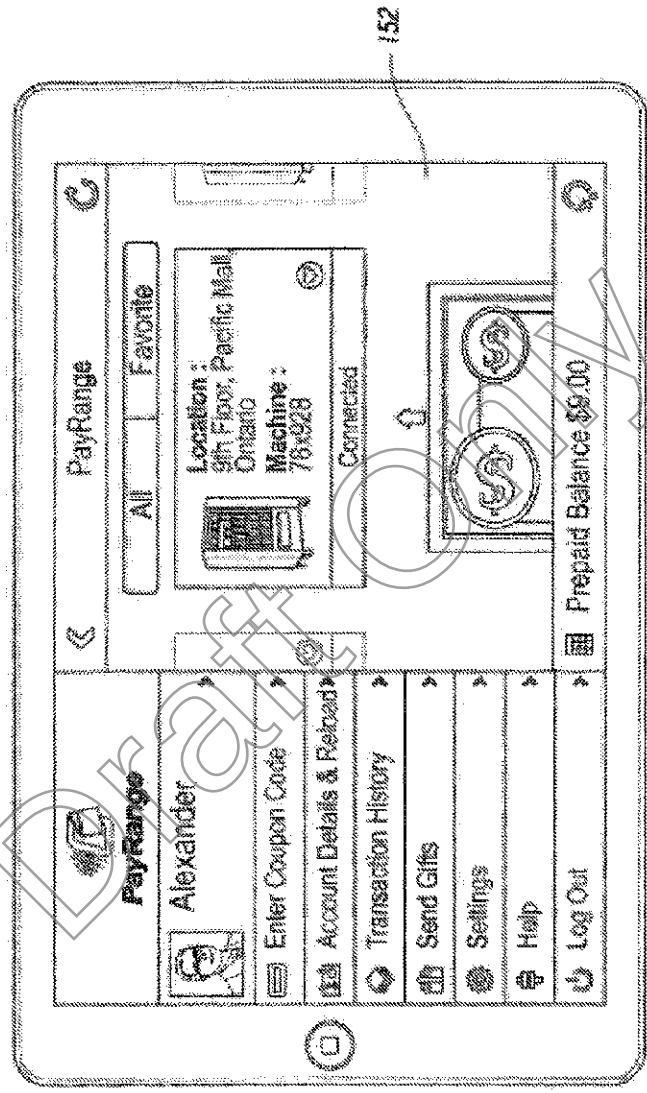


Figure 10C

Draft Only

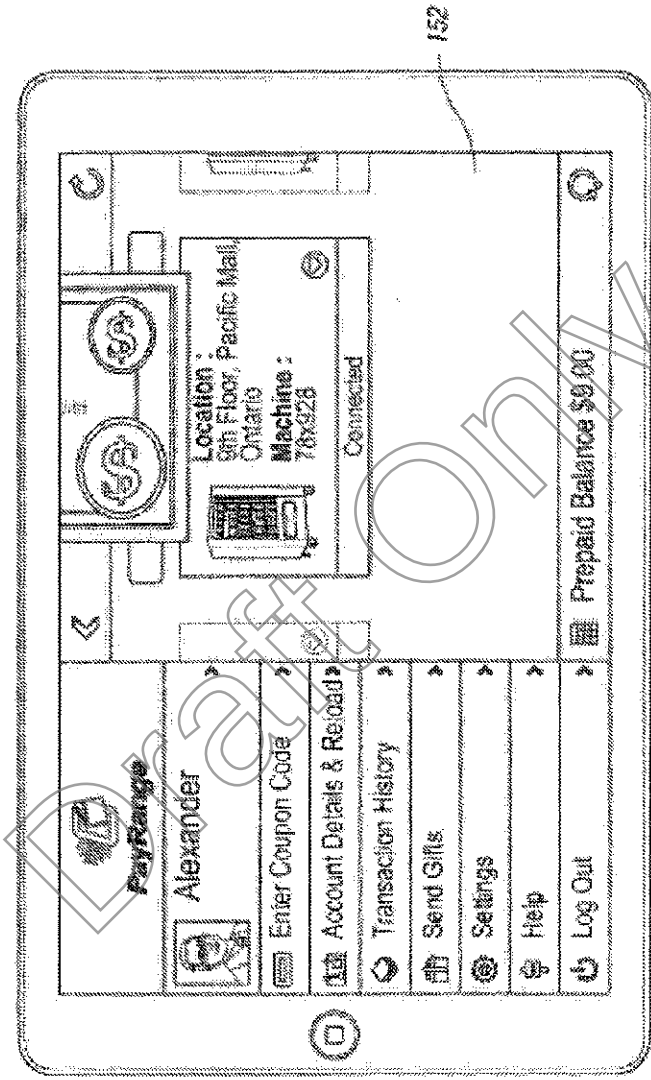


Figure 10D

Draft Only

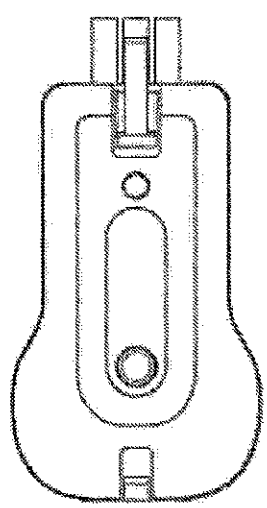


Figure 12

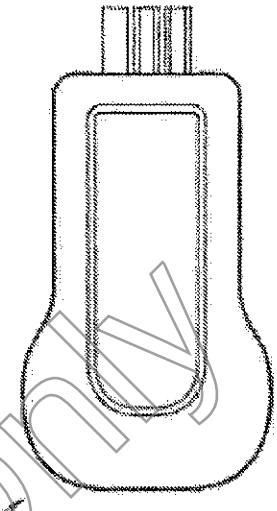


Figure 13

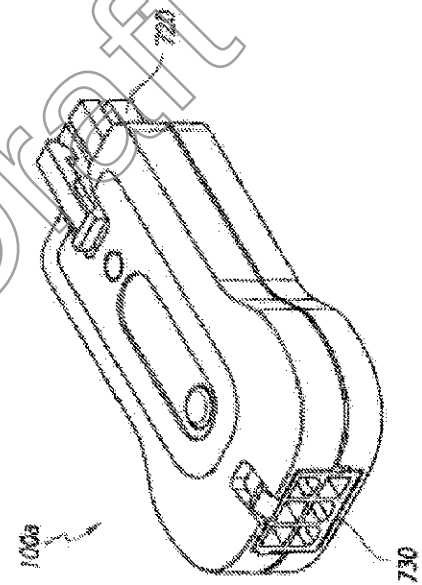


Figure 11

Draft Only

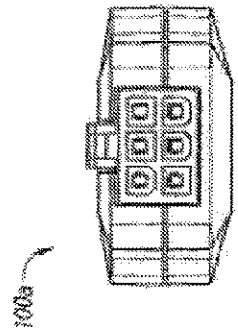


Figure 16

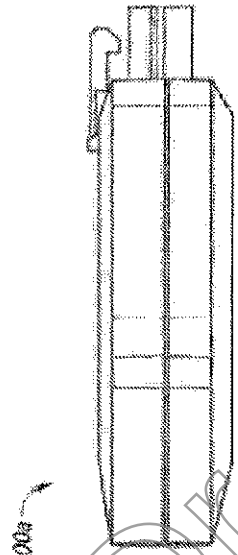


Figure 14

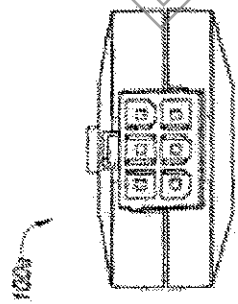


Figure 15

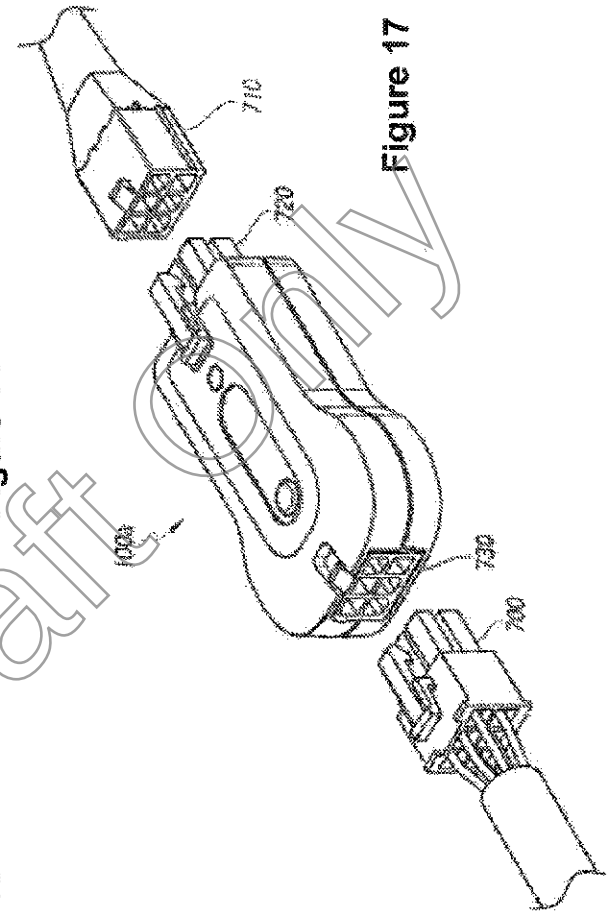


Figure 17

Draft Only

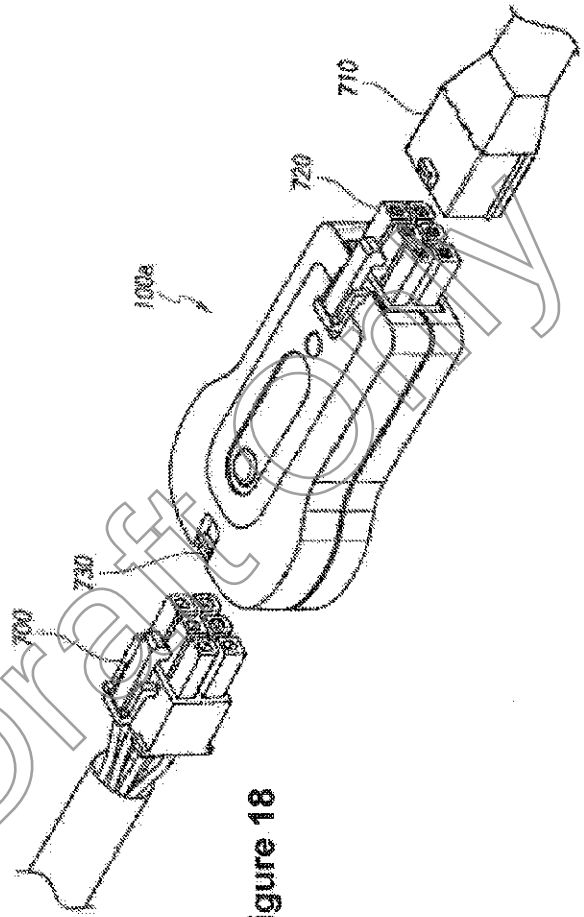


Figure 18

Draft Only

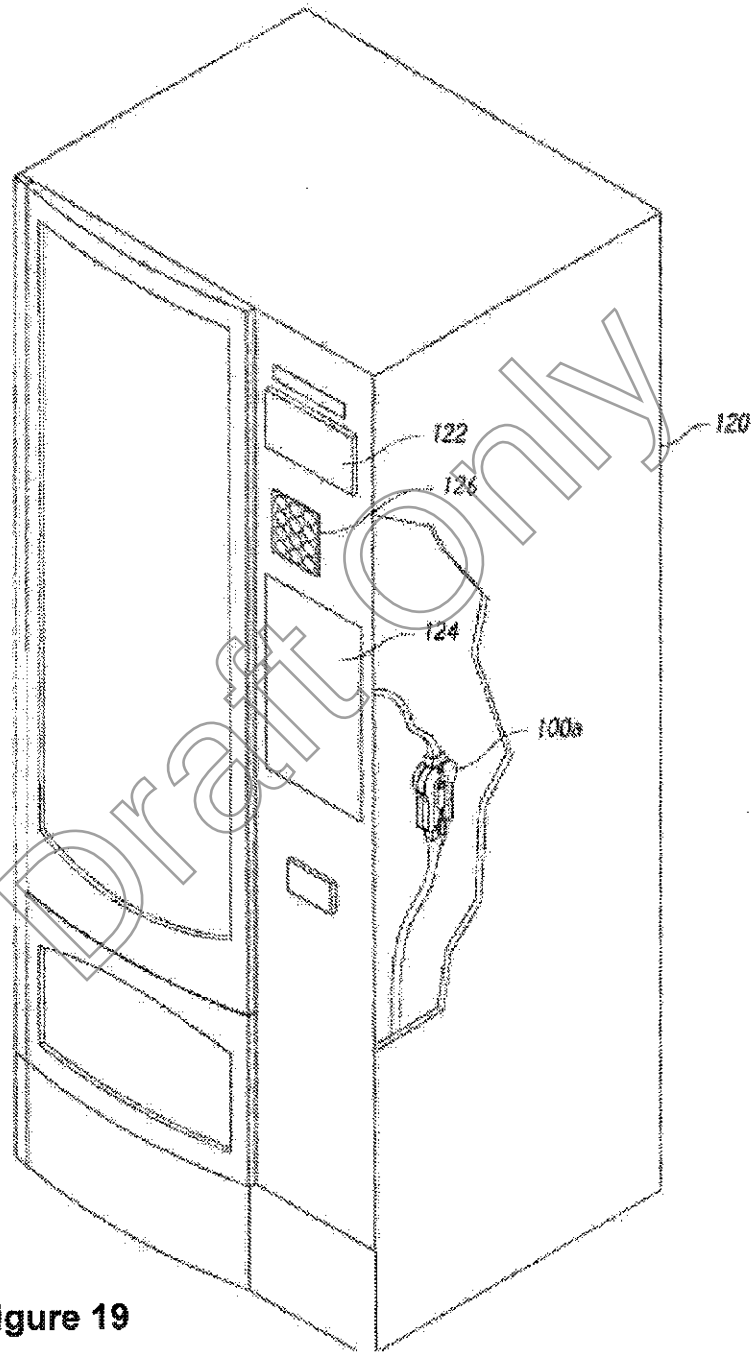
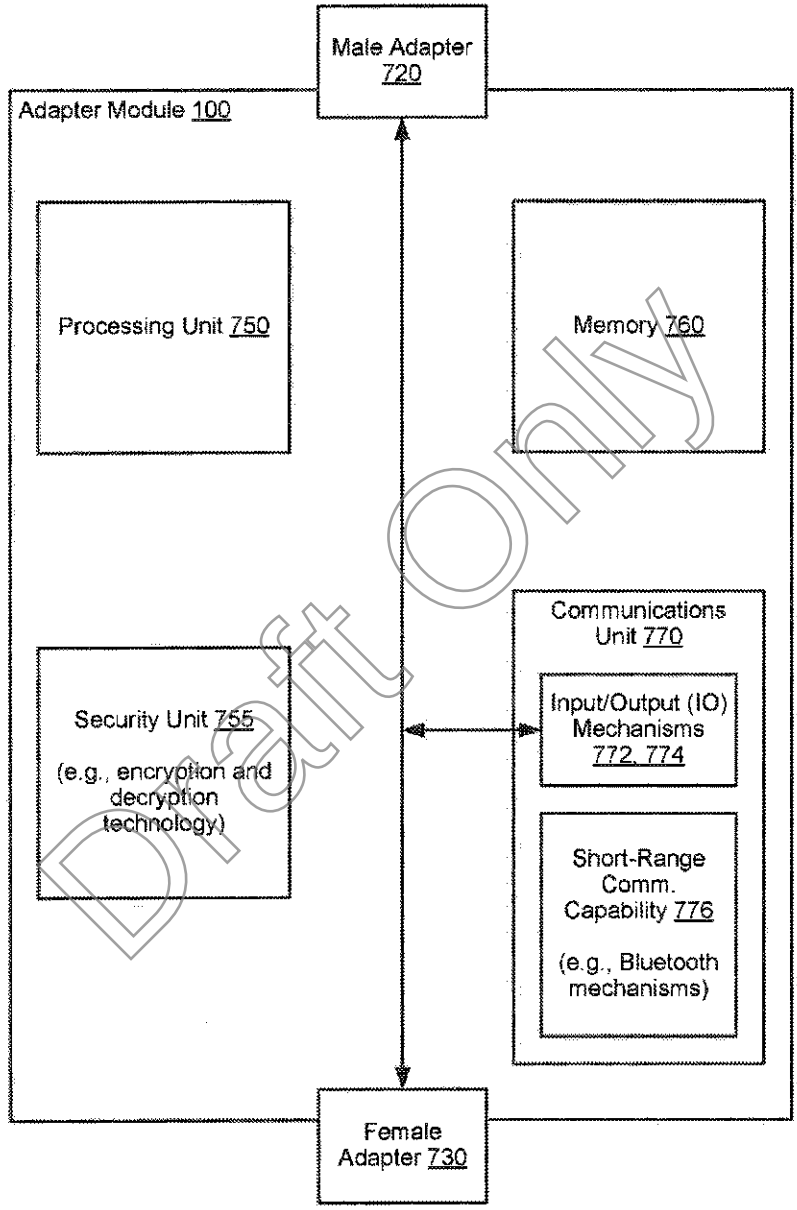


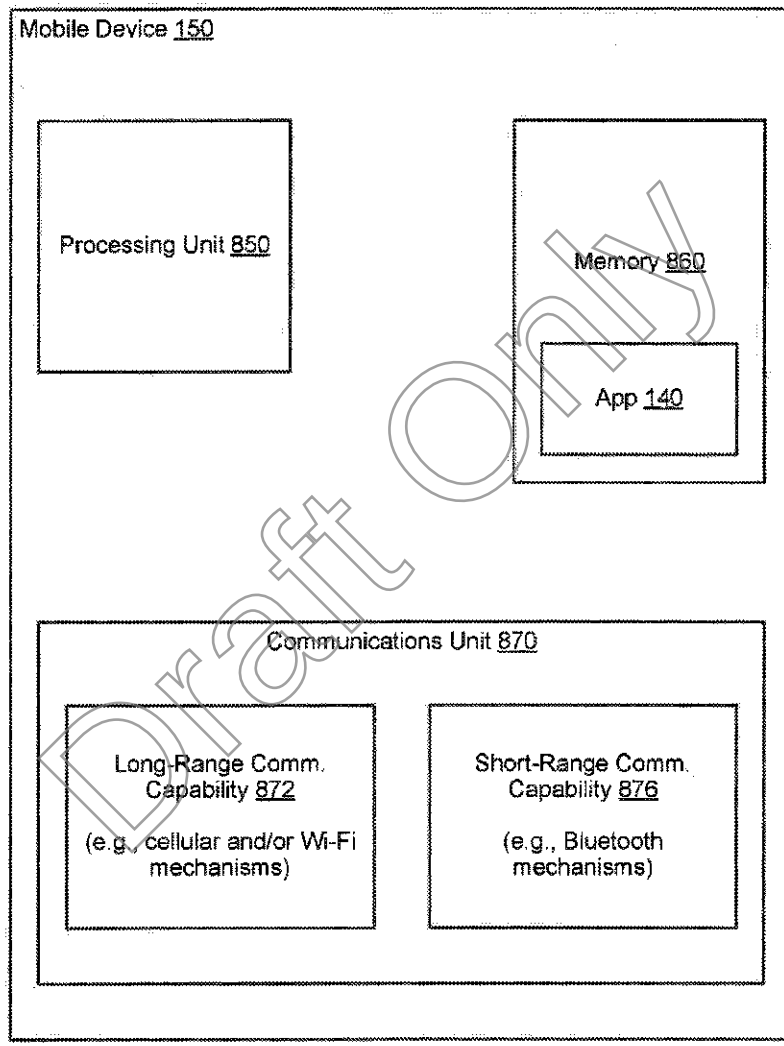
Figure 19

Draft Only



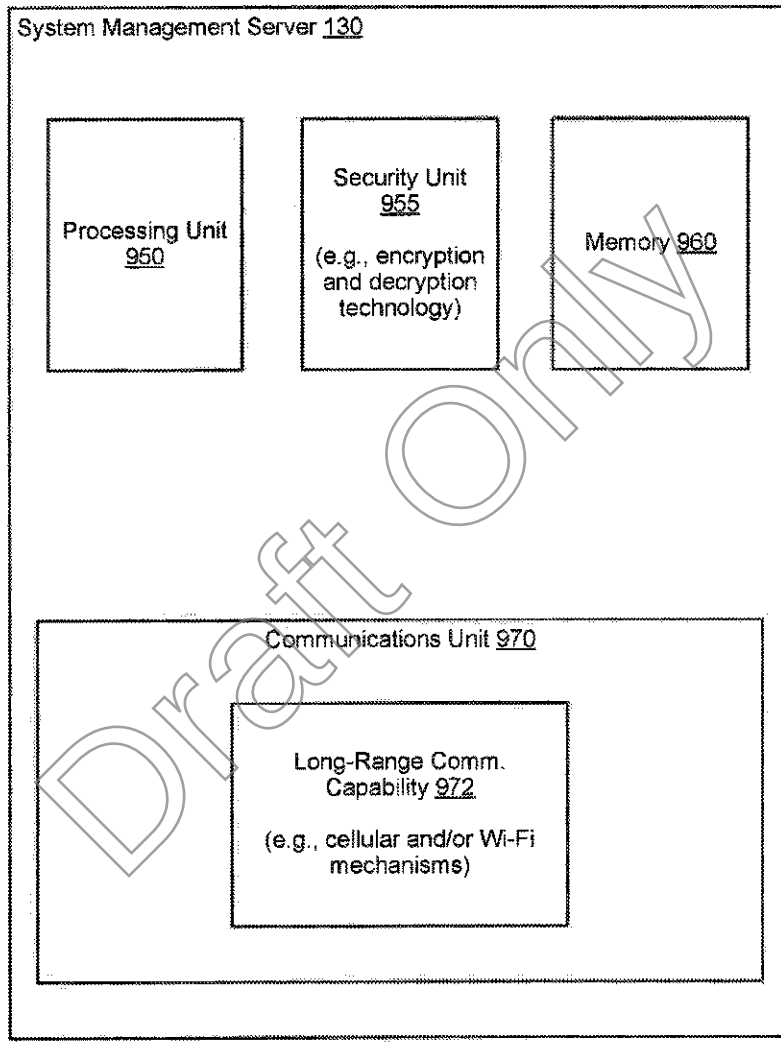
Draft Only

Figure 20



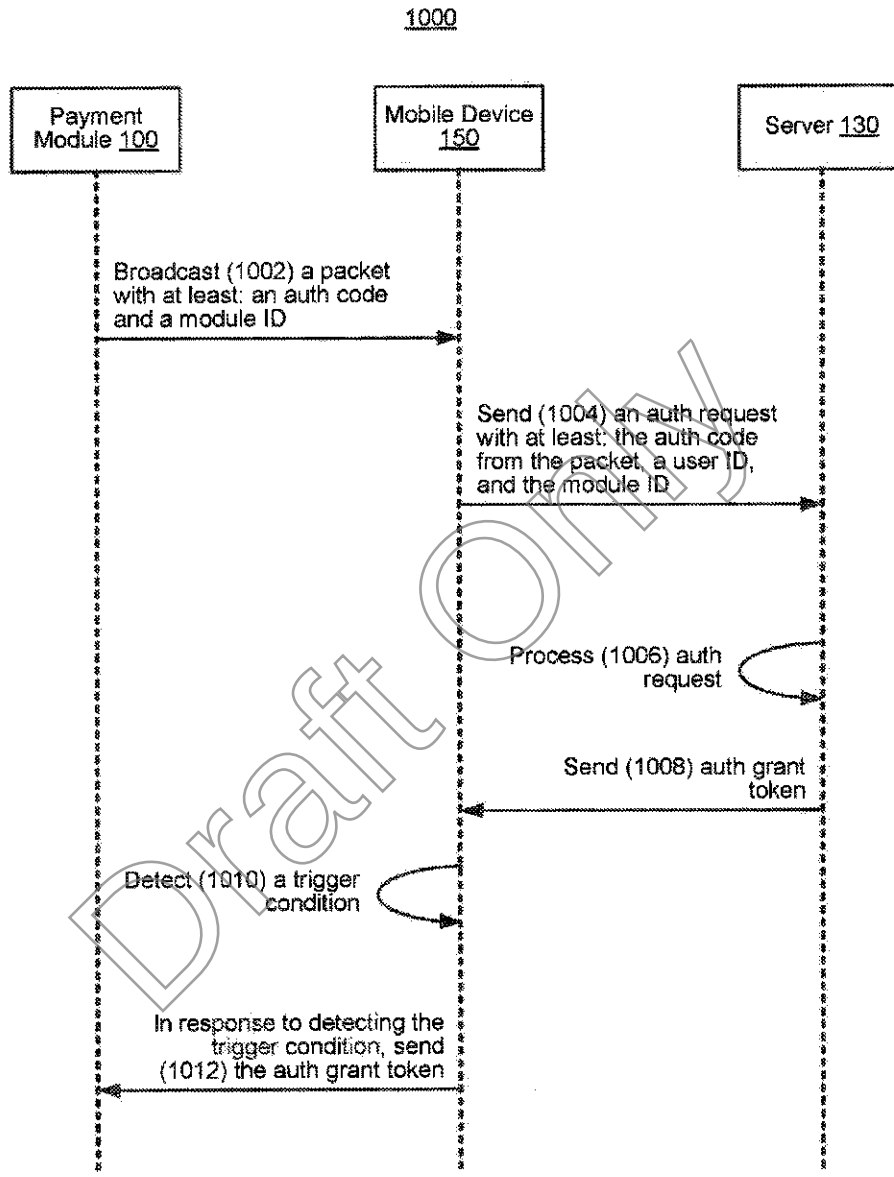
Draft Only

Figure 21



Draft Only

Figure 22



Draft Only

Figure 23

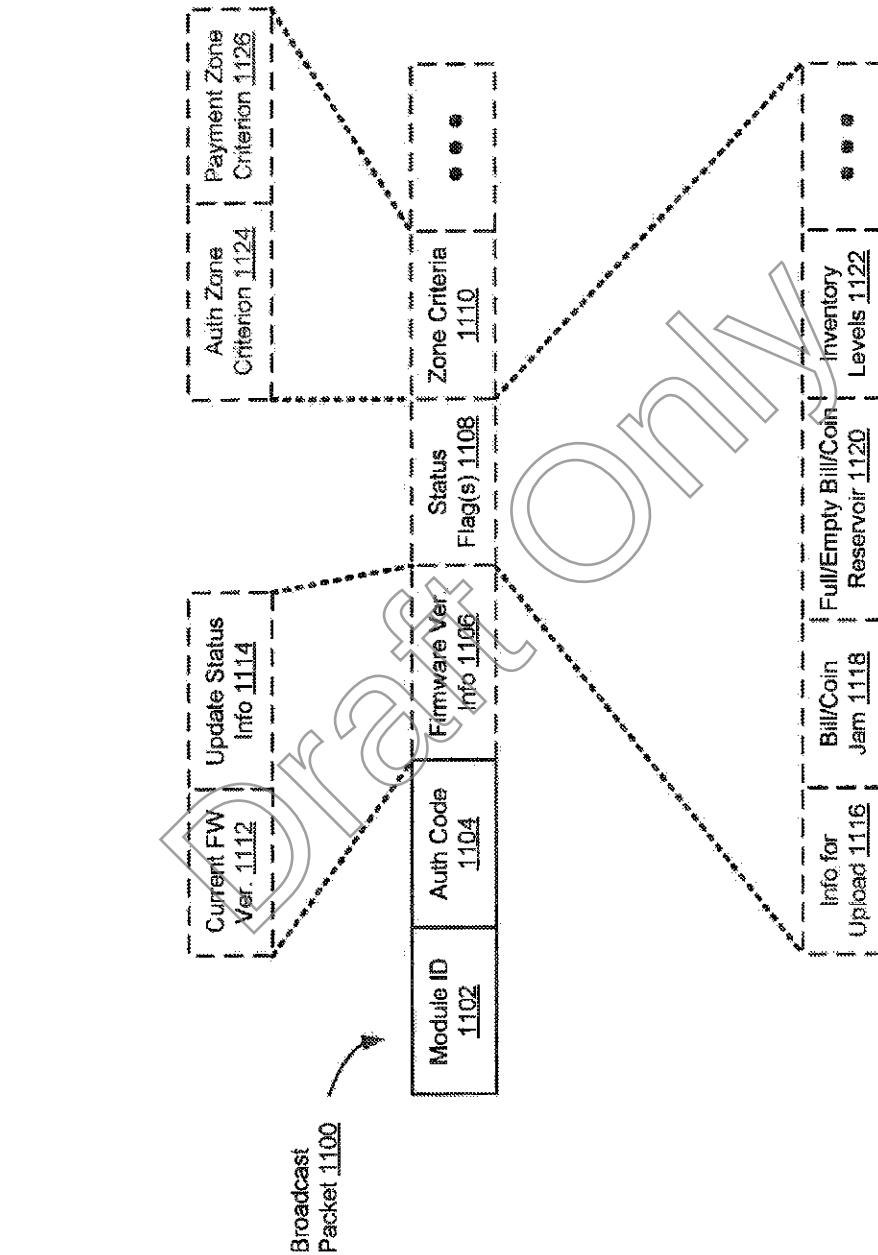


Figure 24A

Draft Only

Figure 24B

Figure 24C

Draft Only

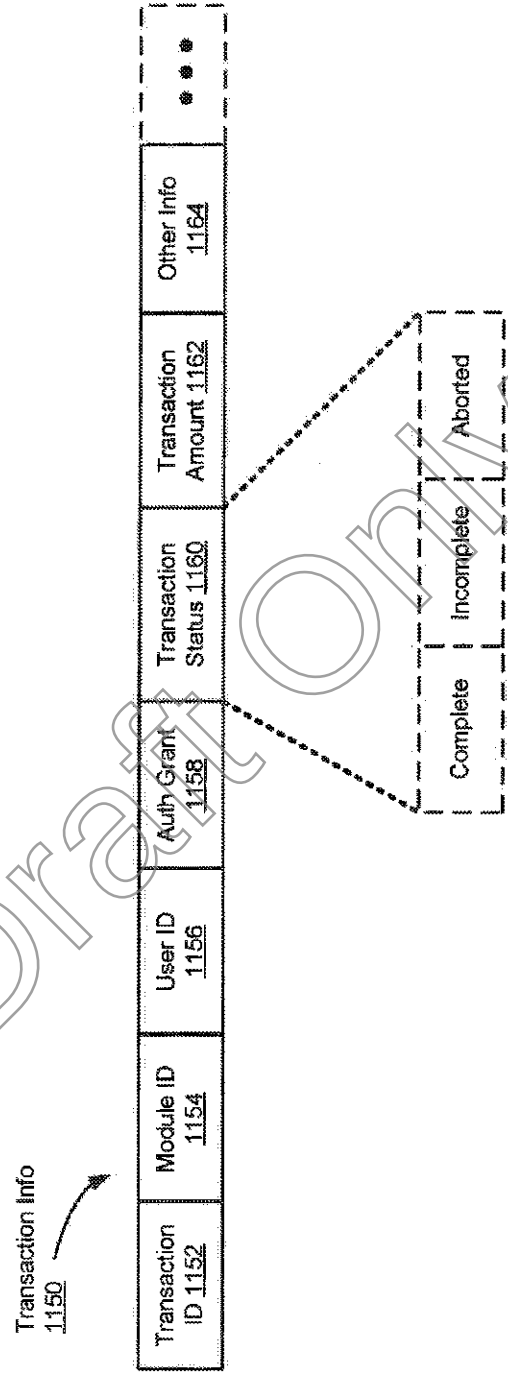
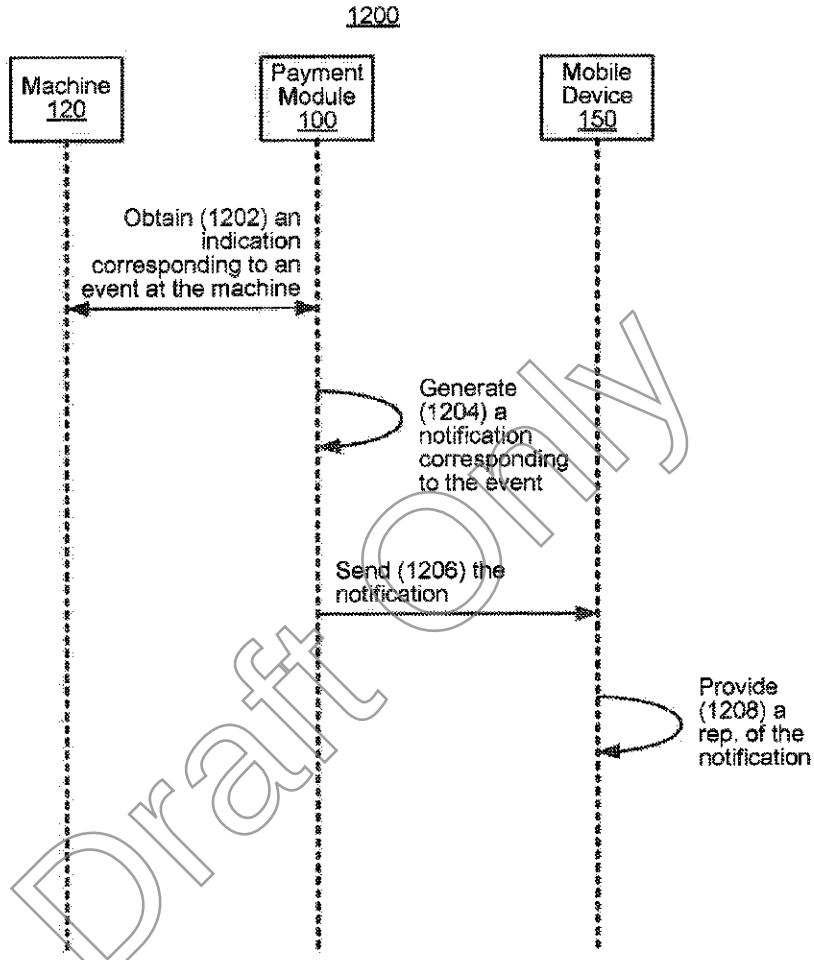


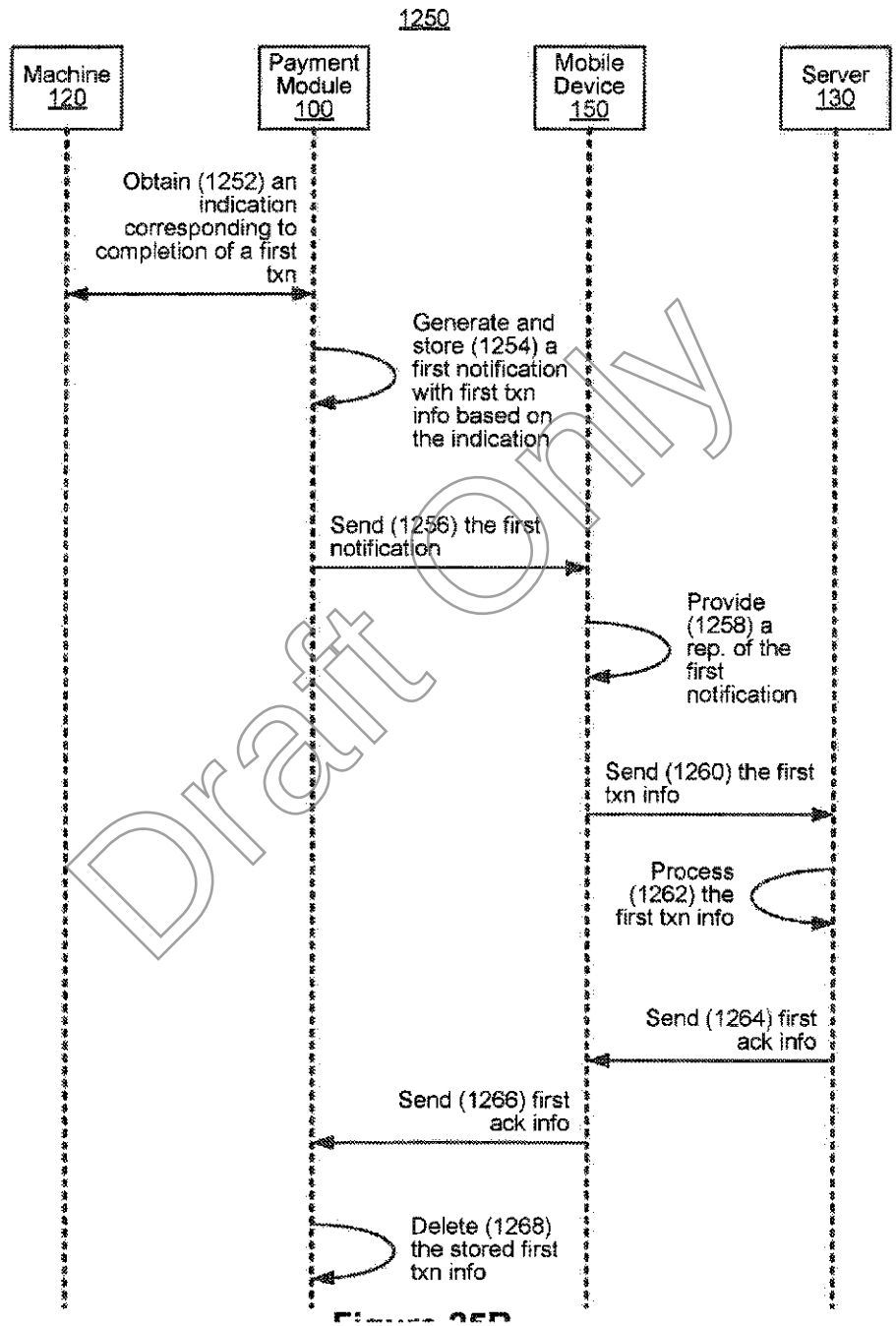
Figure 24D

Draft Only



Draft Only

Figure 25A


1250
Machine 120
Payment Module 100
Mobile Device 150
Server 130
Obtain (1252) an indication corresponding to completion of a first txn
Generate and store (1254) a first notification with first txn info based on the indication
Send (1256) the first notification
Provide (1258) a rep. of the first notification
Send (1260) the first txn info
Process (1262) the first txn info
Send (1264) first ack info
Send (1266) first ack info
Delete (1268) the stored first txn info

Draft Only

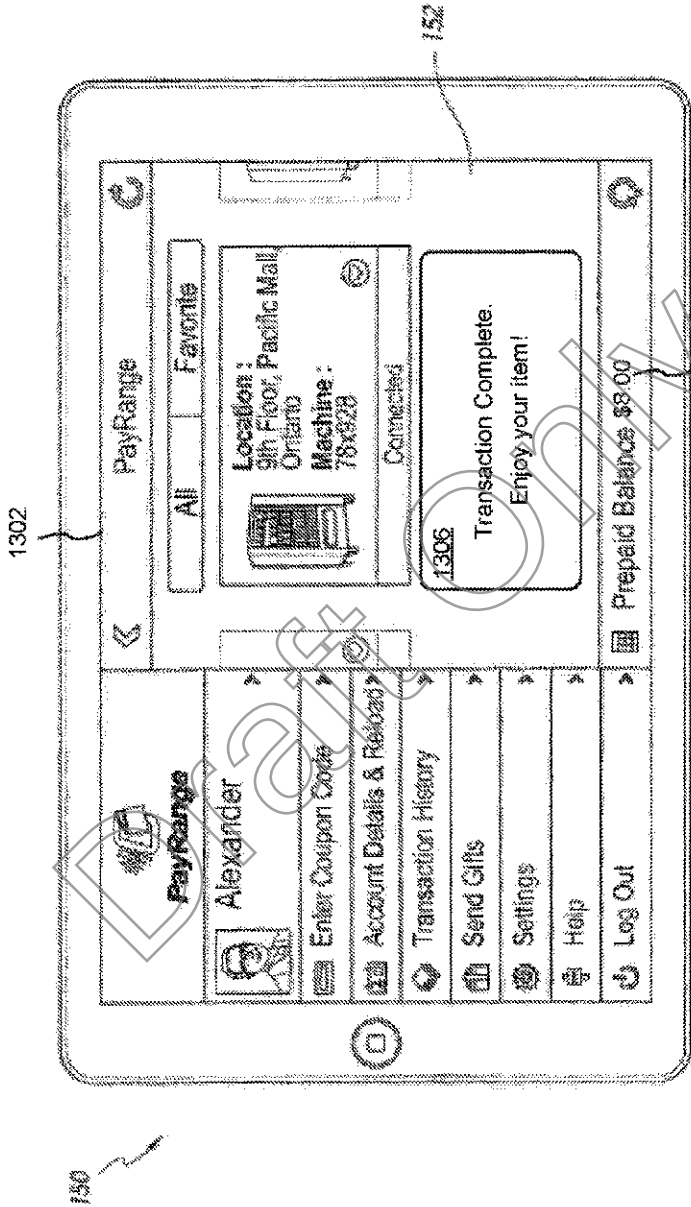


Figure 26A

Draft Only

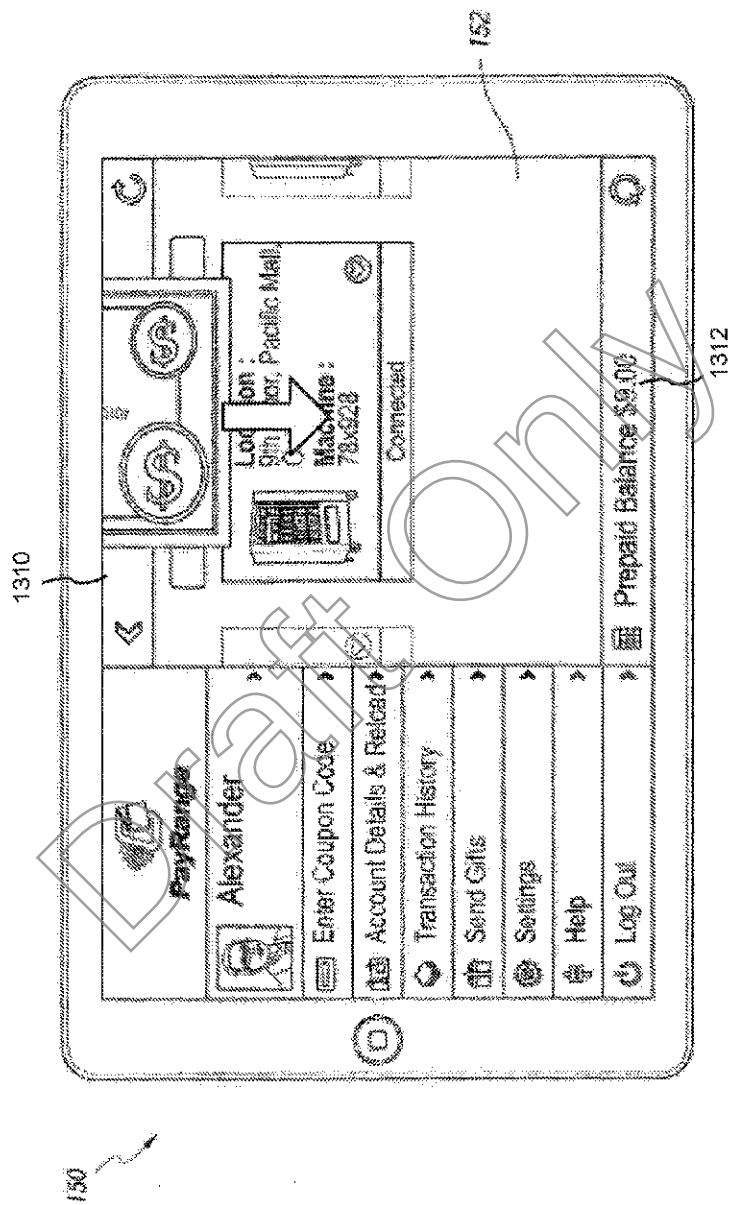


Figure 26B

Draft Only

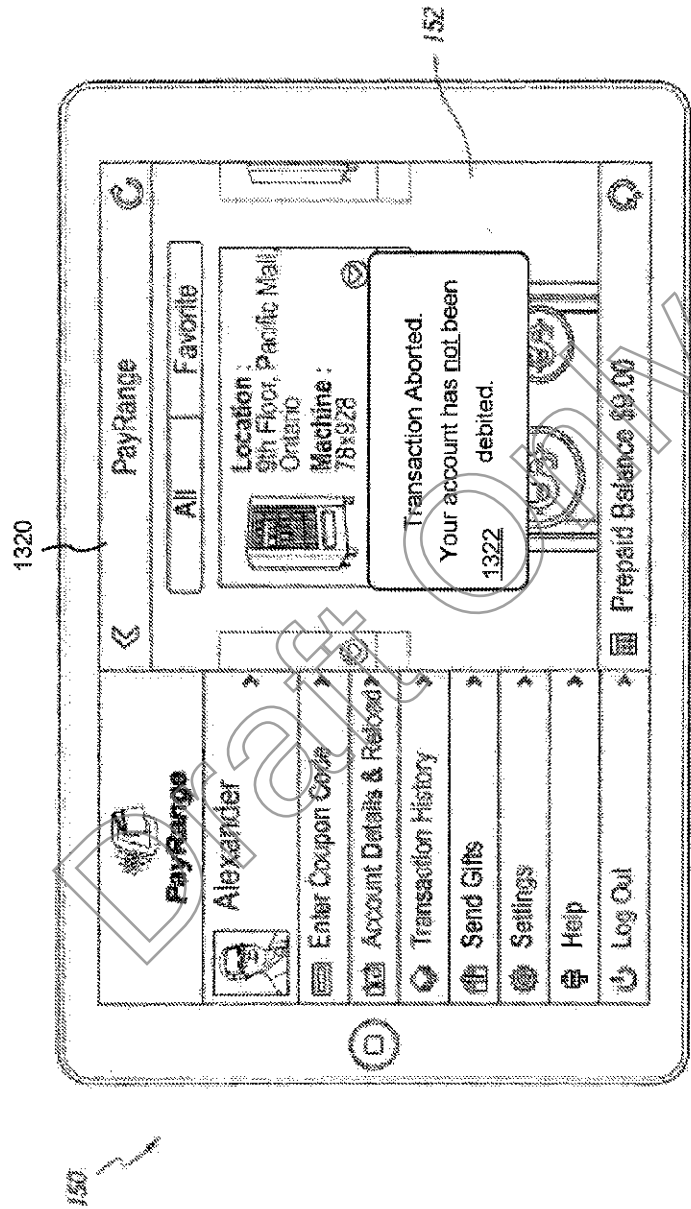


Figure 26C

Draft Only

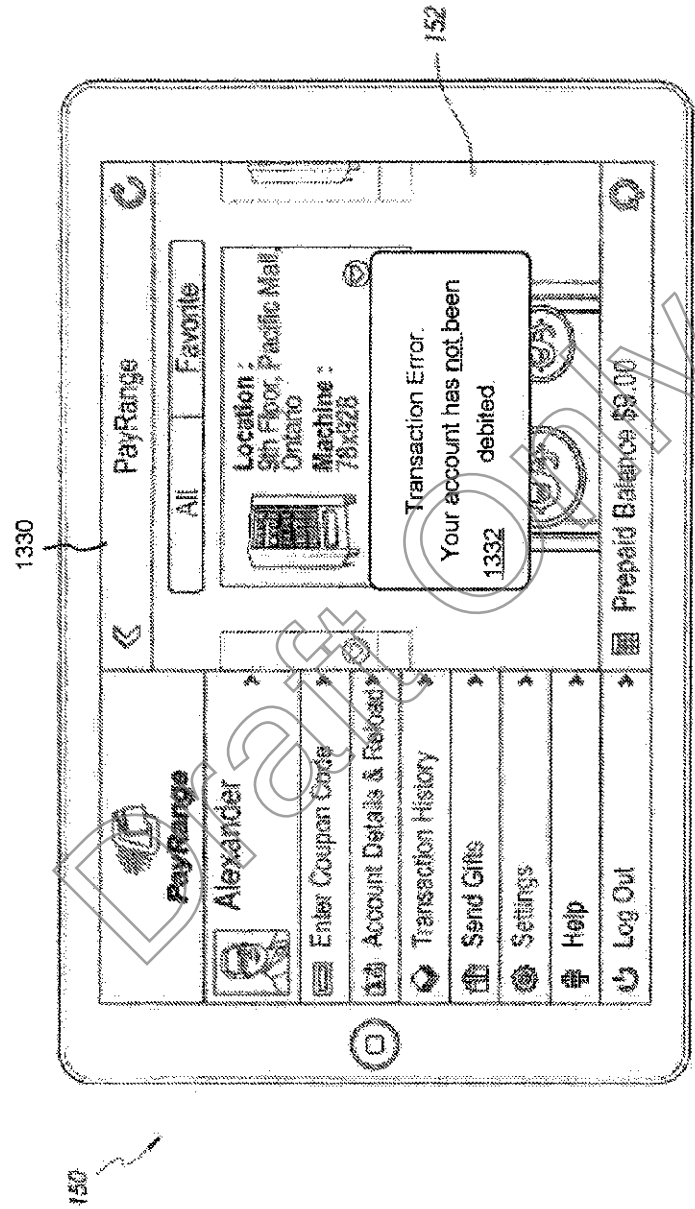


Figure 26D

Draft Only

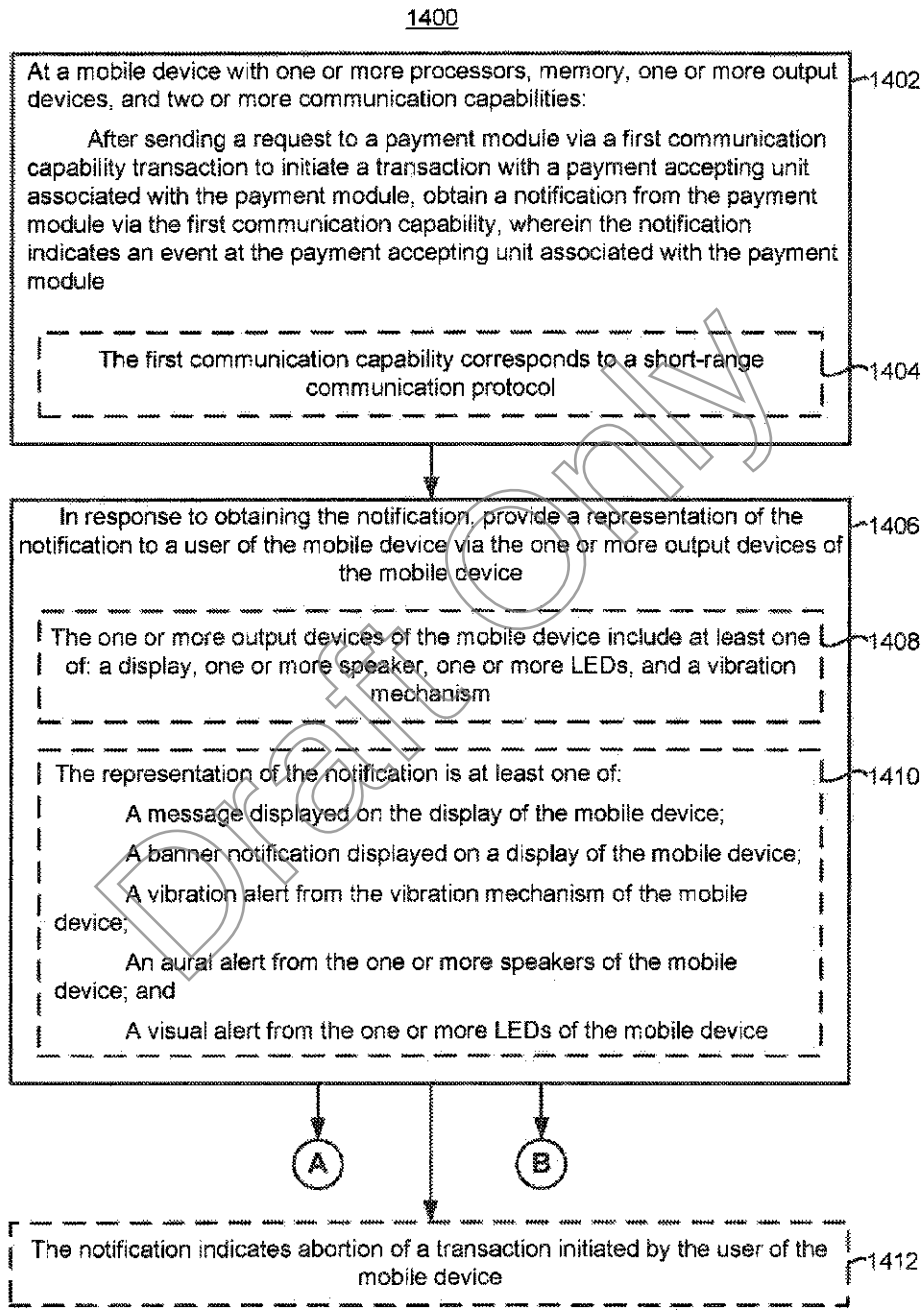
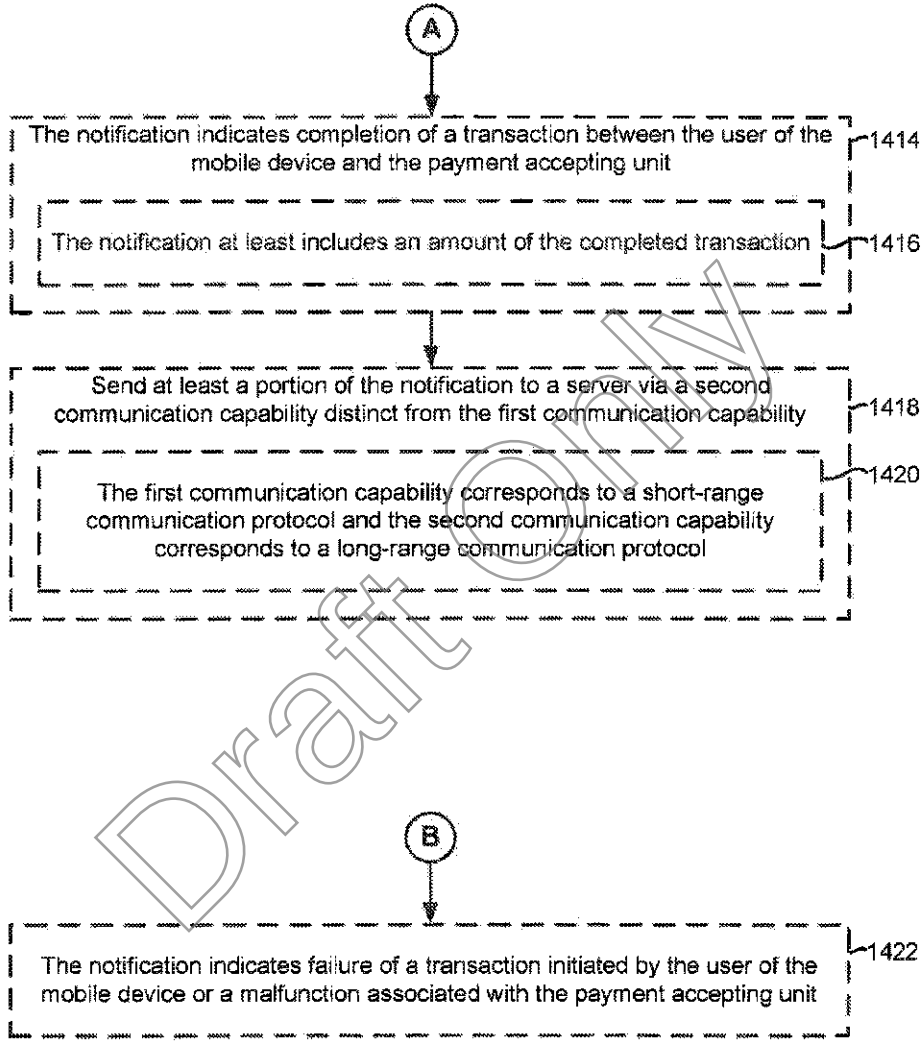


Figure 27A

Draft Only



Draft Only

Figure 27B

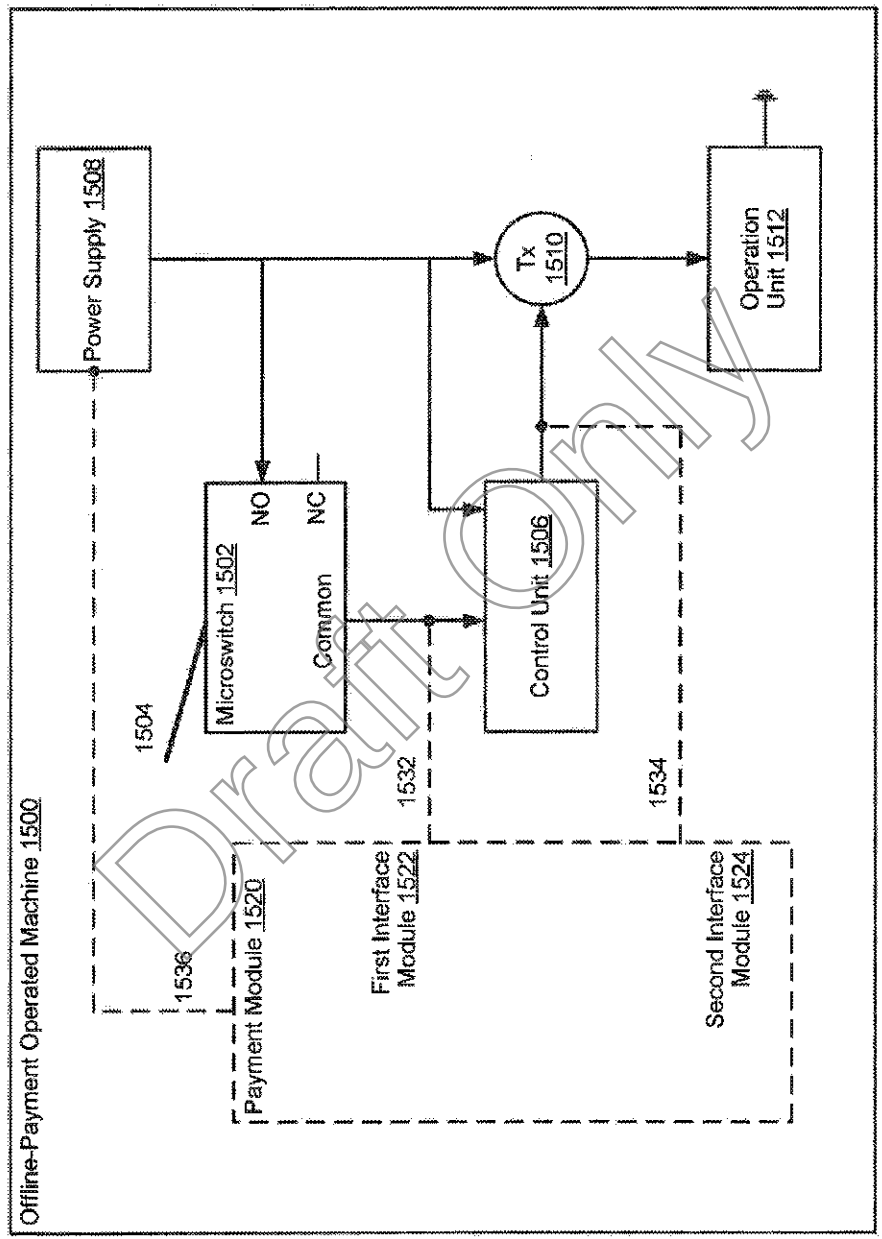


Figure 28A

Draft Only

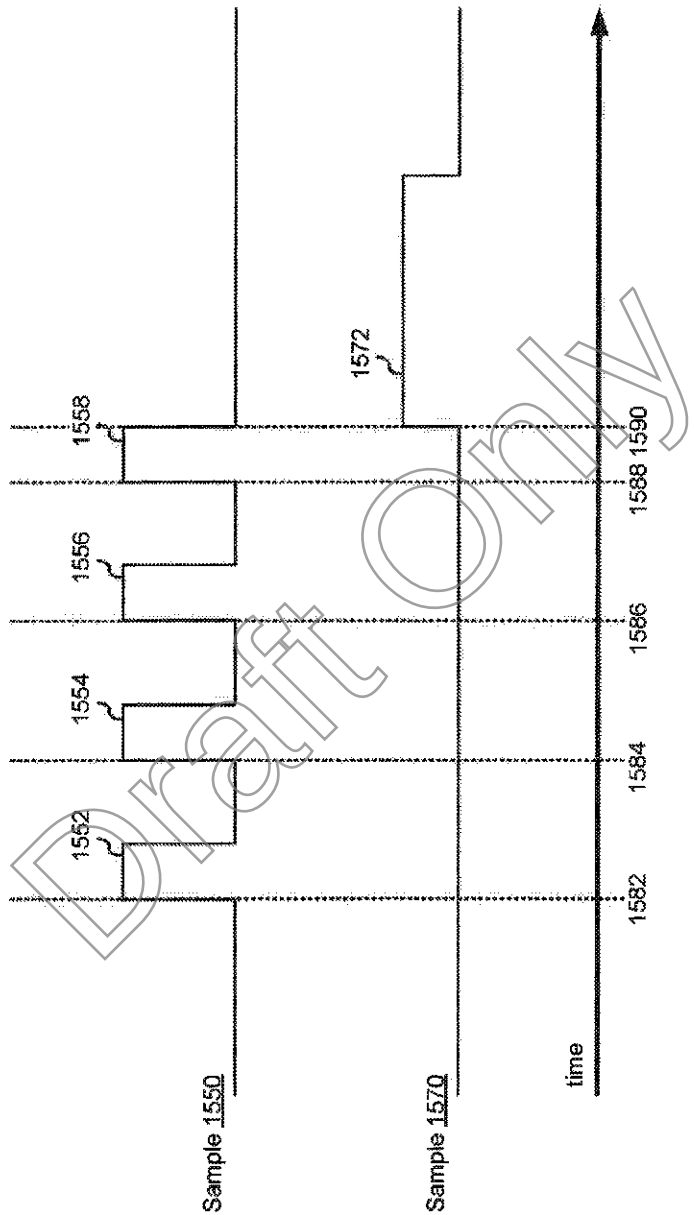


Figure 28B

Draft Only

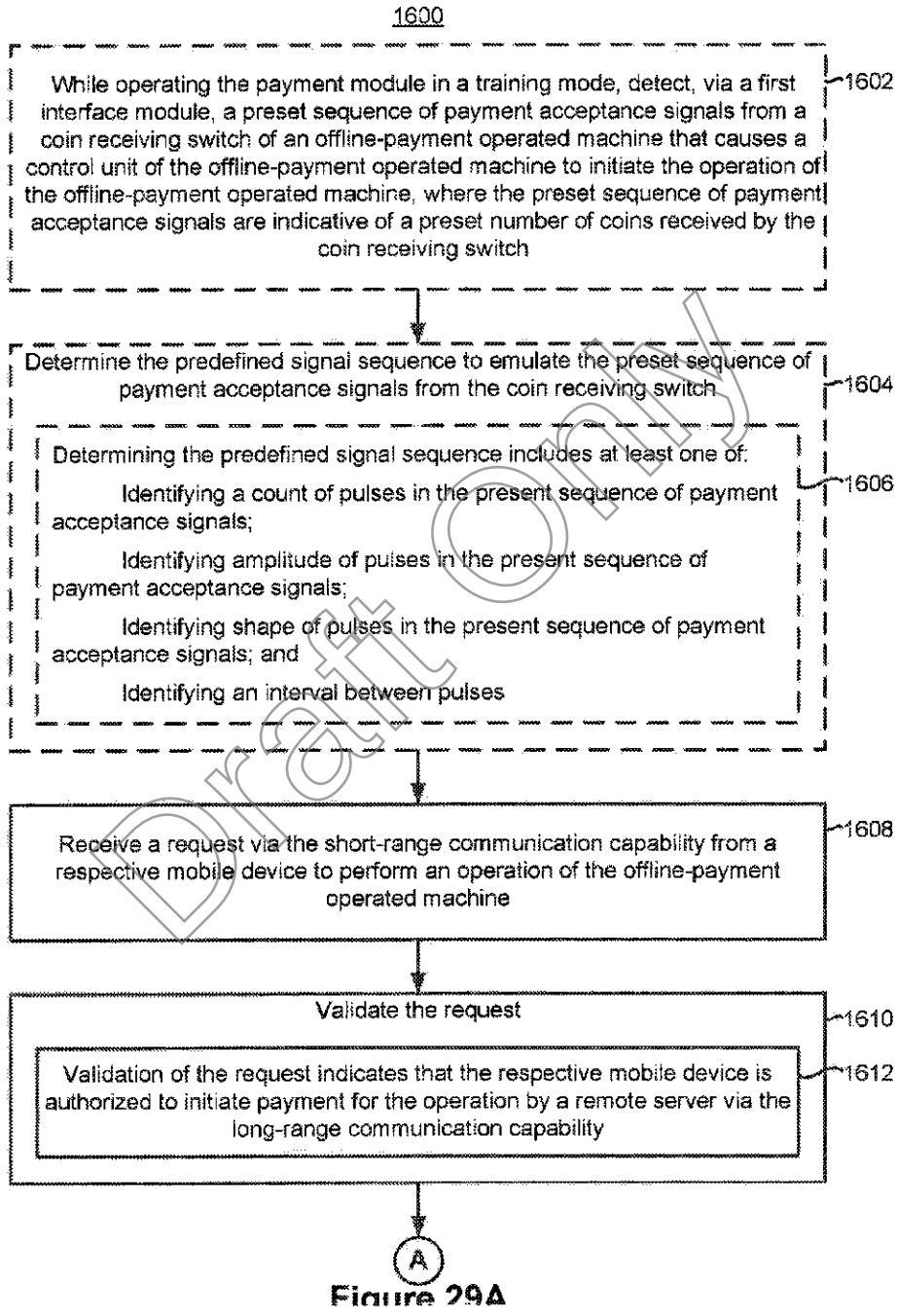
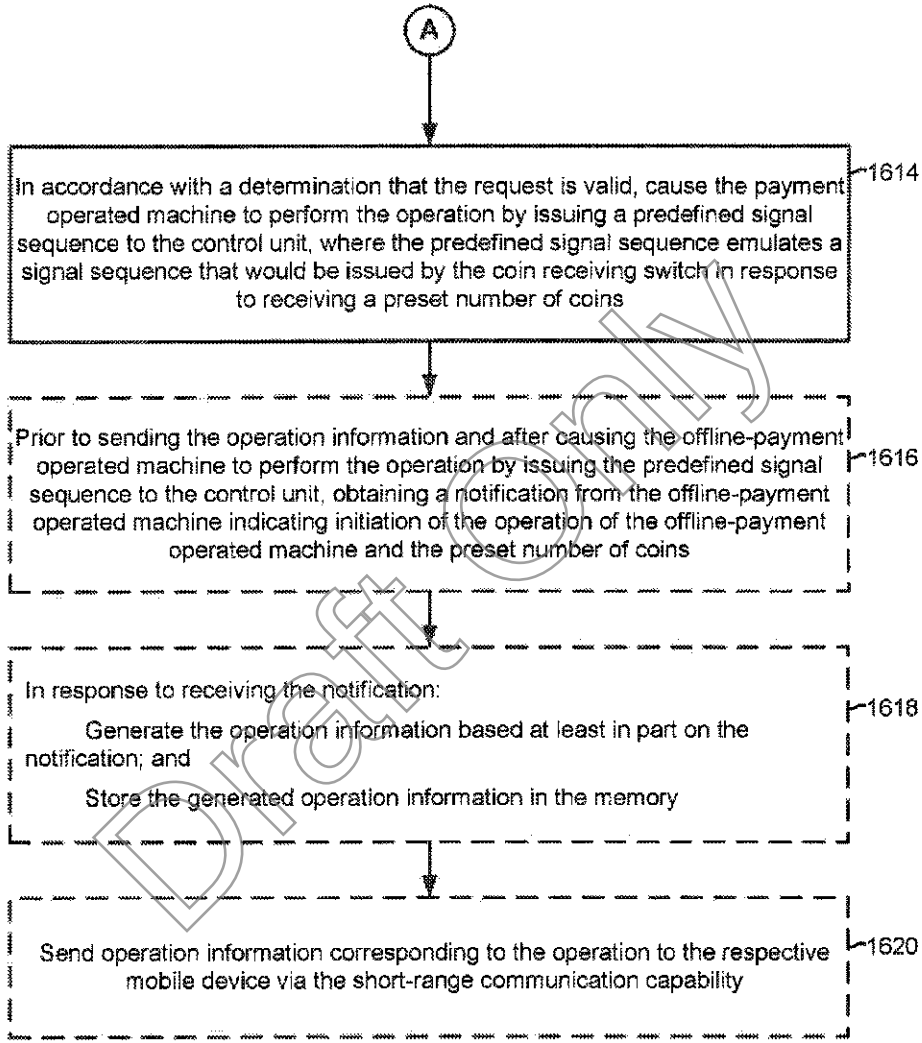


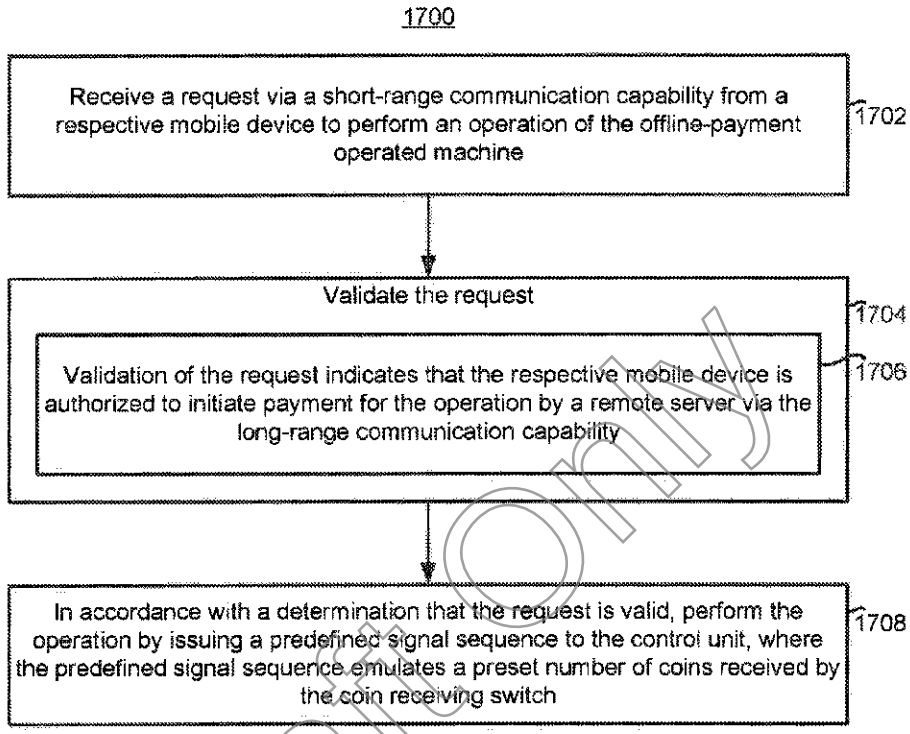
Figure 29A

Draft Only



Draft Only

Figure 29B



Draft Only

Figure 30

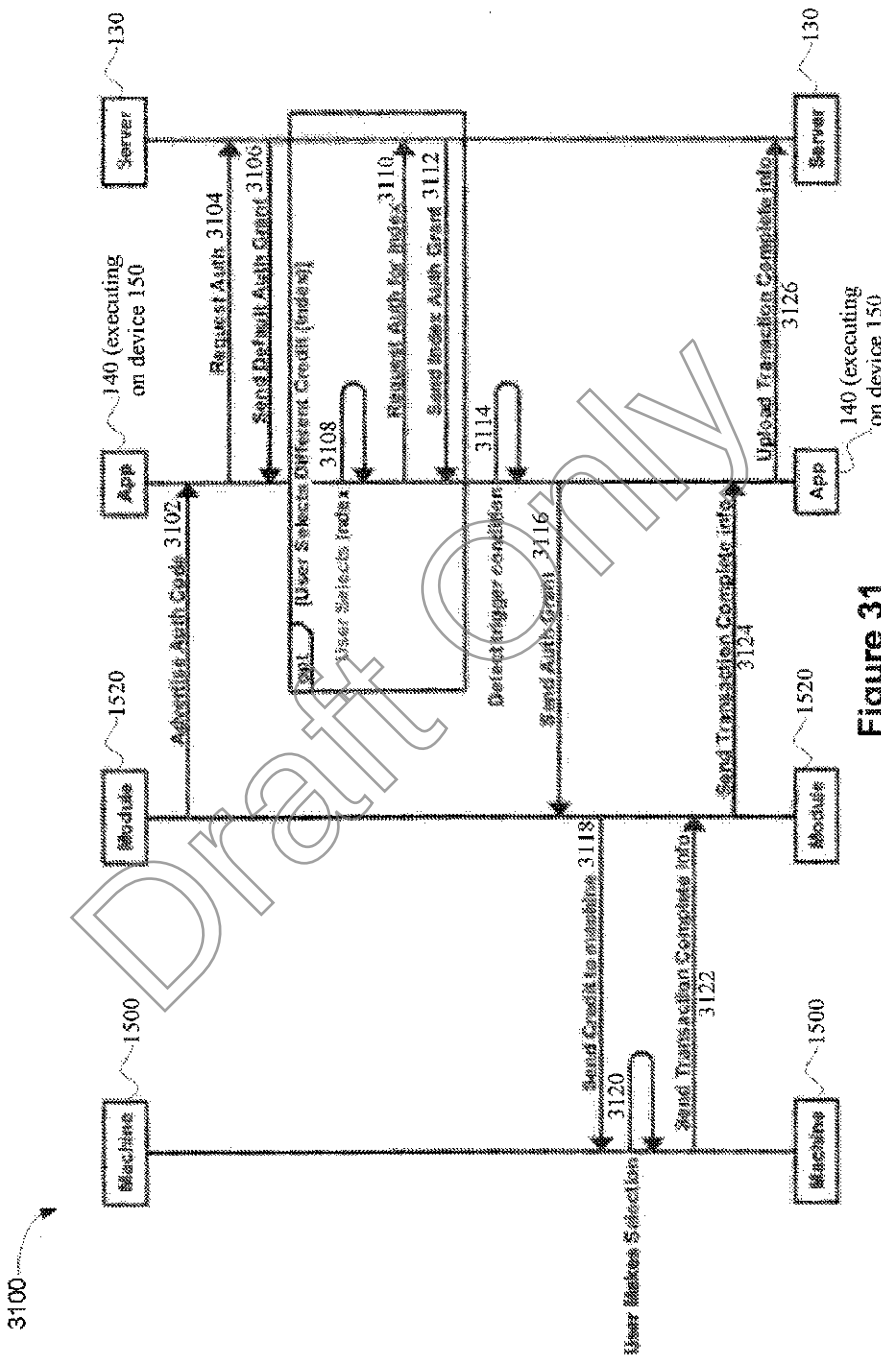


Figure 31

Draft Only

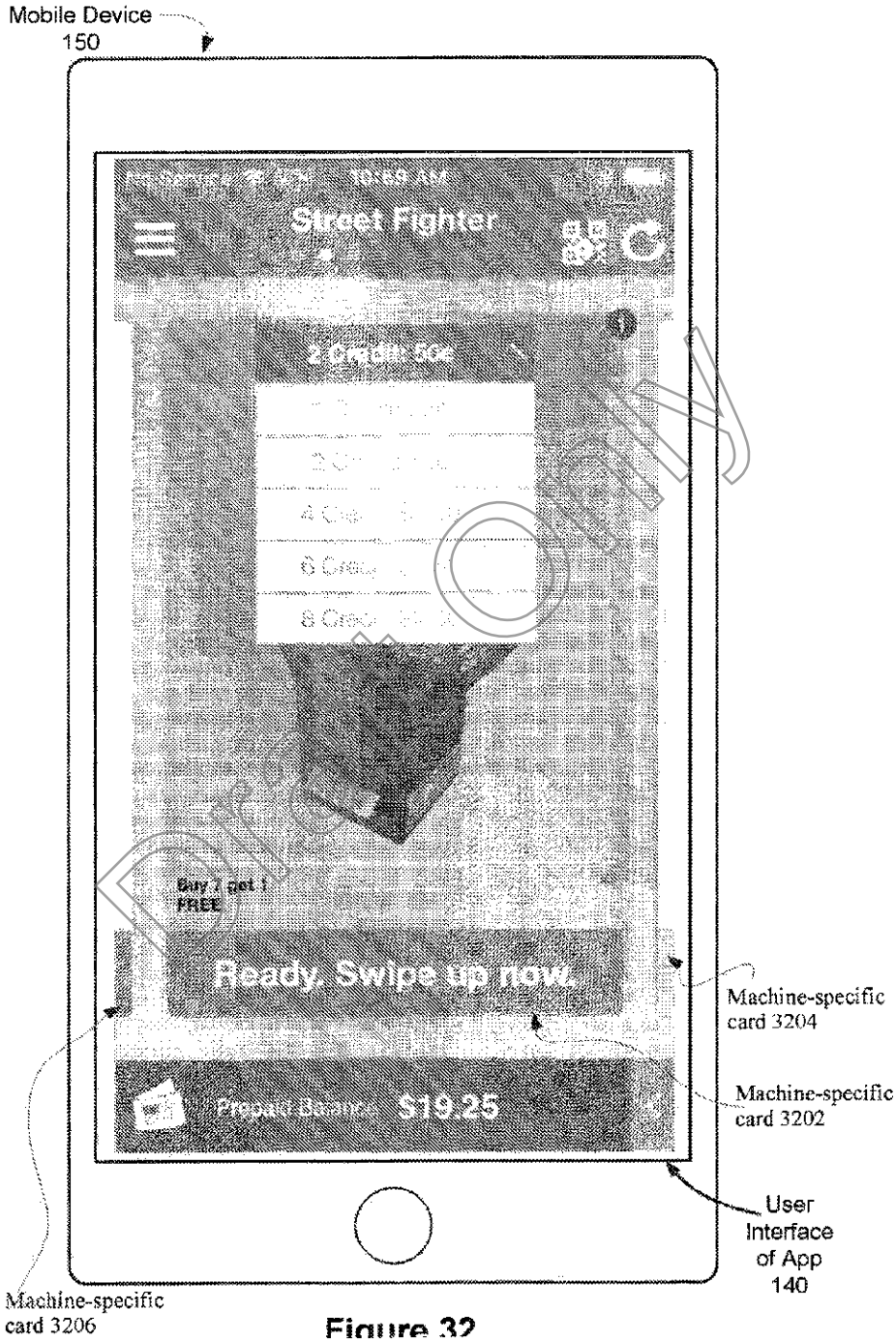
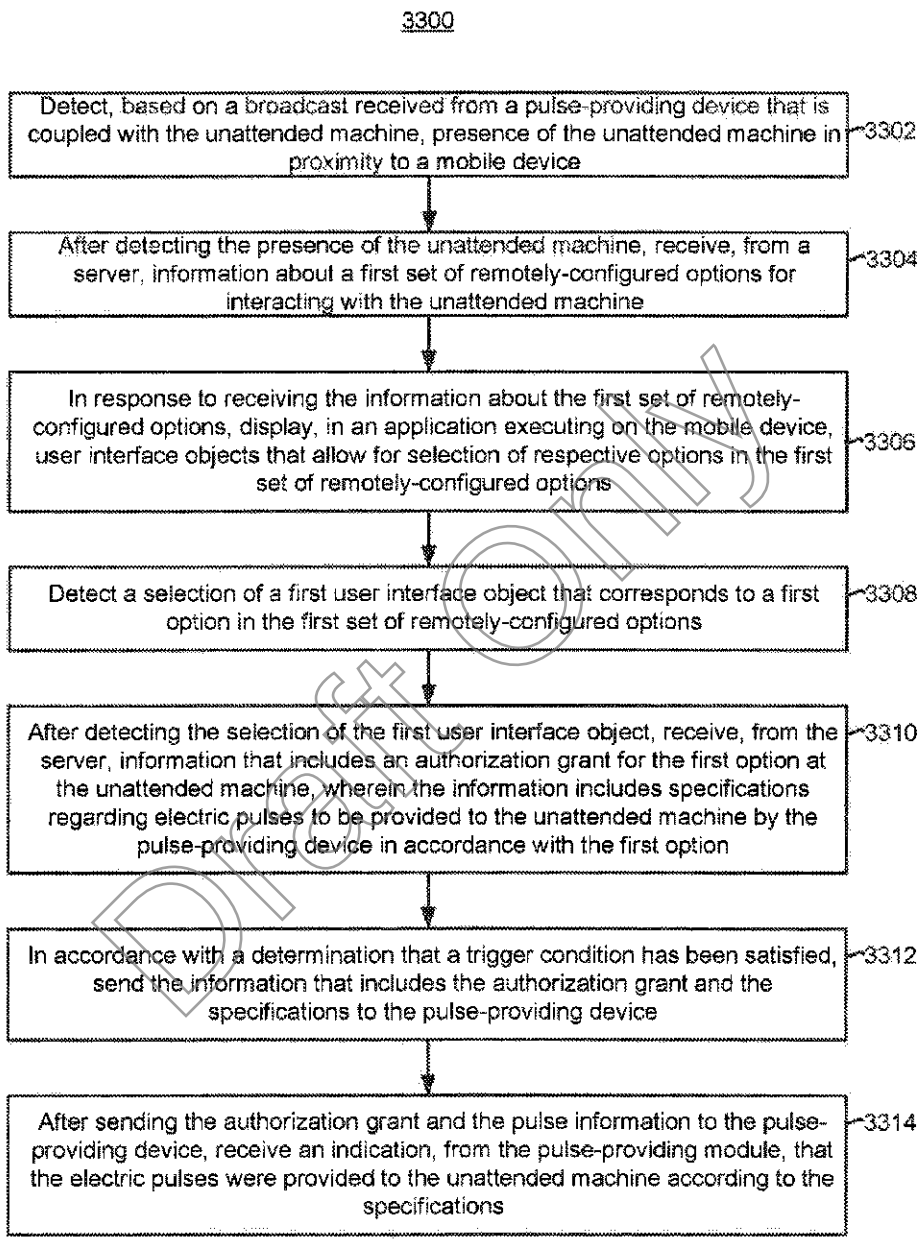

Mobile Device
150
Street Fighter
Buy 7 get 1
FREE
Ready. Swipe tip now.
Prepaid Balance: $19.25
Machine-specific
card 3204
Machine-specific
card 3202
User
Interface
of App
140
Machine-specific
card 3206

Figure 32



Draft Only

Figure 33

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2017/018194

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q30/06 G07F7/00 G06Q20/16 G06Q20/18 G06Q20/20 G06Q20/32
ADD.
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)
G06Q G07F

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)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2015/170131 A1 (PATEL PARESH K [US]) 18 June 2015 (2015-06-18) paragraphs [0085], [0125] - [0129], [0202] - [0206], [0211], [0215] - [0217], [0221], [0226], [0227]; figures 28A, 28B	1-21
A	US 2015/235202 A1 (ZABALA JOSE RAFAEL [US]) 20 August 2015 (2015-08-20) abstract figures 13,15 paragraphs [0009], [0011], [0071], [0082], [0101], [0102]	1-21
A	US 8 600 899 B1 (DAVIS PAUL R [US]) 3 December 2013 (2013-12-03) abstract; figure 2	1-21

-/--

Draft Only

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* 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
5 April 2017	12/04/2017

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040,	Cabniel, Christian

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2003/158891 A1 (LEI JONATHAN L [US] ET AL) 21 August 2003 (2003-08-21) figure 2 paragraphs [0028], [0029]	1-21

Draft Only

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2017/018194

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015170131 A1	18-06-2015	NONE	
US 2015235202 A1	20-08-2015	NONE	
US 8600899 B1	03-12-2013	US 8600899 B1	03-12-2013
		US 2014100977 A1	10-04-2014
US 2003158891 A1	21-08-2003	NONE	

Draft Only

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 January 2017 (19.01.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/010936 A1

(51) International Patent Classification:
G06Q 20/32 (2012.01) *G06Q 40/02* (2012.01)

(21) International Application Number:
PCT/SG2016/050297

(22) International Filing Date:
27 June 2016 (27.06.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
102015055857 16 July 2015 (16.07.2015) SG

(71) Applicant: **TOUREGO GLOBAL PTE. LTD.** [SG/SG]; 141 Cecil Street, #08-07 Tung Ann Association Building, Singapore 069541 (SG).

(72) Inventor: **TAN, Tie Wee**; c/o 14, Robinson Road, #08-01A, Far East Finance Building, Singapore 048545 (SG).

(74) Agent: **YUSARN AUDREY**; 24 Raffles Place, #27-01, Clifford Centre, Singapore 048621 (SG).

(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, BN, BR, BW, BY, BZ, CA, CH, CL, 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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

Draft Only

(54) Title: SYSTEM AND METHOD FOR FACILITATING REFUNDS

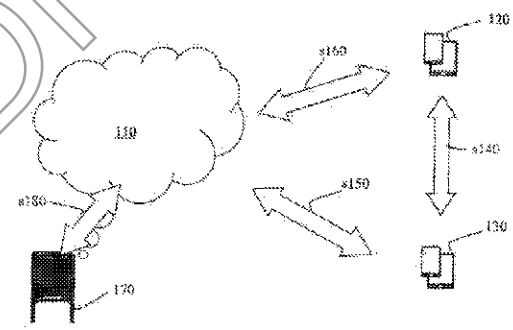


FIG. 1

(57) Abstract: A system and method for facilitating a refund to a user is disclosed. The system comprises a mobile device having means to communicate with a central processor for the generation of a refund account and a unique identifier; the unique identifier associated with the user; a computer device operable to access the unique identifier for verification upon receipt of a refund qualifying transaction associated with the user, the computer device further operable to send information relating to the refund qualifying transaction and generate a refund request upon successful verification; and the central processor operable to be in data communication with the computer device to receive and process the refund request, the central processor further configured to generate an elec-

WO 2017/010936 A1

SYSTEM AND METHOD FOR FACILITATING REFUNDS

FIELD OF THE INVENTION

The present invention relates to a system and method for facilitating refunds, such as but not limited to a tax refund for purchases made by tourists while travelling within their destination countries ("tourist refund").

BACKGROUND ART

The following discussion of the background to the invention is intended to facilitate an understanding of the present invention only. It should be appreciated that the discussion is not an acknowledgement or admission that any of the material referred to was published, known or part of the common general knowledge of the person skilled in the art in any jurisdiction as at the priority date of the invention.

In line with tax principle while at the same time attracting tourists, jurisdictions that levy a Value-Added Tax (VAT) or Goods and Services Tax (GST) or similar would allow individuals such as tourists to claim a tax refund on the goods purchased within a country. This tax refund would be administered upon the departure of the tourists from the country; provided certain criteria are met such as the goods are unopened, unused and exported out of the country.

The Revenue/Customs authorities of the country can administer tourist refund scheme(s), although it is increasingly popular for commercial contractors to be appointed to administer on their behalf. These commercial contractors typically work in cooperation with the Revenue/Customs authorities to ensure that the appropriate amount of tax refunds is paid out to the tourist(s). A service or commission fee will be charged which would form the bulk of the revenue model for the commercial contractor.

Two methods of administration of tourist refund schemes are currently being operated in the world. One is based on the authentication of paper forms and mandatory checks including physical checks at the point of departure by

Draft Only

CSC ServiceWorks - Ex. 1002
Page 837 of 1551

Revenue/Customs officials, and the other that is based on the electronic capture of transaction data by static devices at a participating retailer's shop and the use of this data to perform a risk-based selection of transactions for physical checks at the point of departure by Revenue/Customs officials.

For example, in Singapore the GST paid for purchases at the shops can be refunded via an electronic Tourist Refund Scheme (eTRS). The eTRS scheme starts when a tourist makes a purchase at a participating retailer and shows his passport at the point of purchase to prove his eligibility. Some non-exhaustive examples of the criteria that the tourist must fulfill in order to be eligible for the GST tax refund include:

i. the tourist is not a Singapore citizen or permanent resident of Singapore;

ii. the tourist had not spent more than 365 days in Singapore in the past twenty-four (24) months before the date of purchase;

iii. the tourist has not been employed in Singapore at any time in the past six (6) months before the date of purchase;

iv. the tourist is sixteen (16) years old or above at the time of purchase; and

v. the tourist is not a crew member of any aircraft or international cruise departing Singapore.

When paying for the purchases, the tourist would typically utilize a credit/debit card. Information such as the sixteen-digit primary account number (PAN) related the credit/debit card may be used as an identifier or token for tagging the purchases entitled for refund. The participating retailer (merchant) may also issue a paper eTRS Ticket to the tourist. The eTRS Ticket can also be used as a token instead of the credit/debit card.

With this token, the tourist can apply for a GST refund at the eTRS self-help kiosk before checking in at an airport or other immigration departure points such as, but not limited to, an airport or a cruise centre. If approved, the eTRS self-help kiosk would generate a Notification Slip indicating "Approved". Depending on the mode of refund selected by the tourist, the tourist can

Draft Only

obtain the refund (minus a service fee) by a direct credit into a designated refund account, such as credit card account, by a bank cheque or in cash at a central refund counter using the approved Notification Slip. If not approved, the eTRS self-help kiosk would generate a Notification Slip indicating that the refund is "Not Approved". The tourist then brings his purchases to the Customs counter for physical inspection. If the goods pass Customs inspection, a Customs officer would generate a Notification Slip indicating "Approved" to replace the "Not Approved" Notification Slip. During peak hours, these could become bottlenecks in processing the departing tourists as the customs counter is limited by manpower while the self-help kiosks may be overwhelmed by the number of tourists applying for refunds. Departing tourists typically have to arrive at the immigration departure points earlier to locate these static self-help kiosks in anticipation of a queue.

Further, in order to qualify for the GST refund in Singapore, the tourist must meet certain criteria. These criteria include spending at least S$100 (including GST) that can be accumulated in up to three (3) same-day invoices or receipts from retailers bearing the same GST registration number. Also, the tourist has to depart with the goods via the airport or cruise centre within a predetermined period, such as two (2) months from the date of purchase. The tourist must also depart with the goods within twelve (12) hours after obtaining approval of the GST refund. If the tourist is departing on an international cruise (excluding cruises-to-nowhere, round-trip cruise and regional ferry) from the cruise terminal, he must declare that he is exiting Singapore and will not return via the same voyage on the same ship, using his cruise itinerary as documentary proof of departure, and commit that he will not be returning to Singapore within forty-eight (48) hours. Further additional criteria may be imposed on student pass holders.

The authorities typically require that the purchases are verified against the invoices or receipts, and the goods are unused, unopened and exported out of the country and this is done at a counter either before check in (for goods that are to be checked in) or after immigration, to ensure that the goods are exported. However, the authorities at times do a targeted check instead.

Draft Only

With the proliferation of mobile devices, it is common for tourists to travel with at least one personal mobile device that may be used to connect to the internet either via a wireless fidelity (Wi-Fi) networks or mobile telecommunications networks. Hence, it is envisaged that the functions of the mobile device, in particular smartphones, can be better utilized in allowing electronic tax refunds to be facilitated through the use of a dedicated software application residing on this mobile device together with its onboard camera, geo-location module, wireless communication module (Bluetooth and Wi-Fi), alarm notifications, internet connectivity etc.

The present invention seeks to provide a system and method that alleviates the above-mentioned drawbacks or meet the above needs at least in part.

SUMMARY OF THE INVENTION

Throughout the document, unless the context requires otherwise, the word "comprise" or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated integer or group of integers but not the exclusion of any other integer or group of integers.

Furthermore, throughout the specification, unless the context requires otherwise, the word "include" or variations such as "includes" or "including", will be understood to imply the inclusion of a stated integer or group of integers but not the exclusion of any other integer or group of integers.

The present invention seeks to meet the needs of a tax refund system that does not rely on self-help kiosks, and enables users such as tourists to access their tax refunds efficiently and accurately. The invention proposes a system and method of administration by way of an application software installable on mobile devices to verify user identity, facilitate a completely paperless tourist tax refund experience, and enable more types of transaction data to be captured for a more complete risk-based selection.

A technical problem the invention seeks to solve relates to the bottlenecks faced by customs at peak hour. Another technical problem is associated with

Draft Only

CSC ServiceWorks - Ex. 1002
Page 840 of 1551

the need to verify identities of tourists and transactions, such as purchases against the invoices and receipts in a more effective and efficient manner to reduce identity and transaction frauds.

The above and other problems are alleviated at least in part and an improvement in the art is made by a system in accordance with this invention. A first advantage of the system in accordance with this invention is that the tourist refund process is completely electronic, thereby eliminating the need to deal with paper refund tickets and paper receipts. A second advantage of the system in accordance with this invention is that the tourist is able to register in their own time and convenience on their mobile devices and after logging into the system, the tourist is able to view a consolidated list of all the refund claims they have made via the system, the additional spending required in order to fulfil the minimum spending requirement, as well as the amount of intermediate value accumulated and used. Such intermediate value may be translated into a form of 'rewards points' or the like. An associated third advantage of the system in accordance with this invention is that by having an intermediate value system (in the form of rewards point or the like) that is currency agnostic, there is no need to convert currencies. This mitigates any fluctuations in the exchange rates. Such an arrangement provides more certainty to the tourist in terms of the amount of tax refund obtainable, which can be spent even before the refund was actually approved. In accordance with an aspect of the invention there comprises a system for facilitating refund to a user comprising: a mobile device having means to communicate with a central processor for the generation of a refund account and a unique identifier; the unique identifier associated with the user; a computer device operable to access the unique identifier for verification upon receipt of a refund qualifying transaction associated with the user, the computer device further operable to receive and send information relating to the refund qualifying transaction and generate a refund request upon successful verification; and the central processor operable to be in data communication with the computer device to receive or send information relating to verification of the unique identification and the refund qualifying transaction and process

Draft Only

CSC ServiceWorks - Ex. 1002
Page 841 of 1551

the verification or refund request, the central processor further configured to generate an electronic ticket to be sent to the mobile device for the generation of a refund upon successful process of the refund request.

In some embodiments, the refund may be a tax refund, and be in the form of an intermediate value. The intermediate value may be derived from the actual value of refund based on a conversion rate.

In some embodiments, the computer device may be a point-of-sale device, such that the point-of-sale device may be configured to directly send information relating to the refund qualifying transaction to the central processor.

In some embodiments, the generated unique identifier may be encoded as a quick response (QR) code and the computer device accesses the unique identifier by scanning the QR code displayed on the mobile device.

In some embodiments, the central processor may be operable to send the electronic ticket to a third party server for further verification of the refund qualifying transaction and confirmation of the refund.

In some embodiments, the central processor stores the information relating to the refund qualifying transaction in a database before the electronic ticket is generated and sent to the third party server.

In some embodiments, the mobile device may be operable to send an electronic notification related to a requirement being met. The requirement may be a confirmation of departure, or a Declaration of Eligibility.

In some embodiments, the mobile device may be operable to receive a notification of refund issued by a third party server once the electronic ticket is processed successfully.

Draft only

CSC ServiceWorks - Ex. 1002
Page 842 of 1551

In some embodiments, the central processor is operable to receive a notification of refund issued by a third party server once the at least one electronic ticket is processed successfully and the central processor is operable to send a notification of refund to the mobile device.

In some embodiments, the unique identifier associated with the user is generated based on a passport information of the user.

In some embodiments, the unique identifier is generated after a registration process.

In some embodiments, the unique identifier is further associated with an image capture of the passport.

In some embodiments, the mobile device is integrated with the computing device.

In some embodiments, the central processor is operable to send a notification to the mobile device indicating the success or failure of the refund request.

In some embodiments, there comprises another unique identifier associated with a retailer using the computer device.

In some embodiments, the another unique identifier is generated after a registration process by the retailer.

In some embodiments, the another unique identifier is further associated with an image capture of one or more account information associated with the retailer.

In some embodiments, if the unique identifier is not accessible by the computer device, the computer device is operable to obtain an alternative identifier for verification and send the alternative identifier to the central

Draft Only

CSC ServiceWorks - Ex. 1002
Page 843 of 1551

processor.

In some embodiments, upon receipt of the alternative identifier, the central processor is operable to determine whether a corresponding refund account associated with the user is present and if not, the central processor is operable to generate the refund account and the unique identifier based on the alternative identifier.

In some embodiments, the central processor comprises or is in data communication with a database for storing at least one retailer list of goods and services eligible for tax refund.

In some embodiments, the central processor is operable to receive a wish-list of goods and services from the mobile device and upon receipt of the wish-list, compare the wish-list with the at least one retailer list of goods and services.

In some embodiments, when there is a match between the wish-list and the at least one retailer list, the central processor is operable to provide a matched list to the mobile device.

In some embodiments, where the electronic ticket is a provisional electronic ticket, the provisional electronic ticket comprises a plurality of electronic receipts.

In some embodiments, the provisional electronic ticket is converted to a final electronic ticket at an approved departure point.

In some embodiments, the central processor arranged in data communication with at least one third party server to retrieve information related to the identity of the user, and sends the information related to the identity of the user to the computer device.

Draft Only

In some embodiments, if the refund request is not successfully processed, the central processor is arranged in data communication with another computer device provided to an authorized personnel to perform further processing.

In accordance with another aspect of the invention there is a method for facilitating a refund to a user comprising the steps of: communicating via a mobile device with a central processor for the generation of a refund account and a unique identifier, the unique identifier associated with the user; via a computer device, accessing the unique identifier for verification on receipt of a refund qualifying transaction associated with the user; generating a refund request upon successful verification; sending information relating to the refund qualifying transaction via a central processor; receiving and processing the refund request; wherein the central processor is further configured to generate an electronic ticket to be sent to the mobile device for the generation of a refund upon successful process of the refund request.

In some embodiments, the method further includes the step of converting the refund to an intermediate value after the generation of the refund.

In some embodiments, the intermediate value is derived from the actual value of refund based on a conversion rate.

In some embodiments, the method further comprises the step of exporting the information relating to the refund qualifying transaction via a point-of-sale (POS) device in data communication with the computer device, the point-of-sale device is configured to directly send information relating to the refund qualifying transaction to the central processor.

In some embodiments, the computer device accesses the unique identifier by scanning an image shown on the mobile device.

In some embodiments, the method further comprises the step of sending the electronic ticket to a government server for further verification of the refund

Draft Only

qualifying transaction and confirmation of the refund.

In some embodiments, the mobile device is operable to send an electronic notification related to a requirement being met. The requirement may be a confirmation of departure. The requirement may alternatively, or in conjunction, be a Declaration of Eligibility.

In some embodiments, the generation of electronic ticket is based upon one or more requirements being met.

In some embodiments, the method further comprises a step of sending an electronic notification to the mobile device indicating the success or failure of the refund request.

In some embodiments, the method further comprises a step of obtaining an alternative identifier for verification and sending the alternative identifier to the central processor if the unique identifier is not accessible by the computer device.

In some embodiments, upon receipt of the alternative identifier, the central processor is operable to determine whether a corresponding refund account associated with the user is present and if not, the central processor is operable to generate the refund account and the unique identifier based on the alternative identifier.

In some embodiments, the central processor comprises a database for storing at least one retailer list of goods eligible for tax refund.

In some embodiments, the central processor is operable to receive a wish-list of goods from the mobile device and upon receipt of the wish-list, compare the wish-list with the at least one retailer list of goods or services.

In some embodiments, when there is a match between the wish-list and the at

Draft Only

CSC ServiceWorks - Ex. 1002
Page 846 of 1551

least one retailer list, the central processor is operable to provide a matched list to the mobile device.

In some embodiments, the electronic ticket is a provisional electronic ticket, the provisional electronic ticket comprises a plurality of electronic receipts. The provisional electronic ticket may be converted to a final electronic ticket at an approved departure point.

In accordance with another aspect of the invention there is a non-transitory computer readable medium containing executable software instructions thereon wherein when executed on a mobile device and/or a computer device performs the method of facilitating a refund to a user comprising the steps of: communicating via the mobile device with a central processor for the generation of a refund account and a unique identifier, the unique identifier associated with the user; accessing the unique identifier for verification via a computer device on receipt of a refund qualifying transaction associated with the user; sending information relating to the refund qualifying transaction; generating a refund request upon successful verification; and receiving and processing the refund request by a central processor, wherein the central processor is further configured to generate an electronic ticket to be sent to the mobile device for the generation of a refund upon successful process of the refund request.

The non-transitory computer readable medium may further comprises a software instruction to send an electronic notification to the mobile device indicating the success or failure of the refund request.

Draft Only

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Fig. 1 is the overall architecture of an embodiment of the invention showing how the various parts of the system interact;

CSC ServiceWorks - Ex. 1002
Page 847 of 1551

Fig. 2 is a flowchart of an embodiment of the invention showing how a user is taken through the system when the application is launched;

Fig. 3 is a state machine diagram of an embodiment of the invention; and

Fig. 4 and Fig. 5 show how a single MDCC device may be used for the deployment of tourist refund in accordance with other embodiments of the invention.

Other arrangements of the invention are possible and, consequently, the accompanying drawing is not to be understood as superseding the generality of the preceding description of the invention.

PREFERRED EMBODIMENTS OF THE INVENTION

Particular embodiments of the present invention will now be described with reference to the accompanying drawings. The terminology used herein is for the purpose of describing particular embodiments only and is not intended to limit the scope of the present invention. Additionally, unless defined otherwise, all technical and scientific terms used herein have the same meanings as commonly understood by one of ordinary skill in the art to which this invention belongs.

In accordance with an embodiment of the present invention and with reference to Fig. 1, there is a system 10 for facilitating refunds. The refund may be in the form of tax refund provided to a tourist and will be described in such a context. It is to be appreciated that the system 10 may be adapted for other types of refunds and not limited to a tax refund. The term 'refunds' include refund in an electronic medium.

The system 10 comprises a central processor 110. Central processor 110 may be in the form of one or more processors and/or servers 110 belonging to an organisation administering the tourist refunds. An example of such an organisation is the Central Refund Agency (CRA). The CRA may be a private organisation, a government organisation, or a quasi-government organisation.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 848 of 1551

The CRA may further be in data communication with a Central Clearing House (CCH) 170 for the purpose of settlement and crediting of refund value.

The one or more servers 110 can include a cloud server or a conventional server with data communications capability. For the ease of discussion, the one or more server will hereinafter be referred to as 'server' or 'servers'. Server 110 may be connected to one or more databases (not shown). Such database(s) are operable to contain records and information relating to the tourist refunds such as name, addresses and/or pre-generated or generated unique identifiers associated with the users seeking refunds. Server 110 is also operable to generate and update refund accounts for facilitating, processing and crediting refunds.

In one embodiment, the system 10 comprises a mobile device 120, preferably endowed with communications and computing capabilities and hereinafter referred to as MDCC 120, and computing device 130 (hereinafter referred to as 'Retailer Device' 130). The Retailer Device 130 can also be an MDCC or other computing device like a desktop/laptop computer. A Point-of-Sale (POS) device/system may be in data communication with the Retailer Device 130, the data communication in wired or wireless, remotely or otherwise. Alternatively, the POS device or its associated function may be incorporated/integrated with the Retailer device 130 as a module.

To facilitate the refund process, the mobile device 120 and computing device 130 may be installed with dedicated software applications (colloquially known as 'apps'). Such dedicated software applications may be operating system (OS) such as iOS™ or Android™ specific, and/or device specific.

The software application installable on mobile device 120 provides a user interface for user registration and for retrieving or providing information for the refund process. Once installed, the software application is operable to perform at least the following functions:-

a. receive registration details entered by the user;
b. communicate with the server 110 to send the registration details;
c. receive from the server 110 a unique identifier associated with the user (tourist);
d. receive from the server 110 information related to the refund process;

Draft Only

CSC ServiceWorks - Ex. 1002
Page 849 of 1551

e. display notifications/alerts on the MDCC 120 relating to refund process;
f. provide user interface for user to browse or view account details;
g. search for necessary communication networks for data communication with the server 110 and the computing device 130 (if necessary); and
h. store, organise and retrieve information received from various parties.

The MDCC 120 and the Retailer Device 130 can be any mobile electronic device(s) that can connect wirelessly to Wi-Fi networks or conventional telecommunications networks such as 2G, 3G, 4G, or LTE based networks. The mobile electronic devices include, but are not limited to mobile devices like smartphones, personal digital assistant (PDA) phones and tablets. The devices include mobile devices running on iOS platforms such as the iPhone and the iPad.

The invention will next be described in the context where a user of MDCC 120 (presumably a tourist) downloads a dedicated software application (hereinafter 'software application') onto the MDCC 120 for registration with the system 10; and usage of the MDCC 120 with the installed software application for facilitating refunds.

During the first usage after downloading the dedicated software application, a registration process is initiated where the tourist is prompted to register by entering his or her registration details into the application. The tourist may enter the necessary details for registration via manual entry or via imaging the identification documents associated with the tourist, if the MDCC 120 comprises an imaging device or module such as an on-board camera. The identification documents may include passport or other approved identification papers identifying the user as a tourist. In the case of a passport that comprises a machine readable zone (for example barcode), the MDCC 120 may also be used for reading the readable zone on the passport using the on-board camera or if the MDCC 120 is installed with the necessary hardware and/or software for doing the same.

The registration process can further integrate a verification of the authenticity of passports. The registration process can also include a check against records or entries in one or more authorized databases (for example government immigration records) to ascertain the eligibility of the tourist for a

Draft Only

CSC ServiceWorks - Ex. 1002
Page 850 of 1551

tax refund. Such authorized databases may be public or private databases. With these verifications, the tourist may not need to carry his passport in order for the retailer to verify his tourist status, subject to regulatory acceptance of such method of verifications.

Upon receiving the registration information, the MDCC 120 next sends the registration information to the server 110 for the creation of a user account. Once the user account is created, the server 110 then replies to the MDCC 120 with a unique identifier associated with the user account, for the tourist. The unique identifier can be in the form of an assigned account number and/or encoded into a QR or Quick Response code by the server 110 or software application installed on MDCC 120. The QR code is a type of matrix barcode that is machine readable and can contain information that can quickly be translated into usable data.

Once the unique identifier is generated, the unique identifier can be accessed on the same MDCC 120 used to register the user or on any other mobile devices 120 that is compatible with the form or physical medium that the unique identifier is encoded. In this regard, the unique identifier is therefore device agnostic. Other types of machine readable codes like barcodes can also be used in place of QR codes, although these may hold less data. This QR code is tied/tagged to each and every tax refund qualifying transaction made by the tourist.

It is to be appreciated that the unique identifier may include a simple account number, and/or a combination/hybrid of one or more of the above described codes.

Once registered and a user account is in place, the tourist user may then make tax refund qualifying transactions such as tax refund qualifying purchases at one or more participating retailers.

After the tax refund qualifying purchase is made at the participating retailer, the tourist retrieves his or her unique identifier, in the form of a QR code, for display on the MDCC 120. The participating retailer uses the Retailer Device 130 to scan the QR code (s140) for verification on the eligibility for a tax refund by checking against the server 110 to ascertain if the tourist has a

Draft Only

CSC ServiceWorks - Ex. 1002
Page 851 of 1551

registered account and is eligible for a refund. As an example, the check will include comparing and matching entries with the server 110 and/or its associated processor(s) or database(s) to determine if the passport is a foreign passport and if the tourist is at an age eligible for refund (e.g. 16 years or older). The server 110 can also perform a check against government immigration records via the government server 170 to ascertain the eligibility of the tourist for a tax refund. Alternative ways of unique identifier accessing technology or combinations may be used. Examples of such technologies may include Near Field Communications (NFC), Bluetooth, WiFi, etc. as known to a skilled person. The identification may also be manually entered into the Retailer Device 130. Such a step of verification may include checking the physical passport and the passport information/details submitted, subject to compliance with the necessary regulatory requirements.

Upon scanning of the unique identifier, the participating retailer may enter the purchase/transaction details related to the purchase made by the tourist into the Retailer Device 130. The transaction details may be manually or automatically transmitted. In the latter, the transaction details may be transmitted automatically via a cable or wirelessly from a Point-of-Sale ("POS") system and/or POS device, the POS device configured to send the information relating to the refund qualifying transaction, i.e. purchase/transaction details to the Retailer Device 130 and/or server 110. For example, to facilitate the transmission, a software driver may be installed on the POS system for detecting the Retailer Device 130 as a printer, so that the POS device can print the transaction details to the Retailer Device 130. Alternatively, software may be installed on the POS device or system to capture the transaction details from a payment screen via an Optical Character Recognition (OCR) module. In the case of an Internet-enabled POS system or device, the purchase or transaction details can be directly transmitted to the server 110 via one or more wired or wireless communication means. The transaction details may then be accessible via a web resource locator or link, such as a Uniform Resource Locator (URL).

If a paper receipt is issued for the transaction, the Retailer Device 130 may also be used to image or scan the paper receipt associated with the

Draft Only

CSC ServiceWorks - Ex. 1002
Page 852 of 1551

transaction for the transaction details to be extracted by an image conversion and/or recognition module, such as, for example the OCR module. Once the retailer has verified the transaction details thus captured, he can transmit the transaction details to the server 110 via the Retailer Device 130. In another embodiment, the MDCC 120 may be used in place of the Retailer Device 130 to image or scan the paper receipt associated with the transaction. Once the retailer has verified the transaction details thus captured, he can present the tourist with a retailer identifier, which can be another QR code, unique to the retailer, for scanning by the MDCC 120, as a form of retailer confirmation/receipt.

In another embodiment, if a user is unable to present his unique identifier in the form of a QR code (for example because the user has not yet registered with the server 110), the retailer may scan an alternative identifier, such as but not limited to the Tourist's passport to retrieve his account information. The scanning device may be the Retailer Device 130 or in the form of a barcode scanner or other imaging device and once the passport has been scanned, the server 110 checks if the tourist has a registered account and eligible for a refund, e.g. if passport is a foreign passport and if tourist is at an age eligible for refund (e.g. 16 years or older). The server 110 can also perform a check against third party servers or databases, such as government immigration records via the government server 170 to ascertain the eligibility of the tourist for a tax refund. If the tourist is not eligible, the server 110 prompts an authorized personnel (e.g. a cashier) to inform the tourist that he is not eligible for tourist refund. If the tourist is eligible, the server 110 checks for an existing account by comparing the scanned details with one or more databases of the server 110. If a user account already exists, the app installed on the retailer device 130 is operable to display the user profile or details for validation by the cashier. If the tourist before the cashier matches the user profile, then the cashier confirms the user (customer) identity via a user interface and proceeds to enter receipt details. If a user account does not exist for the tourist, the server 110 creates a user account and the cashier proceeds to enter receipt details.

The Retailer Device 130 (or the MDCC 120) is operable to send the unique

Draft Only

identifier, as well as the transaction details like the cost, the receipt number, the date and time of the transaction, etc. (see s150) to the server 110. No transaction details can be transmitted without the necessary information associated with the unique identifier (in the form of the QR code) on the MDCC 120 (or on the Retailer Device 130). To minimize fraud, the the Retailer Device 130 can be configured (by the retailer or otherwise) to halt all communications outside of the retailer's opening hours. This would prevent unauthorised tax refunds claims from being entered into the system. The security of the system 10 can be further enhanced by a password management system that requires the cashier to log into the retailer account and may require the password to be changed regularly. Sub-accounts may also be created for individual employees of the retailer who are responsible for collecting payment and their supervisors to create a system of checks-and-balances for approving unusual tax refund claims. Prior to use, the retailer account may undergo a similar registration process as described earlier for the user (tourist) account. In some embodiments, the registration process entails the server 110 assigning or issuing retailers with user identifiers (IDs) and passwords. A manager of the retailer may create sub-accounts. Alternatively the server 110 may assign subaccounts to the retailers, who in turn have administrative rights to manage the sub-accounts. Similar to the registration of the user account, another retailer unique identifier such as a QR code may be generated and assigned to each retailer who registers for an account to participate in the system.

Based on the details sent by the participating retailer, the server 110 sends an electronic ticket for the notification of transaction. Such a notification may be in the form of an eTRS Ticket (containing the details mandated by the Revenue/Customs authorities such as a documentary ID or DOC-ID that uniquely identifies the transaction) directly to the MDCC 120, thus recording the purchase as an eTRS Transaction. The server 110 would also notify the participating retailer via the dedicated software application installed on the Retailer Device 130 of the eTRS Ticket (see s150).

The MDCC 120 is operable to image, store and organise the purchase receipts and invoices issued by the participating retailer, and link these with

Draft Only

CSC ServiceWorks - Ex. 1002
Page 854 of 1551

the eTRS Transaction for ease of subsequent retrieval by the tourist or by an inspector of the Revenue/Customs authorities. The server 110 will transmit the transaction details as required by the Revenue/Customs authorities to a Central Clearing House (CCH) 170 for lodgement as an eTRS Transaction 180. In another embodiment of the present invention, the server 110 can also request the CCH 170 to perform an instance of risk assessment after each transaction, and communicate 180 the risk assessment results to the server 110. If the result is such that the tourist is selected to present his or her purchases for inspection by an officer of the Revenue/Customs authorities at the point of departure from the country, the server 110 would then notify the tourist of this requirement via the software application installed on the MDCC 120 either shortly after the transaction itself and/or at the point of departure from the country (s160). This early deterrence would assist to deter potential fraudsters from trying to obtain a tax refund through fraudulent means.

With additional tax refund qualifying purchases, multiple eTRS Tickets can be sent to the MDCC 120 in the same direct way (s160).

When the tourist is leaving the country, the MDCC 120 or the dedicated software application installed on the MDCC 120 would request for confirmation of departure from the tourist. Once the tourist confirms his departure from the country, the tourist can request for a refund together with a Declaration of Eligibility (a requirement by the Singapore Revenue/Customs authorities) or other declarations as required by the Revenue/Customs authorities (s160). The tourist may be guided through the Declaration of Eligibility process by the application on the MDCC 120, which also displays the passport details of the tourist for his or her confirmation as the person making the Declaration. Purchases recorded as eTRS Transactions are also displayed for the tourist to select those for which he or she would like to submit a claim for tax refund. For those tax refundable purchases made through retailers that do not operate the application, the application on MDCC 120 can scan the paper copy of the eTRS Tickets issued by these retailers so that all the transactions are consolidated. Alternatively, the CCH 170 can also transmit electronically, the details contained in the paper eTRS Tickets, to MDCC 120, upon request by the MDCC 120 or the dedicated software

Draft Only

CSC ServiceWorks - Ex. 1002
Page 855 of 1551

application installed on the MDCC 120. The tourist would also confirm the preferred refund option – whether in cash or credited back to a credit/debit card or a bank account or even an electronic wallet account – and the application guides the tourist to confirm the relevant details accordingly. The preferred refund option and details may have already been entered at the point of user registration, otherwise the tourist will be prompted to do so. The tourist may also enter the necessary details via manual entry or via imaging the credit card via the on-board camera on MDCC 120, for example.
Once the various fields are completed, the application can allow the tourist to confirm the details one last time before submitting them to the server 110.

In addition to the tourist proactively initiating a request for refund, one way of reminding the tourist to submit the request for refund would be to use a location-based service, such as Global Positioning System (GPS), geo-fencing, navigation systems etc, to alert the MDCC 120 when the MDCC 120 is detected within range of a departure point installed with a location-based service device, examples of such departure points including an airport or a cruise centre. This would notify and remind the tourist to submit the request for refund. Alternatively, the application on the tourist MDCC 120 can also rely on Wi-Fi networks or cellular base stations at the airport and the cruise centre to remind the tourist when the MDCC 120 accesses these networks. Alternatively, the MDCC 120 can detect transmitters (including but not limited to Bluetooth Low Energy beacons) located at a departure point, such as an airport or a cruise centre, and trigger the application to remind the tourist. This saves the tourist the trouble of having to arrive at the airport early to locate the eTRS self-help kiosk, since the tourist can now submit the request using his or her MDCC 120.

Once the request for refund is submitted (s160) to the server 110, the CCH 170 is notified via s180 and can communicate to the server 110 as to whether the tourist has been selected for inspection by the Revenue/Customs authorities and the server 110 notifies the tourist via the MDCC 120 accordingly (s160).

Draft Only

CSC ServiceWorks - Ex. 1002
Page 856 of 1551

For tourists who have not been selected for inspection, they would receive a digitised Notification of Approval slip on their MDCC 120. Those who have not received a notification of approval slip and/or have been selected for inspection either at any point of purchase or after the submission of the request for refund would receive a digitised Notification of Inspection slip prompting them to proceed to a counter of the Revenue/Customs authorities for further processing. There, upon presenting the digitised eTRS tickets, invoices/receipts and notification slips stored on the tourists' MDCC 120 together with the goods purchased, passport and plane ticket, as required, an authorized personnel such as the Revenue/Customs officer or inspector updates the record stored at the CCH 170. This may be performed via a separate computing device provided to the customs officer having a dedicated software application installed thereon and arranged in data communication with the server 110 to interact with the server 110. In some embodiments, a 'customs officer' identifier in the form of a QR Code may be provided to the customs inspector to present to the tourist after the customs inspector is satisfied with the eligibility of the tourist and the purchases for a refund. Upon scanning of the QR Code, the server 110 then updates the CCH record as "Approved" and issues a Notification of Approval slip.

This Notification of approval may be in paper, or digitised and sent to their MDCC 120.

Cash refunds would be made at a Central Refund Counter (CRC) upon presentation of the Notification of Approval slips, otherwise the monies would be credited to their credit/debit card or bank account as previously indicated, or any payment platforms (e.g. Alipay™, Paypal™) for facilitating the transfer of refund monies to one or more user accounts. The tourists would then proceed to depart Singapore accordingly.

In some embodiments, instead of a cash refund, the refund value may be converted to an intermediate value. Examples of such intermediate value may be coupons, credits, points, or other electronic value etc. One embodiment of

Draft Only

CSC ServiceWorks - Ex. 1002
Page 857 of 1551

an intermediate value is in the form of 'rewards points'. Such a system of rewards points can also be implemented into the tourist refund process, where the rewards points can be applied towards the purchase of goods and services at participating retailers. Retailers participating in this system of rewards points can be the same ones that are accredited under the tourist refund scheme or retailers that are not accredited but can also be equipped with a Retailer Device 130. Tourists can accumulate rewards points issued by the CRA. In the conversion of tax refund to rewards points, the system may refund the full amount, less than or more than the full amount of tax levied depending on the conversion rate between the tax refund to rewards point, instead of withholding a service fee as in the traditional method, although a service fee can still be offered as an alternative. The system can offer the tourist the option to take the refund in the form of tourist refund (whether as cash or via a credit/debit card) or in the form of rewards points, by way of a prompt either at the point of purchase or at the point of departure from the country. The tourist could even be allowed to convert the tourist refund into rewards points (vice versa) at any point in time, with or without a conversion fee. There may be a point in time where the availability of a tourist refund by way of cash or credit card is reduced or even removed. The rewards points can also be tagged with an expiry date, such that they expire if not used within a certain period of time, or the rewards points may be issued without an expiry date.

With reference to Fig. 2, an embodiment of a process for facilitating a tourist refund, wherein like numerals reference like parts, is described. The process begins when the dedicated software application installed on MDCC 120 is launched (step 210). The process begins with checking whether the tourist is already registered or is a new unregistered user (step 220). If the tourist is not registered, the tourist is walked through with a registration procedure (step 230) where an electronic user account is created with the server 110 and the relevant details are captured by the dedicated software application. Backend, the system 10 performs checks against the details like the passport number, nationality, name and/or other relevant information to ensure duplicate records

Draft Only

are not created. The system can also verify the authenticity of the passports based on their security features or the server 110 may be linked with one or more third party servers. These third party servers may be private, public or government databases for the checking of stolen passports, as well as checking for other eligibility criteria such as whether the user is in fact a Permanent Resident of a particular jurisdiction and does not fall under the category of 'tourist', therefore ineligible for tourist refund; or whether the user has entered Singapore on a visit pass that may not strictly fall under a 'tourist pass', such as a student pass, etc. whereupon additional criteria have to be fulfilled. For each user account, a unique identifier like a QR code is created and stored by the application, or created by the server 110 and stored by the application. This process can be integrated with the onboard camera of the mobile device 120 to scan the machine readable zone of the passport to populate the various details or even to scan the passport itself with optical character recognition, or else manual entry of the details is used. The tourist is also given the option of imaging the passport, guiding him through the process of which page to capture, so that he does not have to carry a physical passport when shopping to claim a refund.

At a participating shop, the tourist makes a purchase and the retailer enters or scans the relevant details into the point-of-sale (POS) machine (step 240). After verifying that the purchases qualify for refund and the eligibility of the tourist by checking the tourist's passport, the retailer scans the unique identifier being displayed on the user MDCC 120 by either using the issued retailer device or the retailer's own mobile device with the application installed (step 250). One method of verifying the status of the tourist would be verification upon scanning the unique identifier or QR code via an onboard camera (where available) if the retailer is using a mobile device as the retailer device 130, whereby upon receipt of the scanned information (which includes the unique identifier), the server 110 would inform the retailer device whether the user is a tourist or not, which dispenses with the need to check the physical passport. The details of the transaction are then sent to the central server 110 or a processor belonging to the central refund agency (CRA) (step

Draft Only

CSC ServiceWorks - Ex. 1002
Page 859 of 1551

260), and this may be further sent to CCH 170. Once verified and the records updated, confirmation of the transaction is sent (step 270) together to the retailer and an eTRS Ticket is sent to the tourist either in the application, by email or any other forms of messaging. An electronic image or document of the invoice or receipt issued by the retailer can also be stored in the mobile application for later retrieval.

With some newer POS machines, the purchase details can be transmitted to the retailer device, either wirelessly via Wi-Fi or Bluetooth, or by a cable like a USB or similar, which speeds up the process and reduces the possibility of human error. The purchase details can even be directly transmitted to the server 110 in the form of a central processor. The added security measure of requiring the unique identifier before transmitting means the possibility of non-genuine tourist transactions is reduced. The tourist or the retailer may also use his or her mobile device to image the paper receipt associated with the transaction for the transaction details to be extracted by Optical Character Recognition. The retailer may also be equipped with other devices with imaging or scanning capabilities. Where the details are captured by the tourist's device, once the retailer has verified the transaction details thus captured, he can present the tourist with an identifier, which can be another QR code, unique to the retailer, for scanning by the tourist's device, as a form of retailer confirmation.

The application (and server 110) is also able to track the fulfilment of certain jurisdictional requirements where the purchases made by the tourist are submitted to the server are logged into the system. This feature is available where the tourist images receipts and enters the necessary details relating to the transactions he made. For example, in Singapore in order to qualify for a tax refund, a minimum $100 must be spent from retailers bearing the same GST registration number and this can be accumulated in up to 3 same-day invoices or receipt, thus the application can immediately alert the user, whether tourist or retailer, if this minimum amount has been reached on the same day. This does away with the current need to check physical receipts

Draft Only

and sum them up.

An additional feature of using a system of intermediate value in the form of rewards points as described in the earlier embodiment can be incorporated into the process. During the purchase (step 240), the tourist informs the retailer that he wishes to use his rewards points, and upon scanning the QR code on the tourist's MDCC (step 250), the rewards points balance is retrieved from the server and displayed to the retailer. Based on this amount and confirmation from the tourist via the tourist's MDCC (step 250) of the number of rewards points to redeem, the retailer would apply the rewards points against the purchase price accordingly and update the server (step 260). In another embodiment, during a purchase (step 240), the tourist who wishes to utilize his intermediate value in the form of rewards points may launch the software application installed on the MDCC 120 to retrieve from the server and display the rewards points balance information. The tourist can inform the retailer of his intention to use his rewards points and scan an identifier, which can be another QR code, unique to the retailer before entering and confirming the number of rewards points he wishes to use, for transmission to the server. The server can then push the number of rewards points to be thus used for display on the issued retailer device or the retailer's own mobile device with the application installed, and the retailer would apply the rewards points against the purchase price accordingly and update the server (step 260). Upon receipt of the eTRS Ticket in the application, the tourist can be prompted to choose whether to convert the amount, with or without a service charge to the CRA, into the rewards points. This raises the possibility of the tourist being able to spend his tourist refund at participating retailers even before leaving the country.

A flowchart shown in Fig. 3 describes an embodiment of how the tax refund is credited/made to the tourist when the tourist is departing the country. At a departing point such as the airport or cruise centre, the installed application on the MDCC 120 is launched by the tourist either on his own volition or reminded by notifications displayed on the mobile device 120. Such

Draft Only

CSC ServiceWorks - Ex. 1002
Page 861 of 1551

notifications can be triggered by detecting that the tourist is at a departure point such as the airport or cruise centre. The tourist is then prompted to confirm that he is departing the country (step 310), which triggers the system 10 (either via the installed software application or the server 110) to notify the tourist of the purchases made to date, the eTRS Tickets collected, the amount of refund available, as well as the amount of outstanding refunds which may be in the form of an intermediate value as described. The tourist also indicates how the refund is to be made, either in cash or to the credit card account that was used (based on the purchase or transaction details), or to a specified bank account or even to another different credit card account. A further prompt whether to convert the refund available may be triggered to allow the tourist to do so.

Once the list of purchases is confirmed and verified by the tourist, the tourist is guided through the various steps of completing the Declaration of Eligibility and displays the tourist's passport details for confirmation. After confirmation, the declaration of eligibility and refund claims are submitted to the server (step 320) and to the CCH and confirmation is sent to the tourist (step 330), together with either an approval Notification slip or an inspection Notification slip if the tourist has been selected for inspection. If the inspection is verified and cleared, an approval Notification slip is issued to the tourist, and based on the approval Notification slip, a refund can be obtained (step 340) either in cash at the Cash Refund Counter at the airport or cruise centre, or credited back to the specified credit/debit card or bank account. Alternatively, the tourist can also choose to obtain the refund in the form of an intermediate value such as the rewards points, especially if he plans to visit the country again sometime soon. The tourist then departs the country (step 350). The Declaration of Eligibility can be submitted together with the refund claims via the application on the mobile device, which means that process is simplified and the tourist can do so at their own convenience, e.g. while queuing to check in or clearing immigration or even in the transport on the way to the airport.

In another embodiment of the present invention and with reference to Fig. 4

Draft Only

CSC ServiceWorks - Ex. 1002
Page 862 of 1551

and 5, wherein like numerals reference like parts, the functions associated with the MDCC 120 and retailer device 130 may be integrated into a single MDCC device 420. Such an arrangement is advantageous in the sense that one single MDCC 420 may be utilized for the whole refund process. It is to be appreciated that either:-

the associated functions described for both mobile device 120 and computing device 130 as earlier described would have to be implemented on the MDCC 420, or

another dedicated software application incorporating essential functions for mobile device 120 and the computing device 130 would have to be installed on the MDCC 420.

In the single device arrangement, the participating retailer's premises may be equipped with a transmitter and/or receiver (including but not limited to Bluetooth Low Energy 'Bluetooth LE' beacons) 410 operable to transmit to/receive from a MDCC 420 (used interchangeably with the term 'single device') within range of the transmitter/receiver.

An example of the single device arrangement 400 is shown in Fig. 4. The arrangement 400 comprises one or more Bluetooth LE (BLE) beacons 410 installed within the retailer's shop at a designated location, such as around a cashier. The BLE beacons 410 can operate in a 'broadcast' or 'advertisement' mode to notify nearby devices of its presence via an address. The address follows a specific format, such as a predefined prefix, followed by a variable UUID, and a major, minor pair. When a user with the MDCC 420, such as a tourist is within the pre-determined range of the designated location, the MDCC 420 detects the BLE beacons 410 and prompts the user to launch his dedicated software application, or directly launches the software application without prompt once the BLE beacons 410 are detected, which can be programmed to inform the user that he is at a participating retailer based on matching and verifying the broadcast format of the BLE. The retailer specific information can then be displayed on the MDCC 420.

The user next shops and transacts at the retailer shop. Upon payment for the merchandise, the tourist requests for a tax refund. The cashier then requests

Draft Only

CSC ServiceWorks - Ex. 1002
Page 863 of 1551

the tourist to send the request for refund from his MDCC 420, together with the refund account number and BLE address to the server 110.

The server 110 opens a session between the user account and the retailer account. The tourist is prompted to scan the transaction receipt using the MDCC 420 via the OCR module as described in previous embodiments, or via other means including manual or POS system as described. Once scanned, the transaction details are displayed on the MDCC 420.

The tourist presents the transaction details to the cashier or other personnel authorized by the retailer. The cashier verifies the transaction details and presents a retailer identifier to the tourist. The retailer identifier may be a QR code. The retailer identifier encoded in the form of a QR code may further comprise one or more of the following information:-

i. Retailer's account number held with the server 110; and

ii. Sub-accounts created by the retailer for each authorized personnel (e.g. cashier).

The sub-accounts provide a means for identifying the cashier in case of suspected transaction activity(ies), such as collusion between cashier and tourist.

The tourist scans the retailer QR code and the software application transmits the same to the server 110 for verification.

Upon receipt of the information related to the retailer identifier, the server 110 matches the QR code with the BLE address to verify that the MDCC 420 is on site. Upon verification, the MDCC 420 transmits the transaction details to the server 110. The server 110 then runs checks on the transaction details. The checks may include (but not limited to) ensuring that the transaction details are current, i.e. with current date and time, and relate to the correct retailer.

Upon completion of the checks, the server 110 then sends the transaction details to the CCH 170. The CCH 170 then acknowledges the lodgement of the refund claim to the server 110. The server 110 generates the eTRS Ticket, assigns the DOC-ID and sends the same to MDCC 420.

With reference to Fig. 5, at the point of departure, such as an airport or cruise center, the location of the MDCC 420 is determined by the software application via GPS or other location-based services. Alternatively, the

Draft Only

CSC ServiceWorks - Ex. 1002
Page 864 of 1551

application on the tourist MDCC 120 can also rely on Wi-Fi networks or cellular base stations at the airport and the cruise centre for detecting the MDCC 420. Once detected, the software application guides the user through the declaration of eligibility as described earlier (see steps 310 to 350). Next the tourist confirms his departure and eligibility. The MDCC 420 then retrieves the transaction records from the server 110 for the tourist to select for refund. Once the user selects the transaction records, he is prompted to select the refund method (e.g. rewards points, direct credit into specified account etc.). Upon selection, the MDCC 420 sends the declaration of eligibility; selected refund transaction(s); and refund method to the server 110. The server 110 in turn transmits the information to the CCH 170. The CCH 170 then replies with an approval or non-approval Notification slip to the server 110, which in turn transmit the approval or non-approval Notification to the MDCC 420. If the refund is approved, the CCH 170 further instructs or informs the CRC 430 to process the refund.

Where the CCH 170 replies with the non-approval notification slip, in some embodiments the tourist may be directed to the customs officer or inspector as described in the earlier embodiment for further inspection. The customs officer may be provided with a separate computer device with a dedicated software application installed thereon to facilitate inspection by the customs officer. A 'customs officer approval' identifier in the form of a QR Code may be provided to the customs inspector to present to the tourist after the customs inspector is satisfied with the eligibility of the tourist. Upon scanning of the 'customs officer approval' QR Code, the server 110 then updates the CCH record as "Approved" and issues a Notification of Approval slip. If still not approved, the purchases will not be eligible for tax refunds.

During a purchase (step 240), the tourist who wishes to utilize his intermediate value in the form of rewards points can inform the retailer of his intention to use his rewards points. He may launch the software application installed on the MDCC 420 to retrieve from the server 110 his rewards points balance and enter and confirm the number of rewards points he wishes to use, before showing to the retailer for verification. Once the retailer has verified the

Draft Only

CSC ServiceWorks - Ex. 1002
Page 865 of 1551

number of rewards points to be used, he can present the tourist with a retailer identifier, which can be another QR code, unique to the retailer, for scanning by the single device 420 as a form of retailer confirmation, and the server will be updated (step 260). The retailer would apply the rewards points against the purchase price accordingly. Also, upon receipt of the eTRS Ticket in-app, the tourist can be prompted to choose whether to convert the amount, with or without a service charge to the server 110, into the rewards points. This raises the possibility of the tourist being able to spend his tourist refund at participating retailers even before leaving the country.

The single device arrangement is based on the use of a mobile device 420 and eliminates the need for a Retailer Device. Instead of issuing each retailer with a separate device, Bluetooth Low Energy (BLE) beacons (transmitters/receivers) can be placed in each retailer outlet, and each authorized personnel may access the retailer's identifier (which may be in the form of a QR code or otherwise) in a variety of ways. For example an authorized personnel such as a cashier at the retailer shop can be provided with a QR Code Staff Pass, or each retailer outlet can be provided with its own QR Code identifier. The BLE can ensure transactions only take place at participating shops and the QR Code Staff Pass or identifier acts as retailer acknowledgement that the cashier has done her checks. The BLE can also be used to push targeted retailing information to the tourist, e.g. discounts, advertisements, etc. It is to be appreciated that both the QR code and BLE may be utilized in the form of a two-layered check to ensure that the transactions take place within the retailer's shop or premise. Such a two-layered check reduces the risk of any collusion between a member of the retailer's staff and the tourist.

In some embodiments, the server 110 may be operating the system of intermediate value. In such an arrangement, the server 110 may comprise a predictive engine operable to predict which user refund account is likely to be fraudulent so as to be able to take pre-emptive action. Otherwise the system may compromise on account integrity. The predictive engine can be based on at least one criterion of user demographics (e.g. location, countries visited for a past predetermined time frame), transaction profile (e.g. value of

Draft Only

CSC ServiceWorks - Ex. 1002
Page 866 of 1551

transaction, type of goods, etc.), the type of identifier (e.g. credit card) used to register for a refund account, gender, nationality etc. Based on these criteria, an algorithm can be developed to run in the server 110 to pick out suspicious user accounts. For example, the predictive engine may attribute high risk weights to transactions exceeding certain value arising from certain countries. In some embodiments, in addition to identifying suspicious user accounts, the predictive engine may further be configured to data communicate and send selected details relating to the 'suspicious accounts' to the relevant authorities, which include the customs. The selected details are sent to the authorities for further follow up checks in order to provide a more targeted and focused check In other embodiments, the system 10 may refuse the registration of any requested refunds accounts deemed not to pass an initial security check based on one or more of the at least one criterion. In yet other embodiments, based on the profile identified by the predictive engine, selected users or tourists may be banned from purchasing certain tax free eligible items. In some embodiments, the predictive engine may be arranged in data communication with one or more database servers, such database servers for maintaining user information.

The above arrangements are advantageous in that more parameters for the selection of tourists for inspection are considered, compared to that considered by the CCH 170 currently. In addition, the selection performed at the servers 110 effectively provide an additional layer of check which is pre-emptive in nature, as compared to that currently done at the exit point(s) which is 'reactive'. In this regard, it is to be appreciated that the existing system performs selection at the end of a tourist's trip/visit which is deemed less efficient compared to selection performed before the tourist starts his trip. This is because based on the existing structure, the retailers would have already taken the trouble to process the eTRS transactions of a fraudster, only for the transactions to be subsequently found invalid (this is assuming the CCH is able to select the tourist for inspection) when the fraudster attempts to make a claim for a refund as he leaves the country. The above arrangements effectively prevent suspicious transactions from being performed by would-be

Draft Only

CSC ServiceWorks - Ex. 1002
Page 867 of 1551

fraudsters, saving time and effort for both the retailers as well as the Customs. In another embodiment, the server 110 is configured to link to at least one retailer for the provision of one or more retailer item list(s) available for sale and tax refund. In the app installed on the tourist's MDCC 120, a user interface may then be provided to the tourist which displays the retailer item list of available items for sale and/or tax refund for the tourist to view before the tourist arrives at the country and/or before he/she leaves the country. Once a wish list or checklist of selected items from a tourist is communicated to the server 110 via the app, the server 110 is operable to provide a list of retailer(s) and details of the retailers selling the one or more items, via a data push or pull mechanism that the tourist desire to purchase. The wish list and retailer list may be compared by any compare and match algorithm between the entries on the tourist's wish-list with what the retailers have to offer. The compare and match may be performed at the server 110 side or the app installed on the MDCC 120.

In the creation of the tourist's checklist, the tourist can record a plurality of parameters related to each item. Non-exhaustive examples of these parameters may include the item's name, category, quantity and recipient's name and insert short notes and images (such as pictures) related to each item. Newly created items can be added to a temporary 'pending list' which the tourist can check off to move the items to a completed list whenever a purchase is made. Interfaces for sorting the items in alphabetical or other order may also be provided to the user.

Each time the tourist creates a new item, the app is operable to retrieve a list of retailer(s) selling the item from the server 110, and then provide to the tourist, retailers that sell the item or related items. The tourist can download the names of the recommended retailers to add them to his shopping list (via an interface) or to access the retailer's profile on the app. Through the list and/or a BLE located at the retailer's outlet, the tourist can be notified by the server 110 via the app and/or the retailer that sells the item or related items whenever the tourist is near to the retailer's shop and/or send content e.g. sales voucher from the retailer to the Tourist. This is advantageous to provide

Draft Only

CSC ServiceWorks - Ex. 1002
Page 868 of 1551

a seamless experience for the tourist and to aid the retailers in selling their products. Further, the arrangement provides an advantageous hybrid between a pure online shopping experience and a real shopping experience where goods can be inspected before it is purchased. Amongst other advantages, the above arrangement reduces the shopping time required for a tourist to look or source for an item and whether that item is eligible for tax refund; provides an alert or other forms of notification when the tourist is nearby a retailer; and provides an informed list on prices and quality before committing to the purchase.

In some embodiments, the server 110 is operable to issue one eTRS ticket for each refund claim at each retailer store and charge a service fee for each eTRS Ticket issued. Each eTRS Ticket may comprise more than one sales receipt accumulated at the same store (GSTN), subject to one or more regulations to meet a minimum threshold eligible for refund (e.g. SGD 100). For each eTRS ticket issued, the server 110 may also be required to pay a CCH Fee of SGD 1.50.

As an alternative embodiment, instead of issuing an electronic ticket in the form of an eTRS ticket for each transaction, the server 110 is instead operable to issue a provisional eTRS for the first transaction eligible for a refund claim, and add all subsequent transaction receipts to this provisional eTRS ticket. This is akin to a batch mode process and allows multiple retailers' transactions to be combined into a single formal/final eTRS ticket. The formal eTRS ticket will be issued only when the tourist is at an approved departure point. In such a way, both the user and the service provider may save on CCH Fees because only one Refund Ticket per user per trip is issued, instead of one Refund Ticket per user, per store, per trip. This can be performed without compromising on security or authenticity, as the tourist user will have to undergo the verification step at each retailer store.

In some embodiments, users of the system, such as approved retailers, may be provided with a user interface accessible to a portal, the user interface accessible via any computer device such as, but not limited to, a mobile device. The user interface may be used to display business information related to the retailer described as follow. An example of the interface is a

Draft Only

CSC ServiceWorks - Ex. 1002
Page 869 of 1551

webpage. The server will retrieve and store input received from various sensors such as Bluetooth LE beacons, image capturing devices located around the retailer's shop, for purpose of tracking, monitoring, obtaining, and/or deriving one or more parameters associated with the retailer. Examples of such one or more parameters include number of shoppers in a retailer shop. Such data may be provided on a real-time or near real-time basis displayed on the user interface. The data obtained may be further analyzed to provide business intelligence information useful for the retailer. Such business intelligence information may include shopper traffic in the retailer shop, busiest period of a weekday or weekend, busiest period over one or more months, etc.

In some embodiments, the system may be linked up with other commercial databases related to cruise ship services for example, to provide users with information such as Qualifying Cruise Ships eligible for tourist refund, as well as pre-populating travel itinerary to achieve certain level of convenience for the users of the system.

The described embodiments are advantageous as they provide a three-tier checking and verification process. In particular, a first level of check/verification is performed when a user (tourist) registers with the central processor 110. The second level of check/verification is performed before or during the generation of the eTRS ticket, and the third level of check/verification is performed at the point of departure prior to the generation of an electronic notification indicating the success or failure of the refund transaction.

Further, it is to be appreciated that the capturing of detailed information at the point of user registration allows a tourist to specify a desired account for refund upfront. Such an arrangement is useful to alleviate any time pressure that a tourist may face when he is leaving the country, as he needs to complete all form of formalities prior to boarding the aircraft / cruise ship. By shifting the data collection point to prior to the tourist embarking on his trip or

Draft Only

CSC ServiceWorks - Ex. 1002
Page 870 of 1551

at the point of registration, precious time is saved for the tourist when he faces the most time pressure.

The above is a description of embodiments of systems and methods for facilitating refunds, in particular tax refunds to tourists in accordance with the present invention. It is envisioned that those skilled in the art can design alternative embodiments of this invention that falls within the scope of the invention. In particular, it is to be appreciated that features from various embodiment(s) may be combined to form one or more additional embodiments. Further, the following are non-exhaustive examples of features that may be combined with the described embodiments to form further embodiments that falls within the scope of the invention:-

- In the single device embodiment, the user (tourist) may send both the retailer identifier and the transaction details to the server 110 for further processing upon scanning the retailer QR code. As a pre-requisite, the server 110 will however process the transaction details if and only if the retailer identifier is verified.
- The verification or scanning of the retailer's identifier may be performed either during the refund qualifying transaction is made or after. In the former case, the transaction details are captured before the retailer identifier is scanned before transmission to the server 110. This is particularly relevant for the single device embodiment. In the latter case, the retailer identifier may be verified or scanned for purpose of opening the transaction session before either the user or an authorized representative of the retailer retrieves the transaction details.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 871 of 1551

WE CLAIM

1. A system for facilitating refund to a user comprising:

a mobile device having means to communicate with a central processor for the generation of a refund account and a unique identifier; the unique identifier associated with the user;

a computer device operable to access the unique identifier for verification upon receipt of a refund qualifying transaction associated with the user, the computer device further operable to receive and send information relating to the refund qualifying transaction and generate a refund request upon successful verification; and

the central processor operable to be in data communication with the computer device to receive or send information relating to verification of the unique identification and the refund qualifying transaction and process the verification or refund request, the central processor further configured to generate an electronic ticket to be sent to the mobile device for the generation of a refund upon successful process of the refund request.

2. The system according to claim 1, wherein the refund is a tax refund and in the form of an intermediate value.

3. The system according to claim 2, wherein the intermediate value is derived from the actual value of refund based on a conversion rate.

4. The system according to claim 1, wherein the computer device is a point-of-sale device, the point-of-sale device is configured to directly send information relating to the refund qualifying transaction to the central processor.

5. The system according to claim 1, wherein the unique identifier is encoded as a quick response (QR) code and the computer device accesses the unique identifier by scanning the QR code displayed on the mobile device.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 872 of 1551

6. The system according to claim 1, wherein the central processor is operable to send the electronic ticket to a third party server for further verification of the refund qualifying transaction and confirmation of the refund.

7. The system according to claim 6, wherein the central processor stores the information relating to the refund qualifying transaction in a database before the electronic ticket is generated and sent to the third party server.

8. The system according to claim 1, wherein the mobile device is operable to send an electronic notification related to a requirement being met.

9. The system according to claim 8, wherein the requirement is a confirmation of departure.

10. The system according to claim 8, wherein the requirement is a Declaration of Eligibility.

11. The system according to claim 10, wherein the mobile device is operable to receive a notification of refund issued by a third party server once the electronic ticket is processed successfully.

12. The system according to claim 1, wherein the central processor is operable to receive a notification of refund issued by a third party server once the at least one electronic ticket is processed successfully and the central processor is operable to send a notification of refund to the mobile device.

13. The system according to claim 1, wherein the unique identifier associated with the user is generated based on a passport information of the user.

14. The system according to claim 13, wherein the unique identifier is generated after a registration process by the user.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 873 of 1551

15. The system according to claim 13, wherein the unique identifier is further associated with an image capture of the passport.

16. The system according to any one of the preceding claims, wherein the mobile device is integrated with the computing device.

17. The system according to any one of the preceding claims, wherein the central processor is operable to send a notification to the mobile device indicating the success or failure of the refund request.

18. The system according to claim 1, wherein there comprises another unique identifier associated with a retailer using the computer device.

19. The system according to claim 18, wherein the another unique identifier is generated after a registration process by the retailer.

20. The system according to claim 18, wherein the another unique identifier is further associated with an image capture of one or more account information associated with the retailer.

21. The system according to claim 1, wherein if the unique identifier is not accessible by the computer device, the computer device is operable to obtain an alternative identifier for verification and send the alternative identifier to the central processor.

22. The system according to claim 21, wherein upon receipt of the alternative identifier, the central processor is operable to determine whether a corresponding refund account associated with the user is present and if not, the central processor is operable to generate the refund account and the unique identifier based on the alternative identifier.

23. The system according to claim 2, wherein the central processor comprises a database for storing at least one retailer list of goods and

Draft Only

CSC ServiceWorks - Ex. 1002
Page 874 of 1551

services eligible for tax refund.

24. The system according to claim 23, wherein the central processor is operable to receive a wish-list of goods and services from the mobile device and upon receipt of the wish-list, compare the wish-list with the at least one retailer list of goods and services.

25. The system according to claim 24, wherein when there is a match between the wish-list and the at least one retailer list, the central processor is operable to provide a matched list to the mobile device.

26. The system according to claim 1, wherein the electronic ticket is a provisional electronic ticket, the provisional electronic ticket comprises a plurality of electronic receipts.

27. The system according to claim 26, wherein the provisional electronic ticket is converted to a final electronic ticket at an approved departure point.

28. The system according to claim 1, the central processor arranged in data communication with at least one third party server to retrieve information related to the identity of the user, and sends the information related to the identity of the user to the computer device

29. A method for facilitating a refund to a user comprising the steps of:

communicating via a mobile device with a central processor for the generation of a refund account and a unique identifier, the unique identifier associated with the user;

via a computer device,

accessing the unique identifier for verification on receipt of a refund qualifying transaction associated with the user;

generating a refund request upon successful verification; and

sending information relating to the refund qualifying transaction

Draft Only

via a central processor,

receiving and processing the refund request;,

wherein the central processor is further configured to generate an electronic ticket to be sent to the mobile device for the generation of a refund upon successful process of the refund request.

30. The method of claim 29, further including the step of converting the refund to an intermediate value after the generation of the refund.

31. The method of claim 30 wherein the intermediate value is derived from the actual value of refund based on a conversion rate.

32. The method of claim 29 further comprising the step of exporting the information relating to the refund qualifying transaction via a point-of-sale (POS) device in data communication with the computer device, the point-of-sale device is configured to directly send information relating to the refund qualifying transaction to the central processor.

33. The method of claim 29 wherein the computer device accesses the unique identifier by scanning an image shown on the mobile device.

34. The method according to claim 29, further comprising the step of sending the electronic ticket to a government server for further verification of the refund qualifying transaction and confirmation of the refund.

35. The method according to claim 34, wherein the mobile device is operable to send an electronic notification related to a requirement being met.

36. The method according to claim 35, wherein the requirement is a confirmation of departure.

37. The method according to claim 35, wherein the requirement is a Declaration of Eligibility.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 876 of 1551

38. The method of claim 29 wherein the generation of electronic ticket is based upon one or more requirements being met.

39. The method of claim 35 further comprising the step of sending an electronic notification to the mobile device indicating the success or failure of the refund request.

40. The method according to claim 29, further comprises a step of obtaining an alternative identifier for verification and sending the alternative identifier to the central processor if the unique identifier is not accessible by the computer device.

41. The method according to claim 29, wherein upon receipt of the alternative identifier, the central processor is operable to determine whether a corresponding refund account associated with the user is present and if not, the central processor is operable to generate the refund account and the unique identifier based on the alternative identifier.

42. The method according to claim 29, wherein the central processor comprises a database for storing at least one retailer list of goods and services eligible for tax refund.

43. The method according to claim 31, wherein the central processor is operable to receive a wish-list of goods and services from the mobile device and upon receipt of the wish-list, compare the wish-list with the at least one retailer list of goods and services.

44. The method according to claim 32, wherein when there is a match between the wish-list and the at least one retailer list, the central processor is operable to provide a matched list to the mobile device.

45. The method according to claim 29, wherein the electronic ticket is a

Draft Only

CSC ServiceWorks - Ex. 1002
Page 877 of 1551

provisional electronic ticket, the provisional electronic ticket comprises a plurality of electronic receipts.

46. The method according to claim 45, wherein the provisional electronic ticket is converted to a final electronic ticket at an approved departure point.

47. A non-transitory computer readable medium containing executable software instructions thereon wherein when executed on a mobile device and/or a computer device performs the method of facilitating a refund to a user comprising the steps of:

communicating via the mobile device with a central processor for the generation of a refund account and a unique identifier, the unique identifier associated with the user;

accessing the unique identifier for verification via a computer device on receipt of a refund qualifying transaction associated with the user;

sending information relating to the refund qualifying transaction;

generating a refund request upon successful verification; and

receiving and processing the refund request by a central processor,

wherein the central processor is further configured to generate an electronic ticket to be sent to the mobile device for the generation of a refund upon successful process of the refund request.

48. The non-transitory computer readable medium according to claim 47, further comprising a software instruction to send an electronic notification to the mobile device indicating the success or failure of the refund request.

49. The system of claim 1, wherein if the refund request is not successfully processed, the central processor is arranged in data communication with another computer device provided to an authorized personnel to perform further processing.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 878 of 1551

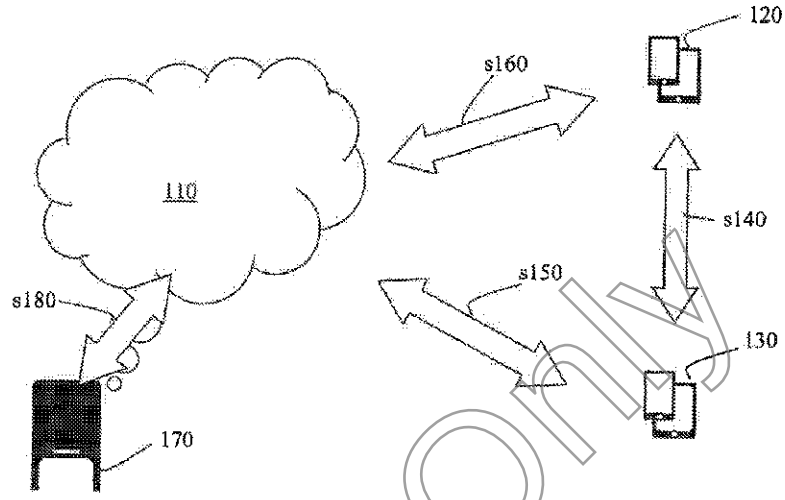


FIG. 1

Draft Only

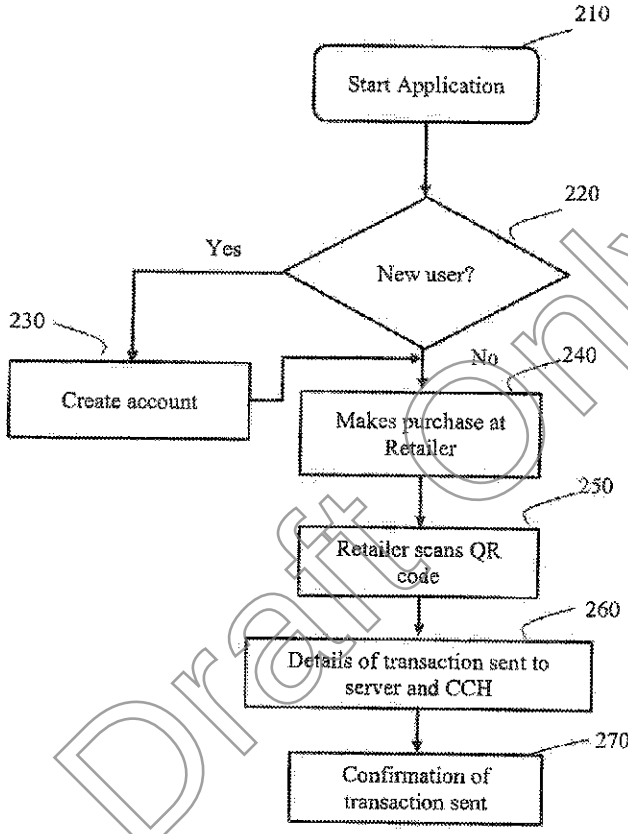
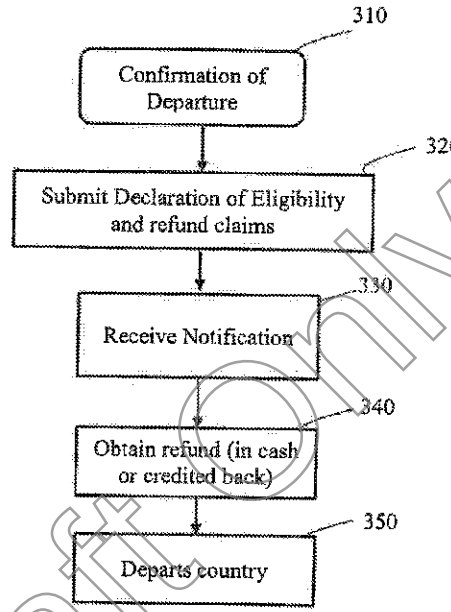


FIG. 2

Draft Only



Draft Only

FIG. 3

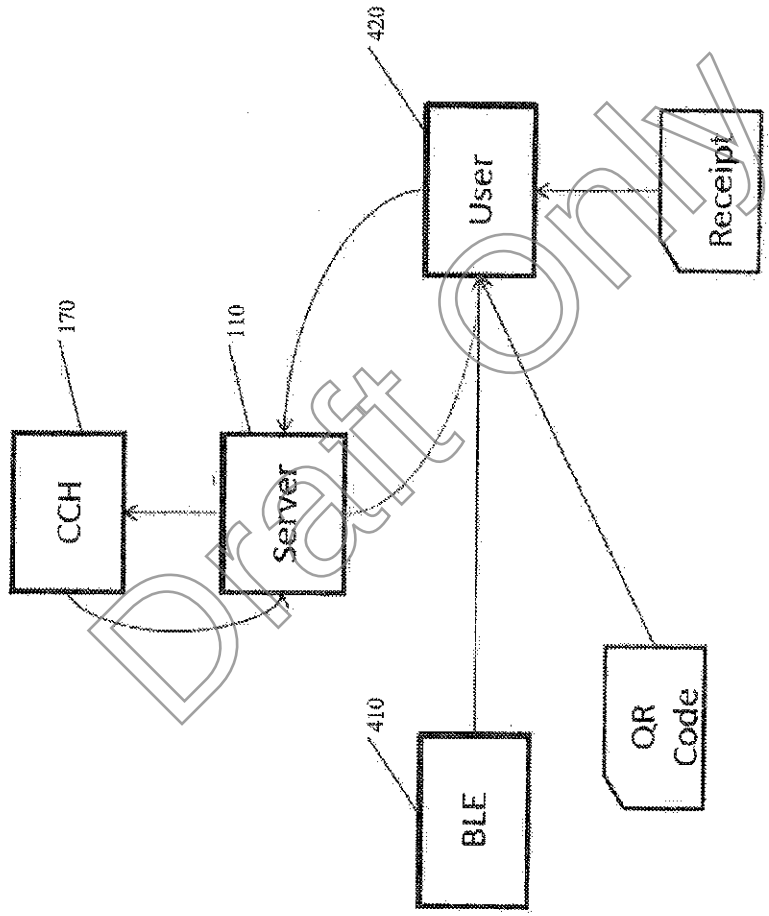
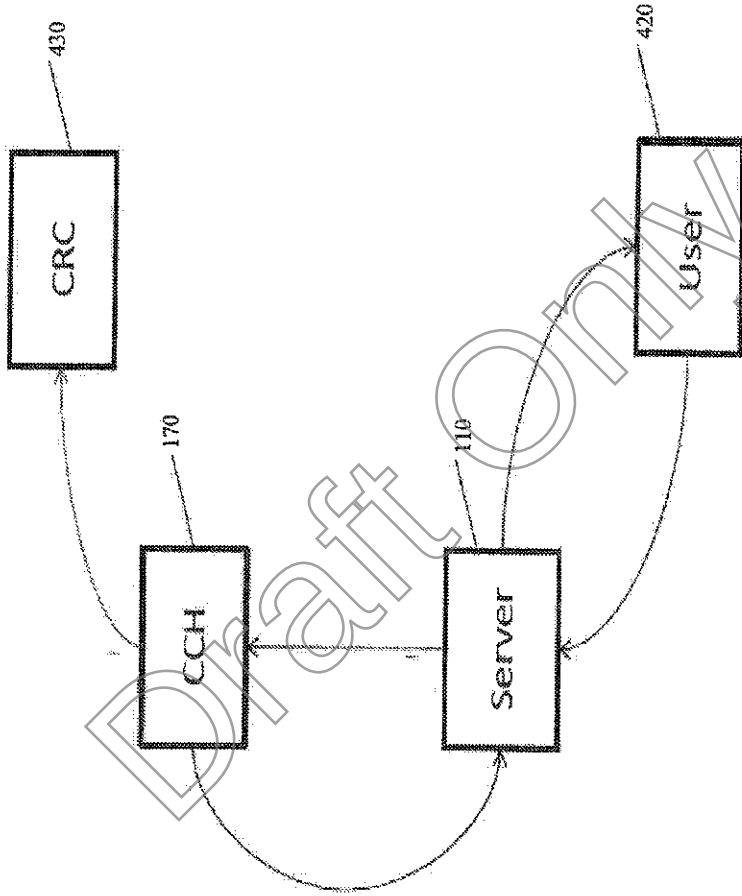


FIG. 4

Draft Only



Draft Only

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2016/050297

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/32 (2012.01) *G06Q 40/02 (2012.01)*

According to International Patent Classification (IPC)

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q

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)

FAMPAT: mobile device, smartphone, tax, VAT, GST, refund, rebate, reimbursement, electronic ticket, voucher, QR code and other related terms

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KR 10-2014-0032089 A (KTIS CORPORATION) 14 March 2014 paragraphs [0001], [0025], [0068]-[0071], [007e], [0077], [0086]-[0088], [0113], [0114], [0124], [0125] of the machine translation	1-49
A	WO 2011/147912 A1 (GLOBAL BLUE HOLDINGS AB) 1 December 2011 paragraphs [0069], [00143], [00153]	-
A	US 2015/0127534 A1 (BHAMBHANI, M. M.) 7 May 2015 paragraph [0035]	-
A L	How VAT refund claim on purchases works, 6 July 2015 [Retrieved on 2016-09-28 from https://web.archive.org/web/20150706170705/http://www.optimal-tax-free.com/en/vat-refund/; for the purpose of establishing publication date of this citation] the whole document	-

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

*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
28/09/2016 (day/month/year)	30/09/2016 (day/month/year)

Name and mailing address of the ISA/SG

IPOS INTELLECTUAL PROPERTY OFFICE OF SINGAPORE

Intellectual Property Office of Singapore
51 Bras Basah Road
#01-01 Manulife Centre
Singapore 189554

Authorized officer

Lee Yi Chau

Draft Only

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/SG2016/050297

Note: This Annex lists known patent family members relating to the patent documents cited in this International Search Report. This Authority is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
KR 10-2014-0032089 A	14/03/2014	WO 2014/038775 A1	13/03/2014
WO 2011/147912 A1	01/12/2011	AU 2011257210 A1	06/12/2012
		AU 2011257210 B2	21/05/2015
		AU 2011257210 B8	11/06/2015
		EP 2577592 A1	10/04/2013
		EP 2577593 A1	10/04/2013
		EP 2577595 A1	10/04/2013
		EP 2577596 A1	20/04/2013
		GB 2480662 A	30/11/2011
		GB 2480664 A	30/11/2011
		JP 2013-527555 A	27/06/2013
		JP 5764751 B2	29/07/2015
		JP 2013-534653 A	05/09/2013
		JP 5791128 B2	07/10/2015
		KR 2013-0052577 A	22/05/2013
		KR 101560868 B1	15/10/2015
		KR 2013-0050943 A	16/05/2013
		KR 2015-0036708 A	08/04/2015
		SG 176401 A1	29/12/2011
		SG 176403 A1	29/12/2011
		SG 176405 A1	29/12/2011
		WO 2011/147913 A1	01/12/2011
		WO 2011/147914 A1	01/12/2011
		WO 2011/147918 A1	01/12/2011
US 2015/0127534 A1	07/05/2015	NONE	

Draft Only

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 August 2016 (04.08.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/123545 A1

(51) International Patent Classification:
G06Q 30/02 (2012.01) *G06Q 30/06* (2012.01)
G06Q 20/18 (2012.01)

(21) International Application Number:
PCT/US2016/015763

(22) International Filing Date:
29 January 2016 (29.01.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14/611,065 30 January 2015 (30.01.2015) US
14/614,336 4 February 2015 (04.02.2015) US

(71) Applicant: **PAYRANGE, INC.** [US/US]; 700 NE Multomah Street, Suite 1400, Portland, OR 97232 (US).

(72) Inventor: **PATEL, Paresh, K.**; 700 NE Multomah Street, Suite 1400, Portland, OR 97232 (US).

(74) Agents: **CRISMAN, Douglas J.** et al.; Morgan Lewis & Bockius LLP, 2 Palo Alto Square, 3000 El Camino Real, Suite 700, Palo Alto, CA 94306 (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, BN, BR, BW, BY, BZ, CA, CH, CL, 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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report (Art. 21(3))*

(54) Title: METHOD AND SYSTEM FOR PROVIDING OFFERS FOR AUTOMATED RETAIL MACHINES VIA MOBILE DEVICES

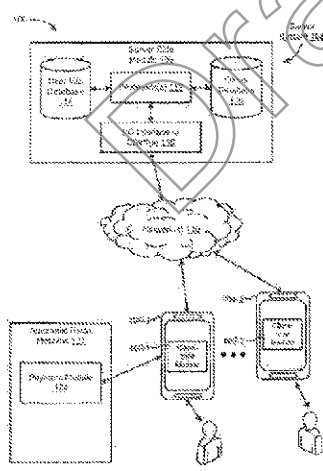


Figure 1

(57) Abstract: A mobile device with a display, processor(s), and memory: displays promotional offers; detects a user input selecting one of the promotional offers; and initiates performance of a transaction with an automatic retail machine to purchase a product stocked by the automatic retail machine. The mobile device also: receives a transaction completion notification from the payment module indicating that the product corresponding to the selected promotional offer was vended by the automatic retail machine; and, in response to receiving the transaction completion notification, provides a prompt to the user of the mobile device to obtain a product code for the vended product to validate the promotional offer. The mobile device further: obtains the product code for the vended product; transmits the product code to the server; and, in response: receives promotion validation information from the server; and displays the promotion validation information indicating whether the respective promotion offer was validated.

Draft Only

WO 2016/123545 A1

METHOD AND SYSTEM FOR PROVIDING OFFERS FOR AUTOMATED RETAIL MACHINES VIA MOBILE DEVICES

TECHNICAL FIELD

[0001] The present application relates to the field of payment processing systems, and in particular, to a mobile-device-to-machine payment processing system over a non-persistent network connection.

BACKGROUND

[0002] Vending machines (or more broadly "automatic retail machines"), in the broadest sense, have been around for thousands of years. The first simple mechanical coin operated vending machines were introduced in the 1880s. Modern vending machines stock many different types of products including, but not limited to drinks (e.g., water, juice, coffee, and soda) and edible food products/items (e.g., snacks, candy, fruit, and frozen meals), as well as a wide variety of non-food items. In this fast paced world, vending machines are ubiquitous.

[0003] Vending machines are one type of "payment accepting unit" (payment accepting units are also referred to herein generically as "machines"). A payment accepting unit (or machine) is equipment that requires payment for the dispensing of products and/or services. In addition to vending machines, payment accepting units can also be other machines that require payment for the dispensing of a product and/or services including, but not limited to parking meters, toll booths, laundromat washers and dryers, arcade games, kiosks, photo booths, toll booths, transit ticket dispensing machines, and other known or yet to be discovered payment accepting units.

[0004] In using a payment accepting unit, a user will (1) approach the payment accepting unit, (2) determine from the face of the payment accepting unit the product (or service) he/she desires, (3) insert payment (e.g., coins, bills, or payment cards), and (4) input his/her selection into the payment accepting unit using a user interface (e.g., a series of buttons, a key pad, touch screen, or other input mechanism using, for example, the column and row at which a product is located). Based on the user's inputted selection, technology within the payment accepting unit provides the desired product (or service) to the user.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 887 of 1551

[0005] As the number of people with Internet-connected mobile devices proliferates, so does the variety of uses for such devices. Mobile payment is a logical extension. There is a large development effort around bringing mobile payment to the retail sector in an effort to not only provide options to the user, but also increased convenience.

SUMMARY

[0006] In some implementations, a method of providing and handling promotional offers for an automatic retail machine is performed at a mobile device (e.g., the mobile device 104, Figures 1-2) with a display, one or more processors, and memory. The method includes: displaying one or more promotional offers on the display; detecting a user input selecting a respective promotional offer of the one or more promotional offers; and initiating performance of a transaction with an automatic retail machine coupled with a payment module, where the transaction corresponds to purchase of a product stocked by the automatic retail machine. The method also includes: receiving a transaction completion notification from the payment module, where the transaction completion notification indicates that the product corresponding to the selected respective promotional offer was vended by the automatic retail machine; and, in response to receiving the transaction completion notification, providing a prompt to the user of the mobile device to obtain a product code for the vended product to validate the respective promotional offer. The method further includes: obtaining the product code for the vended product; after obtaining the product code, transmitting the product code to the server; and, in response to transmitting the product code: receiving promotion validation information from the server; and displaying the promotion validation information on the display, where the promotion validation information indicates whether the respective promotion offer was validated.

[0007] In some implementations, a mobile device (e.g., the mobile device 104, Figures 1-2) includes a display, one or more processors, and memory storing one or more programs for execution by the one or more processors, the one or more programs include instructions for performing, or controlling performance of, the operations of any of the methods described herein. In some implementations, a non-transitory computer readable storage medium storing one or more programs, the one or more programs comprising instructions, which, when executed by a mobile device (e.g., the mobile device 104, Figures 1-2) with one or more processors and a display, cause the computing device to perform, or control performance of, the operations of any of the methods described herein. In some

Draft Only

implementations, a mobile device (e.g., the mobile device 104, Figures 1-2) includes means for performing, or controlling performance of, the operations of any of the methods described herein.

[0008] (A1) In some implementations, a method is performed at a mobile device including a display, one or more processors, and memory. The method includes: displaying one or more promotional offers on the display; detecting a user input selecting a respective promotional offer of the one or more promotional offers; and initiating performance of a transaction with an automatic retail machine coupled with a payment module. In some implementations, the transaction corresponds to purchase of a product stocked by the automatic retail machine. The method also includes: receiving a transaction completion notification from the payment module, wherein the transaction completion notification indicates that the product corresponding to the selected respective promotional offer was vended by the automatic retail machine. In response to receiving the transaction completion notification, the method includes: providing a prompt to the user of the mobile device to obtain a product code for the vended product to validate the respective promotional offer. The method further includes: obtaining the product code for the vended product. After obtaining the product code, the method includes: transmitting the product code to the server. In response to transmitting the product code, the method includes: (i) receiving promotion validation information from the server, and (ii) displaying the promotion validation information on the display. In some implementations, the promotion validation information indicates whether the respective promotion offer was validated.

[0009] (A2) In some implementations of the method of A1, the one or more promotional offers are identified based on at least one of: a unique identifier corresponding to the payment module, at least one of a current time and date, a location of the automatic retail machine, a location of the mobile device, and a unique identifier corresponding to the user of the mobile device.

[0010] (A3) In some implementations of the method of any one A1-A2, the method includes: prior to displaying the one or more promotional offers: (i) obtaining an information packet broadcast by the payment module coupled with the automatic retail machine, the information packet including at least an authorization code and a unique identifier corresponding to the payment module; (ii) sending a transaction authorization request to a server, wherein the transaction authorization includes the authorization code and the unique

Draft Only

CSC ServiceWorks - Ex. 1002
Page 889 of 1551

identifier corresponding to the payment module; and, (iii) in response to the transaction authorization request, receiving authorization information from the server that includes an authorization grant token for initiating a transaction with the automatic retail machine coupled with the payment module and the one or more promotional offers from the server.

[0011] (A4) In some implementations of the method of any one of A3, performance of the transaction with the automatic retail machine coupled with the payment module is initiated by sending the authorization grant token to the payment module, the authorization grant token including the authorization code included in the broadcast information packet.

[0012] (A5) In some implementations of the method of any one of A1-A4, obtaining the product code further includes: (i) capturing an image of the product that includes the product code; and (ii) extracting the product code from the captured image.

[0013] (A6) In some implementations of the method of any one of A1-A5, obtaining the product code further includes: scanning the product code of the product with a scanner unit of the mobile device.

[0014] (A7) In some implementations of the method of any one of A1-A6, the promotion validation information indicates the price of the product after the application of the respective promotional offer.

[0015] (A8) In some implementations of the method of any one of A1-A7, the method further includes: after obtaining the product code, determining whether a predetermined time period has expired. In accordance with a determination that the time period has expired, the method includes: providing a notification to the user of mobile device indicating that the respective promotional offer has expired. In accordance with a determination that the time period has not expired, the method includes: transmitting the product code to the server.

[0016] (A9) In some implementations of the method of any one of A1-A8, the method includes: transmitting the transaction completion notification to the server.

[0017] (A10) In some implementations of the method of any one of A1-A9, the mobile device further includes a first transceiver associated with a short-range communication protocol and a second transceiver associated with a long-range communication protocol.

Draft Only

[0018] (A11) In an additional aspect, a method is performed at a mobile device including a display, one or more processors, a short-range transceiver (e.g., a first communication unit), a long-range transceiver (e.g., a second communication unit) that is distinct from the short-range transceiver, and memory. In some implementations, the method includes: recognizing, by an application executing on the mobile device, an automatic retail machine based at least in part on a signal strength corresponding to broadcasted information from an electronic payment device coupled with the automatic retail machine. The method also includes: displaying one or more promotional offers that are associated with the automatic retail machine on the display. In some implementations, the method further includes: detecting a user input selecting a respective promotional offer of the one or more promotional offers. The method additionally includes: initiating, via the short-range transceiver, performance of a transaction with the automatic retail machine, the transaction corresponding to purchase of a product stocked by the automatic retail machine. The method also includes: receiving, via the short-range transceiver, a transaction completion notification from the electronic payment device, the transaction completion notification indicating that the product was vended by the automatic retail machine. In response to receiving the transaction completion notification, the method includes: providing a prompt instructing a user of the mobile device to obtain a product code for the vended product. The method further includes: obtaining, based on user input provided in response to the prompt, the product code for the vended product. After obtaining the product code, the method includes: transmitting, via the long-range transceiver, the product code to a server. In response to transmitting the product code: (i) receiving, via the long-range transceiver, promotion validation information from the server; and (ii) based on the promotion validation information, displaying, on the display, an indication as to whether the respective promotional offer was validated and information identifying a credit to the user after application of the respective promotional offer.

[0019] (A12) In some implementations of the method of A11, the method further includes any of the operations described in A2-A10 above.

[0020] Various advantages of the present application are apparent in light of the descriptions below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] The aforementioned features and advantages of the disclosed technology as well as additional features and advantages thereof will be more clearly understood hereinafter

Draft Only

CSC ServiceWorks - Ex. 1002
Page 891 of 1551

as a result of a detailed description of preferred implementations when taken in conjunction with the drawings.

[0022] To describe the technical solutions in the implementations of the present disclosed technology or in the prior art more clearly, the following briefly introduces the accompanying drawings required for describing the implementations or the prior art. Apparently, the accompanying drawings in the following description show merely some implementations of the present disclosed technology, and persons of ordinary skill in the art may still derive other drawings from these accompanying drawings without creative efforts.

[0023] Figure 1 is a block diagram of a payment processing system in accordance with some implementations.

[0024] Figure 2 is a block diagram of a mobile device in accordance with some implementations.

[0025] Figure 3 is a block diagram of a server system in accordance with some implementations.

[0026] Figure 4 is a schematic block diagram of an automatic retail machine in accordance with some implementations.

[0027] Figure 5 is a block diagram of a payment module in accordance with some implementations.

[0028] Figure 6A is a perspective view of the payment module of Figure 5 (e.g., an in-line dongle adapter) in accordance with some implementations.

[0029] Figure 6B is a perspective view taken from the first end of the payment module of Figure 6A in accordance with some implementations.

[0030] Figure 6C is a perspective view taken from the second end of the payment module of Figure 6A in accordance with some implementations.

[0031] Figure 7 is a perspective view of the payment module of Figure 6A within the automatic retail machine of Figure 4 in accordance with some implementations.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 892 of 1551

[0032] Figure 8 is a schematic flow diagram of a process for initiating a transaction in accordance with some implementations.

[0033] Figure 9 is a schematic flow diagram of a process for acknowledging a transaction in accordance with some implementations.

[0034] Figure 10A is a block diagram of an information packet broadcast by the payment module in accordance with some implementations.

[0035] Figure 10B is a block diagram of an authorization request in accordance with some implementations.

[0036] Figure 10C is a block diagram of an authorization grant token in accordance with some implementations.

[0037] Figure 10D is a block diagram of transaction information generated by the payment module in accordance with some implementations.

[0038] Figures 11A-11G illustrate exemplary user interface for displaying promotional offers in accordance with some implementations.

[0039] Figures 12A-12C illustrate a flowchart diagram of a method of providing and handling promotional offers for an automatic retail machine in accordance with some implementations.

[0040] Like reference numerals refer to corresponding parts throughout the several views of the drawings.

Draft Only

DESCRIPTION OF IMPLEMENTATIONS

[0041] Reference will now be made in detail to implementations, examples of which are illustrated in the accompanying drawings. In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of the subject matter presented herein. But it will be apparent to one skilled in the art that the subject matter may be practiced without these specific details. In other instances, well-known methods, procedures, components, and circuits have not been described in detail so as not to unnecessarily obscure aspects of the implementations.

CSC ServiceWorks - Ex. 1002
Page 893 of 1551

[0042] The following clearly and completely describes the technical solutions in the implementations of the present application with reference to the accompanying drawings in the implementations of the present application. Apparently, the described implementations are merely a part rather than all of the implementations of the present application. All other implementations obtained by persons of ordinary skill in the art based on the implementations of the present application without creative efforts shall fall within the protection scope of the present application.

[0043] Figure 1 illustrates a payment processing system 100. Figures 2-5 illustrate example devices within the payment processing system 100. Figures 6A-6C and 7 show various views of the payment module 124 and the automatic retail machine 122. Figure 8 illustrates a schematic flow diagram of a process 800 for initiating a transaction within the payment processing system 100. Figure 9 illustrates a schematic flow diagram of a process 900 for acknowledging a transaction within the payment processing system 100. Figures 10A-10D illustrate data structures associated with initiating and performing transactions within the payment processing system 100. Figures 11A-11G illustrate example user interfaces for displaying promotional offers. Figures 12A-12C illustrate a flowchart diagram of a method 1200 of providing and handling promotional offers for an automatic retail machine. The user interfaces in Figures 11A-11G are used to illustrate the method in Figures 12A-12C.

EXAMPLE DEVICES AND SYSTEMS

[0044] Figure 1 is a block diagram of a payment processing system 100 in accordance with some implementations. In accordance with some implementations, the payment processing system 100 includes client-side processing 102-1, 102-2 (hereinafter "client-side modules 102") executed on a mobile device 104-1, 104-2, server-side processing 106 (hereinafter "server-side module 106") executed on a server system 108 (sometimes also herein referred to as "the server"), and a payment module 124 coupled with an automatic retail machine 122. The client-side module 102 provides client-side functionalities for the payment processing system 100 and communications with both the server-side module 106 and the payment module 124. In some implementations, an application associated with the client-side module 102 provides a user interface to the payment processing system 100 for the mobile device 104. The client-side module 102 communicates with the server-side module 106 via a long-range communication protocol (e.g., GSM, CDMA, Wi-Fi, or the like)

Draft Only

through one or more networks 110, and the client-side module 102 communicates with the payment module 124 via a short-range communication protocol (e.g., near-field communication (NFC), BLUETOOH, BLUETOOH low-energy (BLE), or the like). The server-side module 106 provides server-side functionalities for the payment processing system 100 for any number of client modules 102 each residing on a respective mobile device 104.

[0045] The payment processing system 100 harnesses the connectivity of the mobile device 104 to communicate with the payment module 124, which has neither a dedicated communication connection nor a long-range communication transceiver. As such, the mobile device 104 acts as a relay between the payment module 124 and the server system 108. Furthermore, leveraging the connectivity of the mobile device 104 helps to keep costs down from the point of view of the operator of the automatic retail machine 122.

[0046] In some implementations, the server-side module 106 includes one or more processors 112, a user information database 114, an offers database 116, and an input and output (I/O) interface to one or more clients 118. The I/O interface to one or more clients 118 facilitates the client-facing input and output processing for the server-side module 106. In some implementations, the one or more processors 112 authorize transaction requests, determine promotional offers for a particular mobile device 104, perform transaction accounting, and acknowledge completed transactions. The user information database 114 stores information for each user of the payment processing system 100 (e.g., user ID, account credentials (user name and password), transaction history, account balance, linked credit cards and bank accounts, and/or the like), and the offers database 116 stores promotional offers provided by manufacturers, distributors, retailers, and the like.

[0047] Examples of the mobile device 104 include, but are not limited to, a handheld computer, a wearable computing device, a personal digital assistant (PDA), a tablet computer, a laptop computer, a desktop computer, a cellular telephone, a smart phone, an enhanced general packet radio service (EGPRS) mobile phone, a media player, a navigation device, a game console, a television, a remote control, a point-of-sale (POS) terminal, vehicle-mounted computer, an eBook reader, or a combination of any two or more of these data processing devices or other data processing devices.

Draft Only

[0048] Examples of the one or more networks 110 include local area networks (LAN) and wide area networks (WAN) such as the Internet. One or more networks 110 are, optionally, implemented using any known network protocol, including various wired or wireless protocols, such as Ethernet, Universal Serial Bus (USB), FIREWIRE, Long Term Evolution (LTE), Global System for Mobile Communications (GSM), Enhanced Data GSM Environment (EDGE), code division multiple access (CDMA), time division multiple access (TDMA), Bluetooth, Wi-Fi, voice over Internet Protocol (VoIP), Wi-MAX, or any other suitable communication protocol.

[0049] The server system 108 is implemented on one or more standalone data processing apparatuses or a distributed network of computers. In some implementations, the server system 108 also employs various virtual devices and/or services of third party service providers (e.g., third-party cloud service providers) to provide the underlying computing resources and/or infrastructure resources of the server system 108. In some implementations, the server system 108 includes, but is not limited to, a handheld computer, a tablet computer, a laptop computer, a desktop computer, or a combination of any two or more of these data processing devices or other data processing devices.

[0050] The payment processing system 100 shown in Figure 1 includes both a client-side portion (e.g., the client-side module 102) and a server-side portion (e.g., the server-side module 106). In some implementations, data processing is implemented as a standalone application installed on the mobile device 104. In addition, the division of functionalities between the client and server portions of the payment processing system 100 can vary in different implementations. For example, in some implementations, the client-side module 102 is a thin-client that provides only user-facing input and output processing functions, and delegates all other data processing functionalities to a backend server (e.g., the server system 108). Although many aspects of the present technology are described from the perspective of the server system 108, the corresponding actions performed by the mobile device 104 would be apparent to ones skilled in the art without any creative efforts. Furthermore, some aspects of the present technology may be performed by the server system 108, the mobile device 104, or the server system 108 and the mobile device 104 cooperatively.

[0051] Figure 2 is a block diagram of the mobile device 104 associated with a user in accordance with some implementations. The mobile device 104, typically, includes one or more processing units (CPUs) 202, two or more communication devices 204, memory 206,

Draft Only

CSC ServiceWorks - Ex. 1002
Page 896 of 1551

and one or more communication buses 208 for interconnecting these components (sometimes called a chipset). The two or more communication devices 204 include a first transceiver associated with a short-range communication protocol (e.g., NFC, BLE, or the like) and a second transceiver associated with a long-range communication protocol (e.g., GSM, CDMA, Wi-Fi, or the like). The mobile device 104 also includes a user interface 210. The user interface 210 includes one or more output devices 212 that enable presentation of media content (e.g., text, images, audio, video, etc.), including one or more speakers and/or one or more visual displays. The user interface 210 also includes one or more input devices 214, including user interface components that facilitate user input such as a keyboard, a mouse, a voice-command input unit or microphone, a touch screen display, a touch-sensitive input pad, a gesture capturing camera, or other input buttons or controls. Furthermore, in some implementations, the mobile device 104 uses a microphone and voice recognition or a camera and gesture recognition to supplement or replace the keyboard. In some implementations, the mobile device 104 optionally includes one or more sensors 215, which provide context information as to the current state of the mobile device 104 or the environmental conditions associated with mobile device 104. The one or more sensors 215 include, but are not limited, to one or more microphones, one or more cameras, an ambient light sensor, one or more accelerometers, one or more gyroscopes, a temperature sensor, one or more motion sensors, one or more biometric/biological sensors, and so on. In some implementations, the mobile device 104 optionally includes a location detection device 217, such as a GPS (global positioning satellite) or other geo-location receiver, for determining the location of the mobile device 104.

[0052] The memory 206 includes high-speed random access memory, such as DRAM, SRAM, DDR RAM, or other random access solid state memory devices; and, optionally, includes non-volatile memory, such as one or more magnetic disk storage devices, one or more optical disk storage devices, one or more flash memory devices, or one or more other non-volatile solid state storage devices. The memory 206, optionally, includes one or more storage devices remotely located from the one or more processing units 202. The memory 206, or alternatively the non-volatile memory within the memory 206, includes a non-transitory computer readable storage medium. In some implementations, the memory 206, or the non-transitory computer readable storage medium of the memory 206, stores the following programs, modules, and data structures, or a subset or superset thereof:

Draft Only

CSC ServiceWorks - Ex. 1002
Page 897 of 1551

- operating system 216 including procedures for handling various basic system services and for performing hardware dependent tasks;
- communication module 218 for transmitting signals to and receiving signals from other devices (e.g., the server system 108 and the payment module 124) via the two or more communication devices 204;
- presentation module 220 for enabling presentation of information (e.g., a user interface for the application(s) 226 or the application associated with client-side module 102, widgets, websites and web pages thereof, and/or games, audio and/or video content, text, etc.) at the mobile device 104 via one or more output devices 212 (e.g., displays, speakers, etc.) associated with the user interface 210;
- input processing module 222 for detecting one or more user inputs or interactions from the one or more input devices 214 and interpreting the detected inputs or interactions;
- web browser module 224 for navigating, requesting (e.g., via HTTP), and displaying websites and web pages thereof;
- one or more applications 226 for execution by the mobile device 104 (e.g., games, application marketplaces, payment platforms, and/or other web or non-web based applications);
- client-side module 102, which provides client-side data processing and functionalities for the payment processing system 100, including but not limited to:
    - broadcast obtaining module 230 for receiving, via the first transceiver, an information packet broadcast by a respective payment module 124, where the information packet at least includes a unique identifier corresponding to the respective payment module 124 (i.e., the device ID) and an authorization code for initiating a transaction with an automatic retail machine 122 to which the respective payment module 124 is coupled;
    - transaction authorization module 232 for: sending, via the second transceiver, a transaction authorization request to the server system 108 including the authorization code; receiving, via the second transceiver, an authorization grant token from the server system 108, including the authorization code, for initiating a transaction with the automatic retail machine 122 to which the

Draft Only

CSC ServiceWorks - Ex. 1002
Page 898 of 1551

respective payment module 124 is coupled; and storing the received authorization grant token (e.g., in the user data 264);

- offer(s) module 234 for: obtaining (i.e., receiving or retrieving), via the second transceiver, promotional offers from the server system 108 (e.g., in response to sending the transaction authorization request, as part of an update to the application associated with the client-side module 102, or at another time); storing the promotional offers obtained from the server system in the offers database 266; optionally determining one or more promotional offers based on one or more of a plurality of factors (e.g., the device ID, user ID and history, current location of the mobile device 104, current time/date, and/or the like); presenting one or more promotional offers to the user of the mobile device via the one or more output devices 212 (e.g., a display); and detecting a user input selecting a respective one of the one or more promotional offers presented to the user of the mobile device 104;
- trigger detecting module 236 for detecting a trigger to initiate a transaction with the automatic retail machine 122 to which the respective payment module 124 is coupled (e.g., the trigger is a gesture or other user input by the user of the mobile device 104, entrance of the mobile device 104 into a payment zone based on the RSSI observed from the payment module 124, selection of the respective promotional offer, or the like);
- transaction initiating module 238 for initiating a transaction with the automatic retail machine 122 coupled with the respective payment module 124 by sending, via the first transceiver, the stored authorization grant token to the respective payment module 124;
- transaction completion notification receiving module 240 for receiving, via the first transceiver, a transaction completion notification from the payment module 124, where the transaction completion notification includes one or more of: transaction status information (e.g., indicating whether the transaction with the automatic retail machine 122 was successful, aborted, or failed); transaction detail information (e.g., the authorization code, the amount of the transaction, the good/product associated with the transaction, the time/date the transaction was completed, transaction error information, and/or

Draft Only

CSC ServiceWorks - Ex. 1002
Page 899 of 1551

the like); and optionally includes other miscellaneous information regarding the respective payment module 124 and/or the automatic retail machine 122 to which the respective payment module 124 is coupled, such as interrupted transaction information, status flags, inventory information, past hard currency transaction information, other cashless transaction information, and/or the like;

- product code processing module 242 for: providing a prompt to the user of the mobile device 104 via the one or more output devices 212 to obtain a product code for a vended product to validate the respective promotional offer; obtaining the product code for the vended product (e.g., the user of the mobile device 104 manually inputs the product code, the user of the mobile device 104 captures an image of the vended product from which the product code is extracted, the user of the mobile device 104 uses a scanner plug-in of the application associated with the client-side module 102 to obtain the product code, or the like); and either validating the product code or sending, via the second transceiver, the obtained product code to the server system 108 for validation;
- information relaying module 244 for transmitting, via the second transceiver, information from the payment module 124 to the server system 108 (e.g., the transaction status information, the transaction detail information, the other miscellaneous information regarding the respective payment module 124 and/or the automatic retail machine 122 to which the respective payment module 124 is coupled, and/or the like);
  - offer validation module 246 for: receiving, via the second transceiver, promotion validation information from the server system 108; and presenting the promotion validation information to the user of the mobile device via the one or more output devices 212 (e.g., the display); and
- acknowledgment module 248 for sending, via the first transceiver, acknowledgment information to the payment module 124, where the acknowledgment information acknowledges that the server system 108 received and processed the transaction status information and the transaction detail information; and

Draft Only

- client data 260 storing data associated with the payment processing system 100, including, but is not limited to:
    - user profile 262 storing information for the user of the mobile device 104, including but not limited to: a unique user identifier (i.e., a user ID), login credentials (i.e., user name or handle and password), transaction history, payment data (e.g., account balance, linked credit card or bank information, app credit or gift card balance, billing address, shipping address, etc.), contact information (e.g., email address, phone number, etc.), custom parameters for the user (e.g., age, location, hobbies, etc.), identified trends and/or likes/dislikes of the user, and/or the like;
    - user data 264 storing transaction history information, authorization grant tokens, and/or the like; and
    - offers database 266 storing promotional offers provided by manufacturers, distributors, retailers, and/or the like.

[0053] Each of the above identified elements may be stored in one or more of the previously mentioned memory devices, and corresponds to a set of instructions for performing a function described above. The above identified modules or programs (i.e., sets of instructions) need not be implemented as separate software programs, procedures, modules or data structures, and thus various subsets of these modules may be combined or otherwise re-arranged in various implementations. In some implementations, the memory 206, optionally, stores a subset of the modules and data structures identified above. Furthermore, the memory 206, optionally, stores additional modules and data structures not described above.

[0054] Figure 3 is a block diagram illustrating the server system 108 in accordance with some implementations. The server system 108, typically, includes one or more processing units (CPUs) 112, one or more communication devices 304 (e.g., including the I/O interface to one or more clients 118), memory 306, and one or more communication buses 308 for interconnecting these components (sometimes called a chipset). The memory 306 includes high-speed random access memory, such as DRAM, SRAM, DDR RAM, or other random access solid state memory devices; and, optionally, includes non-volatile memory, such as one or more magnetic disk storage devices, one or more optical disk storage devices, one or more flash memory devices, or one or more other non-volatile solid state

Draft Only

CSC ServiceWorks - Ex. 1002
Page 901 of 1551

storage devices. The memory 306, optionally, includes one or more storage devices remotely located from the one or more processing units 112. The memory 306, or alternatively the non-volatile memory within the memory 306, includes a non-transitory computer readable storage medium. In some implementations, the memory 306, or the non-transitory computer readable storage medium of the memory 306, stores the following programs, modules, and data structures, or a subset or superset thereof:

- operating system 310 including procedures for handling various basic system services and for performing hardware dependent tasks;
- network communication module 312 for transmitting signals to and receiving signals from mobile devices 104 via the one or more communication devices 304;
- server-side module 106, which provides server-side data processing and functionalities for the payment processing system 100, including but not limited to:
    - transaction authorization module 314 for: receiving a transaction request from a respective mobile device 104, where the transaction request includes a device ID associated with a respective payment module 124 and an authorization code; and validating the transaction request;
    - encryption/decryption module 316 for: identifying an encryption/decryption key linked to the device ID for the respective payment module 124; decrypting the authorization code with the identified encryption/decryption key; and encrypting the authorization grant token with the identified encryption/decryption key;
    - offer determining module 318 for determining one or more promotional offers based on one or more of a plurality of factors (e.g., the device ID included in the transaction request, the user ID and history associated with the user of the respective mobile device 104, current location of the respective mobile device 104, current time/date, and/or the like);
    - transmitting module 320 for: transmitting, in accordance with a determination that the transaction request is validated, an authorization grant token and the one or more promotional offers to the respective mobile device 104; and transmitting acknowledgment information once a transaction is completed to the respective mobile device 104;

Draft Only

CSC ServiceWorks - Ex. 1002
Page 902 of 1551

- receiving module 322 for receiving information from the respective mobile device 104, including but not limited to: a product code and a corresponding selected promotional offer, the transaction status information for a respective transaction, the transaction detail information for the respective transaction, and/or the other miscellaneous information;
- offer validation module 324 for: validating a promotional offer based on a received product code, transaction status information, and/or transaction detail information; and sending, in accordance with a determination that the promotional offer is validated, promotion validation information to the respective mobile device 104;
- accounting module 326 for debiting an account balance or charging a linked credit card or bank account according to the transaction detail information; and
- acknowledgment module 328 for sending acknowledgment information to the respective mobile device 104 for relay to the respective payment module 124;

- server data 340 storing data for the payment processing system 100, including but not limited to:
  - user information database 114 storing stores information for each user of the payment processing system 100, including but not limited to: a unique user identifier (i.e., a user ID), login credentials (i.e., user name or handle and password), transaction history, payment data (e.g., account balance, linked credit card or bank information, app credit or gift card balance, billing address, shipping address, etc.), contact information (e.g., email address, phone number, etc.), custom parameters for the user (e.g., age, location, hobbies, etc.), identified trends and/or likes/dislikes of the user, and/or the like;
  - offers database 116 storing promotional offers provided by manufacturers, distributors, retailers, and/or the like; and
  - payment module database 342 storing information for each payment module 124 of the payment processing system 100, including but not limited to: a unique payment module identifier (i.e., a device ID), an encryption/decryption key, and/or the like.

Draft Only

[0055] Each of the above identified elements may be stored in one or more of the previously mentioned memory devices, and corresponds to a set of instructions for performing a function described above. The above identified modules or programs (i.e., sets of instructions) need not be implemented as separate software programs, procedures, or modules, and thus various subsets of these modules may be combined or otherwise re-arranged in various implementations. In some implementations, the memory 306, optionally, stores a subset of the modules and data structures identified above. Furthermore, the memory 306, optionally, stores additional modules and data structures not described above.

[0056] In some implementations, at least some of the functions of the server system 108 are performed by the mobile device 104, and the corresponding sub-modules of these functions may be located within the mobile device 104 rather than the server system 108. In some implementations, at least some of the functions of mobile device 104 are performed by the server system 108, and the corresponding sub-modules of these functions may be located within the server system 108 rather than the mobile device 104. The mobile device 104 and the server system 108 shown in Figures 2-3, respectively, are merely illustrative, and different configurations of the modules for implementing the functions described herein are possible in various implementations.

[0057] Figure 4 is a schematic block diagram illustrating the automatic retail machine 122 in accordance with some implementations. For example, the automatic retail machine 122 is a vending machine or kiosk that dispenses an item or product (e.g., snacks, other foodstuffs, school supplies, drinks, tickets, and the like) in response to user payment for and selection of the item or product. The automatic retail machine 122 includes: a controller 402; a power supply 404; memory 406; a user interface 408; one or more optional sensors 414; a multi-drop bus (MDB) 416; and a dispenser 424.

[0058] In some implementations, the controller 402 is a microcontroller, microprocessor, CPU, FPGA, ASIC, or the like that manages the functions of the automatic retail machine 122. The power supply 404 is a connection to an external power source (e.g., AC or DC) or a connection to an internal power source (e.g., a battery). In some implementations, the power supply 404 further includes one or more of a power converter and/or inverter, a rectifier, a power conditioner, or the like for providing power to the various components of the automatic retail machine 122. The memory 406 includes high-speed random access memory, such as DRAM, SRAM, DDR RAM, or other random access solid

Draft Only

CSC ServiceWorks - Ex. 1002
Page 904 of 1551

state memory devices; and, optionally, includes non-volatile memory, such as one or more magnetic disk storage devices, one or more optical disk storage devices, one or more flash memory devices, or one or more other non-volatile solid state storage devices. In some implementations, the memory 406 stores an operating system and instructions for carrying out the functions and processes of the automatic retail machine 122 (e.g., dispensing items, tracking inventory, temperature control, power control, and the like). In some implementations, the memory 406 also stores configuration data and DEX (data exchange) data corresponding to the inventory of the automatic retail machine 122 and transactions performed with the automatic retail machine 122.

[0059] The user interface 408 includes one or more output devices 410 that enable presentation of information (e.g., text, images, audio, video, etc.), for example, one or more speakers and/or one or more visual displays. The user interface 408 also includes one or more input devices 412, including user interface components that facilitate user input and selection of items such as a microphone, a keypad, a touch screen display, a gesture capturing camera, or other input buttons or controls. The one or more optional sensors 414 include, but are not limited, to one or more microphones, one or more cameras, an ambient light sensor, one or more accelerometers, one or more gyroscopes, a temperature sensor, one or more motion sensors, one or more biometric/biological sensors, and so on.

[0060] In some implementations, a variety of payment devices are coupled with the MDB 416 including any combination of one or more cashless payment devices 418 (e.g., credit card reader(s)) for accepting cashless payments, one or more bill validators 420 for accepting and validating bills, and one or more coin accepters 422 for accepting coins and providing change. In some implementations, the dispenser 424 is an electromechanical system (e.g., motors, actuators, and the like) for dispensing or vending items or products stocked by the automatic retail machine. 122 For example, a user inserts a bill into the bill validator(s) 420 and is credited with an amount of money equal to the bill. Continuing with this example, the one or more output devices 410 (e.g., a display) shows the credited amount, and the user selects an item via the one or more input devices 412 (e.g., using a keypad or a sequence of button presses). Subsequently, the controller 402 sends signals to the dispenser 424 to dispense the selected product, and the dispenser dispenses or vends the selected product.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 905 of 1551

[0061] Figure 5 is a block diagram illustrating the payment module 124 in accordance with some implementations. In some implementations, the payment module 124 is an in-line adapter dongle with male and female connectors that couples with the multi-drop bus (MDB) of the respective automatic retail machine 122 as shown in Figures 6B-6C and 7. For example, the payment module is connected in-line into the MDB 416 in Figure 4. The payment module 124, typically, includes one or more processing units (CPUs) 512, a communication device 504 (e.g., a transceiver associated with a short-range communication protocol such as NFC, BLE, or the like), memory 506, and one or more communication buses 508 for interconnecting these components (sometimes called a chipset). The memory 506 includes high-speed random access memory, such as DRAM, SRAM, DDR RAM, or other random access solid state memory devices; and, optionally, includes non-volatile memory, such as one or more magnetic disk storage devices, one or more optical disk storage devices, one or more flash memory devices, or one or more other non-volatile solid state storage devices. The memory 506, optionally, includes one or more storage devices remotely located from one or more processing units 512. The memory 506, or alternatively the non-volatile memory within the memory 506, includes a non-transitory computer readable storage medium. In some implementations, the memory 506, or the non-transitory computer readable storage medium of the memory 506, stores the following programs, modules, and data structures, or a subset or superset thereof:

- operating system 510 including procedures for handling various basic system services and for performing hardware dependent tasks;
- communication module 512 for transmitting signals to and receiving signals from mobile devices 104 via the communication device 504;
- transaction-processing module 514, including but not limited to:
    - broadcasting module 516 for: broadcasting an information packet to zero or more client devices 104 within the communication zone of the payment module 124 (i.e., BLE range), where the information packet at least includes a unique identifier corresponding to the payment module 124 (e.g., the device ID) and an authorization code for initiating a transaction with the automatic retail machine 122 to which the payment module 124 is coupled; and storing broadcast authorization codes in authorization database 532;

Draft only

- encryption/decryption module 518 for: encrypting the authorization code with an encryption/decryption key that corresponds to the payment module 124; and decrypting the authorization grant token with the encryption/decryption key;
- transaction sniffing module 520 for: detecting signals associated with hard currency transactions and/or other cashless transactions not associated with the payment processing system 100 (e.g., credit card transactions); and storing information associated with said hard currency transactions and/or other cashless transactions (e.g., in the other information database 536);
- validating module 522 for validating a transaction by checking the authorization code from the decrypted authorization grant token against previously broadcast authorization codes stored in the authorization database 532;
- transaction processing module 524 for: causing, in accordance with a determination that the transaction is validated, the automatic retail machine 122 to vend a product or perform a service; and storing transaction detail information in the transaction database 534; and
- acknowledgement module 526 for deleting transaction detail information from the transaction database 534 in accordance with a determination that the corresponding transaction is acknowledged by the server system 108; and

* data 530 storing data, including but not limited to:
  - authorization database 532 storing previously broadcast authorization codes;
  - transaction database 534 storing transaction detail information for transactions processed by the payment module 124; and
  - other information database 536 storing miscellaneous information regarding the payment module 124 and/or the automatic retail machine 122 coupled with the payment module 124 such as status flags, inventory information, past hard currency transaction information, other cashless transaction information, and/or the like.

[0062] Each of the above identified elements may be stored in one or more of the previously mentioned memory devices, and corresponds to a set of instructions for

Draft Only

CSC ServiceWorks - Ex. 1002
Page 907 of 1551

performing a function described above. The above identified modules or programs (i.e., sets of instructions) need not be implemented as separate software programs, procedures, or modules, and thus various subsets of these modules may be combined or otherwise re-arranged in various implementations. In some implementations, the memory 506, optionally, stores a subset of the modules and data structures identified above. Furthermore, the memory 506, optionally, stores additional modules and data structures not described above.

[0063] Figures 6A-6C show various views of the payment module 124 of Figure 5 in accordance with some implementations. The payment module 124 is a relatively low cost hardware component that is pre-configured to work with the industry standard multi-drop bus (MDB). On machines without MDB technology, the payment module 124 can be configured or designed to work with other serial protocols or activate a switch (e.g., a cherry switch mechanism). For example, see U.S. Patent Application No. 14/458,192, entitled "Method and System for Retrofitting an Offline-Payment Operated Machine to Accept Electronic Payments," which is incorporated by reference in its entirety. In essence, the payment module 124 simulates establishing payment on the automatic retail machine 122 in much the same manner as other alternative forms of payment (e.g., cash).

[0064] The payment module 124 is preferably designed to be used as an adapter dongle for in-line insertion within, for example, the MDB of the automatic retail machine 122 (e.g., a vending machine). The wire used in MDB technology uses male and female connection ends or adapters to allow the attachment of peripherals. In the case of a vending machine, the MDB with connection ends or adapters would be present to allow the attachment of a payment receiving mechanism (e.g., a coin mechanism). The MDB male and female adapters 612, 614 of the MDB may be separated (as shown in Figures 6B-6C). The payment module 124 in Figures 6A-6C has a male adapter 602 and a female adapter 604. The payment module 124 may be plugged (inserted) in serial ("in-line") with the MDB. For example, the MDB female adapter 614 may be connected to the male adapter 602 of the payment module 124, and the MDB male adapter 612 may be connected to the female adapter 604 of the payment module 124. The resulting in-line configuration is shown in Figure 7. It should be noted that the payment module 124 is designed to allow pass-through communications so that if the mobile-device-to-machine payment processing system is not enabled (e.g., for a particular purchase or simply turned off) the MDB functions as though the payment module 124 is not there and the automatic retail machine 122 can function normally.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 908 of 1551

In Figure 7, the automatic retail machine 122 includes a display 722 showing user selections, current credit, and the like. In Figure 7, the automatic retail machine 122 also includes a touch-screen display 724 and buttons 726 for selecting a product.

USER INTERFACES AND RELATED PROCESSES

[0065] Figure 8 is a schematic flow diagram of a process 800 for authenticating a user to perform a transaction in the payment processing system 100 in accordance with some implementations. In some implementations, the payment processing system 100 includes one or more payment modules 124 (e.g., each associated with a respective automatic retail machine 122 such a vending machine for dispensing goods and/or services), one or more mobile devices 104, and the server 108. Each of the one or more mobile devices 104 executes an instance of the client-side module 102 (e.g., as an application) as a foreground or background process to access and communicate with other devices (e.g., the server 108 and the payment modules 124) in the payment processing system 100. The server 108 manages the payment processing system 100 and, in some cases, is associated with an entity that supplies, operates, and/or manufactures the one or more payment modules 124. For brevity, the process 800 will be described with respect to a respective payment module 124 and a respective mobile device 104 within the payment processing system 100.

[0066] The payment module 124 broadcasts (802), via a short-range communication capability (e.g., BLE), an information packet. The information packet at least includes an authorization code and a unique identifier associated with the payment module 124 (i.e., the device ID). In some implementations, the information packet further includes a current firmware version of the payment module 124 and one or more status flags corresponding to one or more states of the payment module 124 and/or the automatic retail machine 122. The information packet is further discussed below with reference to Figure 10A.

[0067] In some implementations, the payment module 124 sends out a unique authorization code every X seconds (e.g., 100 ms, 200 ms, 500 ms, etc.). In some implementations, the unique authorization codes are randomly or pseudo-randomly generated numbers. In some implementations, the payment module 124 initializes a random number and then the authorization codes are sequential counts from this random number. In such implementations, the payment module 124 stores the earliest valid (unexpired) counter without a need to store every valid authorization code. In some implementations, the

Draft Only

CSC ServiceWorks - Ex. 1002
Page 909 of 1551

authentication code included in the broadcast information packet is a hash value of the randomly or pseudo-randomly generated number or the sequential number.

[0068] In some implementations, the payment module 124 stores broadcast authorization codes (e.g., in authorization database 542, Figure 5) until a received authorization grant token matches one of the stored authorization codes and subsequently deletes the matching authorization code. In some implementations, the broadcast authorization codes are one-time use codes whereby a broadcast authorization code may only be used by one mobile device 104 before it is invalidated and/or deleted to prevent re-play attacks. In some implementations, the payment module 124 stores previously broadcast authorization codes for a predetermined amount of time (e.g., Y minutes) after which time an authorization code expires and is deleted. In some implementations, the authorization code is encrypted with a shared secret key known by the server system 108 but unique to the payment module 124.

[0069] The mobile device 104 receives the broadcast information packet, and the mobile device 104 sends (804), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), an authorization request to the server system 108. For example, an application associated with the client-side module 102 is executed as a foreground or background process on the mobile device 104. The application is used for accessing the payment processing system 100. In this example, the application receives the broadcast information packet when the mobile device 104 is within the communication zone of the payment module 124 (i.e., BLE range) and either automatically sends the authorization request to the server system 108 or sends the authorization request to the server system 108 when the mobile device 104 is within the authorization zone of the payment module 124.

[0070] In some implementations, the broadcast information packet includes a baseline authorization zone threshold (i.e., an authorization zone criterion) indicating a baseline received signal strength indication (RSSI) that the mobile device 104 (or the application associated with the client-side module 102) is required to observe from the payment module 124 before being within the authorization zone of the payment module 124. In some implementations, the mobile device 104 (or the application associated with the client-side module 102) offsets the baseline authorization zone threshold based on the reception strength its short-range communication capability (e.g., BLE radio/transceiver) and/or other similar factors. In some implementations, the authorization request at least includes the authorization

Draft Only

code which was included in the broadcast information packet, an identifier associated with the user of the mobile device 104 or the user account under which the user of the mobile device 104 is logged into the application (i.e., user ID), and the identifier associated with the payment module 124 (i.e., device ID). In some implementations, the authentication code included in the authorization request is a hash value in cleartext. The authorization request is further discussed below with reference to Figure 10B.

[0071] After receiving the authorization request, the server system 108 processes (806) the authorization request. In some implementations, the server system 108 identifies a shared secret key based on the device ID and decrypts the authorization code included in the authorization request with the identified shared secret key. The server system 108 determines whether the user associated with the user ID in the authorization request has sufficient funds in his/her account for the payment processing system to perform a transaction at the automatic retail machine 122 to which the payment module 124 corresponding to the device ID is coupled.

[0072] The server system 108 sends (808), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), an authorization grant token to the mobile device 104. In some implementations, the server system 108 does not send the authorization grant token if the authorization code in the authorization request cannot be decrypted with the shared secret key corresponding to the payment module 124 (e.g., the authorization code is corrupted or hacked). In some implementations, the server system 108 does not send the authorization grant token if the user associated with the user ID in the authorization request does not have sufficient funds in his/her account or has exceeded a predefined daily limit. In some implementations, in addition to the authorization grant token (or lack thereof if the authorization is declined), the server system 108 sends a message directly to the mobile device 104 which is not encrypted with the shared secret key corresponding to the payment module 124. After receiving the message, the mobile device 104 displays an appropriate message to the user such as sufficient funds, transaction authorized, insufficient balance, or declined authorization. In some implementations, the server system 108 sends an authorization grant token for an amount equal to zero; in which case, the payment module 124 interprets this as a declined or failed authorization which can result for any number of reasons including, but not limited to, insufficient balance or credit. In some implementations,

Draft Only

CSC ServiceWorks - Ex. 1002
Page 911 of 1551

the mobile device 104 stores the authorization grant token (e.g., in the user data 264) until a trigger condition is detected.

[0073] The mobile device 104 receives the authorization grant token, and, subsequently, the mobile device 104 detects (810) a trigger condition. In some implementations, the mobile device 104 (or the application) detects the trigger condition via the hand-free mode (e.g., upon entrance into the payment zone of the payment module 124) or manual mode (e.g., interacting with the user interface of the application to initiate a transaction with the payment accepting unit associated with the payment module 124).

[0074] In some implementations, the trigger condition is satisfied when the mobile device 104 detects a user input on the user interface displayed by the mobile device 104. For example, with reference to Figure 11A, a transaction is initiated between the user of the mobile device 104 and the 8th floor snack machine when the mobile device 104 detects an upward swipe gesture originating from region 1120 of the user interface 1108. In another example, with reference to Figure 11D, a transaction is initiated between the user of the mobile device 104 and the 8th floor snack machine when the mobile device 104 detects selection of Offer A 1152 with contact 1166.

[0075] In some implementations, the trigger condition is satisfied when the mobile device 104 observes an RSSI from a respective automatic retail machine that is greater than or equal to the payment zone criterion. For example, once the mobile device 104 is within the payment zone, a transaction between the respective automatic retail machine and the user of the mobile device 104 is automatically initiated. In some implementations, after the RSSI observed from the respective retail machine is greater than or equal to the payment zone criterion, the mobile device 104 prompts the user to provide a transaction confirmation, which when detected serves to satisfy the trigger condition. For example, once the mobile device 104 is within the payment zone, the mobile device 104 provides a prompts to the user, such as an audible prompt, displayed notification, or vibration, to confirm his/her intention to initiate a transaction with the respective retail machine. Continuing with this example, the user may confirm his/her intention to initiate the transaction with the respective retail machine by flicking the mobile device 104 towards the automatic retail machine, shaking the mobile device, providing an audible command, or performing a touch input/gesture on the displayed user interface.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 912 of 1551

[0076] In some implementations, unused authorization grants (e.g., if there was no trigger condition or it expired) are canceled by the mobile device 104 by sending a cancellation message to the server system 108 corresponding to the unused authorization grant. In some implementations, the server system 108 denies or limits the number of authorization grants sent to the mobile device 104 until it has received transaction information or cancellation of authorization outstanding authorization grants sent to the mobile device 104.

[0077] In response to detecting the trigger condition, the mobile device 104 sends (812), via the short-range communication capability (e.g., BLE), the authorization grant token to the payment module 124. Subsequently, the automatic retail machine 122 displays credit to the user (e.g., via one of the displays 722 or 724 shown in Figure 7) and the user interacts with the input mechanisms of the automatic retail machine 122 (e.g., via the buttons 726 or a touch screen display 724 shown in Figure 7) to purchase products and/or services.

[0078] It should be understood that the particular order in which the process in Figure 8 has been described is merely exemplary and is not intended to indicate that the described order is the only order in which the operations could be performed. One of ordinary skill in the art would recognize various ways to reorder the operations described herein. Additionally, it should be noted that details of other processes described herein with respect to other methods and/or processes described herein (e.g., the process 900 and the method 1200) are also applicable in an analogous manner to the process 800 described above with respect to Figure 8.

[0079] Figure 9 is a schematic flow diagram of a process 900 for processing acknowledgment information in the payment processing system 100 in accordance with some implementations. In some implementations, the payment processing system 100 includes one or more payment modules 124 (e.g., each associated with a respective automatic retail machine 122 such a vending machine for dispensing goods and/or services), one or more mobile devices 104, and the server 108. Each of the one or more mobile devices 104 executes an instance of the client-side module 102 (e.g., as an application) as a foreground or background process to access and communicate with other devices (e.g., the server 108 and the payment modules 124) in the payment processing system 100. The server 108 manages the payment processing system 100 and, in some cases, is associated with an entity that supplies, operates, and/or manufactures the one or more payment modules 124. For brevity,

Draft Only

CSC ServiceWorks - Ex. 1002
Page 913 of 1551

the process 900 will be described with respect to a respective payment module 124 coupled with a respective automatic retail machine 122 and a respective mobile device 104 in the payment processing system 100. In the process 900, the payment module 124 receives first acknowledgment information for a first transaction via the mobile device 104 that initiated the first transaction.

[0080] The payment module 124 obtains (902) a first notification indicating completion of a first transaction from the automatic retail machine 122. For example, after the process 800 in Figure 8, the user of the mobile device 104 selects a product to purchase from the automatic retail machine 122 by interacting with one or more input mechanisms of the automatic retail machine 122 (e.g., he buttons 726 or a touch screen display 724 shown in Figure 7), and the automatic retail machine 122 dispenses the selected product. Continuing with this example, after the product is dispensed, the transaction is complete and the payment module 124 obtains a notification from the machine of the completed transaction. In some implementations, the notification includes the amount of the transaction and (optionally) machine status information associated with the automatic retail machine 122 such as inventory information as to one or more products of the automatic retail machine 122 and/or the like.

[0081] After obtaining the first notification, the payment module 124 generates (904) first transaction information based on the first notification, and the payment module 124 stores the first transaction information. In some implementations, the transaction information includes a transaction ID for the first transaction, a device ID corresponding to the payment module 124, a user ID corresponding to the mobile device 104, transaction status information indicating that the first transaction is complete, and the transaction amount indicated by the first notification. In some implementations, the payment module 124 retains the authorization code included in the original broadcasted packet and/or the authorization grant token and includes the authorization code in the first transaction information. In some implementations, the authorization code is encrypted with a secret key corresponding to the payment module 124, which is shared with the server system 108 but not the mobile device 104. In some implementations, the first transaction information further includes other information such as the machine status information included in the first notification or transaction information corresponding to previous interrupted transaction(s). See Figure 10D and the accompanying text for further discussion regarding the transaction information 1050.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 914 of 1551

[0082] The payment module 124 sends (906), via a short-range communication capability (e.g., BLE), the first transaction information to the mobile device 104.

[0083] The mobile device 104 sends (908), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), the first transaction information to the server system 108.

[0084] The server system 108 processes (910) the first transaction information. For example, the server system 108 debits the account of the user associated with the user ID in the first transaction information in the amount indicated by the first transaction information.

[0085] The server system 108 sends (912), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), first acknowledgment information to the mobile device 104. In some implementations, the first acknowledgment information acknowledges that the server system 108 received the first transaction information. In some implementations, the first acknowledgment information includes the user ID, the device ID, the transaction ID, and (optionally) the authorization grant included in the transaction information (e.g., the authorization code 1058, Figure 10D).

[0086] After receiving the first acknowledgement information, the mobile device 104 sends (914), via a short-range communication capability (e.g., BLE), the first acknowledgment information to the payment module 124.

[0087] After receiving the first acknowledgment information, the payment module 124 deletes (916) the stored first transaction information.

[0088] It should be understood that the particular order in which the process in Figure 9 has been described is merely exemplary and is not intended to indicate that the described order is the only order in which the operations could be performed. One of ordinary skill in the art would recognize various ways to reorder the operations described herein. Additionally, it should be noted that details of other processes described herein with respect to other methods and/or processes described herein (e.g., the process 800 and the method 1200) are also applicable in an analogous manner to the process 900 described above with respect to Figure 9.

[0089] Figure 10A is a block diagram of an information packet 1000 broadcast by the payment module 124 (e.g., in step 802 of the process 800 in Figure 8) in accordance with

Draft Only

CSC ServiceWorks - Ex. 1002
Page 915 of 1551

some implementations. In some implementations, the information packet 1000 at least includes: device ID 1002 and authorization code 1004. In some implementations, the information packet 1000 additionally includes: a current firmware version 1006; one or more status flags 1008; and zone criteria information 1010.

[0090] In some implementations, the device ID 1002 is a unique identifier corresponding to the payment module 124 that broadcast the information packet 1000.

[0091] In some implementations, the authorization code 1004 is a hash value in cleartext. In some implementations, the payment module 124 randomly or pseudo-randomly generates a number or determines a sequential number (*See* step 802 of the process 800 in Figure 8) and performs a predetermined hash function (e.g., SHA-256) on the number to produce the hash value as the authorization code 1004. In some implementations, the authorization code 1004 is a unique code that is encrypted with a secret encryption key corresponding to the payment module 124. The secret encryption key is shared with the server system 108, which enables the server system 108 to decrypt the authorization code 1004 and encrypt the authorization grant token but not the mobile device 104. In some implementations, the encryption between server system 108 and payment module 124 is accomplished by two pairs of public/private keys.

[0092] In some implementations, the firmware version information 1006 identifies a current firmware version 1012 of the payment module 124. In some implementations, the firmware version information 1006 also includes update status information 1014 indicating one or more packets received by the payment module 124 to update the firmware or one or more packets needed by the payment module 124 to update the firmware.

[0093] In some implementations, the one or more status flags 1008 indicate a state of the payment module 124 and/or the automatic retail machine 122 to which the payment module 124 is coupled. In some implementations, the one or more status flags 1008 indicate a state of the payment module 124 such upload information indicator 1016 indicating that that the payment module 124 has information to be uploaded to the server system 108 (e.g., transaction information for one or more interrupted transactions). In some implementations, upload information indicator 1016 triggers the mobile device 104 to connect to payment module 124 immediately (e.g., if it has interrupted transaction information to be uploaded to the server system 108). In some implementations, the one or more status flags 1008 indicate a

Draft Only

CSC ServiceWorks - Ex. 1002
Page 916 of 1551

state of the automatic retail machine 122 including one or more of an error indicator 1018 (e.g., indicating that a bill and/or coin acceptor of the automatic retail machine 122 is experiencing a jam, error code, or malfunction), a currency level indicator 1020 (e.g., indicating that the level of the bill and/or coin acceptor reservoir of the automatic retail machine 122 is full or empty), and/or inventory level(s) indicator 1022 (e.g., indicating that one or more products of the automatic retail machine 122). In some implementations, the one or more status flags 1008 are error codes issued by the automatic retail machine 122 over the MDB.

[0094] In some implementations, the zone criteria information 1010 specifies an authorization zone criterion 1024 (e.g., a baseline authorization zone threshold indicating a baseline RSSI that the mobile device 104 (or the application) is required to observe before being within the authorization zone of the payment module 124) and/or a payment zone criterion 1026 (e.g., a baseline payment zone threshold indicating a baseline RSSI that the mobile device 104 (or the application) is required to observe before being within the payment zone of the payment module 124). In some implementations, the baseline authorization zone threshold and the baseline payment zone threshold are default values determined by the server system 108 or stored as variables by the application, in which case the authorization zone criterion 1024 and payment zone criterion 1026 are offsets to compensate for the strength and/or reception of the short-range communication capability (e.g., BLE radio/transceiver) of the payment module 124. Alternatively, zone criteria information 1010 includes a spread between the baseline authorization zone threshold and the baseline payment zone threshold. Thus, the mobile device 104 (or the application) determines the baseline authorization zone threshold and the baseline payment zone threshold based on the spread value and a default value for either the baseline authorization zone threshold or the baseline payment zone threshold. For example, the spread indicates -10 db and the default baseline payment zone threshold is -90 db; thus, the baseline authorization zone threshold is -80 db. Continuing with this example, after determining the baseline authorization zone threshold and the baseline payment zone threshold, the mobile device 104 (or the application) may further adjust the authorization zone threshold and/or the payment zone threshold based on the strength and/or reception of its short-range communication capability (i.e., BLE radio/transceiver).

Draft Only

CSC ServiceWorks - Ex. 1002
Page 917 of 1551

[0095] Figure 10B is a block diagram of an authorization request 1030 sent by the mobile device 104 to the system server 108 (e.g., in step 804 of the process 800 in Figure 8) in accordance with some implementations. In some implementations, the authorization request 1030 at least includes: a device ID 1002; a user ID 1034; and an authorization code 1004.

[0096] In some implementations, the device ID 1002 is a unique identifier corresponding to the payment module 124 that broadcast the information packet 1000 that included the authorization code 1004.

[0097] In some implementations, the user ID 1034 is a unique identifier associated with the user of the mobile device 104 sending the authorization request 1030 to the server system 108. In some implementations, the user ID 1034 is associated with the user account under which the user of the mobile device 104 is logged into the application.

[0098] In some implementations, the authorization code 1030 is the authorization code 1004 included in the information packet 1000 of that was broadcast by the payment module 124.

[0099] Figure 10C is a block diagram of an authorization grant token 1040 sent by the server system 108 to the mobile device 104 (e.g., in step 808 of the process 800 in Figure 8) in accordance with some implementations. In some implementations, in accordance with a determination that the authorization code 1036 included in the authorization request 1030 from the mobile device 104 is valid and that the user associated with the mobile device 104 has sufficient funds in his/her account for the payment processing system, the server system 108 generates the authorization grant token 1040. In some implementations, the authorization grant token 1040 at least includes: a device ID 1002; a user ID 1034; an authorized amount 1046; (optionally) an expiration period 1048; and (optionally) the authorization code 1004. In some implementations, the authorization grant token 1040 is encrypted with the shared secret key corresponding to the payment module 124.

[00100] In some implementations, the device ID 1002 is a unique identifier corresponding to the payment module 124 that broadcast the information packet 1000 that included the authorization code 1004.

Draft Only

[00101] In some implementations, the user ID 1034 is a unique identifier associated with the user of the mobile device 104 that sent the authorization request 1030 to the server system 108.

[00102] In some implementations, the authorized amount 1046 indicates a maximum amount for which the user of the mobile device 104 is authorized to perform transaction(s) using the authorization grant token 1140. For example, the authorized amount 1046 is predefined by the user of the mobile device 104 or by the server system 108 based on a daily limit or based on the user's total account balance or based on a risk profile of the user associated with the user ID 1034.

[00103] In some implementations, the expiration period 1048 indicates an offset to the amount of time that the payment module 124 holds the authorization grant token 1040 valid for initiation of a transaction with the automatic retail machine 122 associated with the payment module 124. For example, the expiration period 1048 depends on the history and credit of the user of the mobile device 104 or a period predefined by the user of the mobile device 104.

[00104] In some implementations, the authorization grant token 1040 further includes the authorization code 1004 that was included in the authorization request 1030. In some implementations, when the authorization code 1004 is the hash value, the server system 108 encrypts the authorization grant token 1040 including the hashed value with the shared secret encryption key associated with the payment module 124. Subsequently, when the mobile device 104 sends the authorization grant token 1040 to the payment module 124 after detecting a trigger condition, the payment module 124 decrypts the authorization grant token 1040 using the secret key known only to the server system 108 and the payment module 124 (which authenticates the message and the authorization grant), and then matches the hash value included in the decrypted authorization grant token 1040 to previously broadcast valid (i.e., unexpired and un-used) hash values (e.g., stored authorization codes) to determine the validity of the hash value (which was known only by the payment module 124).

[00105] Figure 10D is a block diagram of transaction information 1050 generated by the payment module 124 (e.g., in step 904 of the process 900 in Figure 9) in accordance with some implementations. In some implementations, the transaction information 1050 includes: a transaction ID 1052 for the respective transaction; a device ID 1054; a user ID 1056;

Draft Only

CSC ServiceWorks - Ex. 1002
Page 919 of 1551

(optionally) the authorization code 1058; transaction status information 1060; the transaction detail information 1062; and miscellaneous information 1064. In some implementations, the transaction information 1050 is encrypted with the shared secret key corresponding to the payment module 124.

[00106] In some implementations, the transaction ID 1052 is a unique identifier corresponding to the respective transaction. In some implementations, the transaction ID 1052 is encoded based on or associated with the time and/or date on which and the location at which the respective transaction took place.

[00107] In some implementations, the device ID 1054 is a unique identifier corresponding to the payment module 124 that performed the respective transaction.

[00108] In some implementations, the user ID 1056 is an identifier associated with the user of the mobile device 104 that initiated the respective transaction.

[00109] In some implementations, the authorization code 1058 corresponds to the original authorization code (e.g., the auth code 1004, Figures 10A-10C) and/or authorization grant token (e.g., the auth grant token 1040, Figure 10C) that was used to initiate the respective transaction. In some implementations, the authorization code 1056 is encrypted with a unique encryption key corresponding to the payment module 124.

[00110] In some implementations, the transaction status information 1060 includes an indication whether the respective transaction was completed, not-completed, or aborted. For example, the respective transaction is incomplete if a jam occurred at the automatic retail machine 122 and the user did not receive the product associated with the respective transaction. For example, if the user walks away from the automatic retail machine 122 after money was credited for the respective transaction, the respective transaction is aborted. In another example, if respective transaction times out after a predetermined time period because the user failed to select a product at the automatic retail machine 122, the respective transaction is aborted. In another example, if the user actuates a bill or coin return mechanism of the automatic retail machine 122, the respective transaction is aborted.

[00111] In some implementations, the transaction detail information 1062 indicates the amount of the respective transaction or the amount of each of multiple transactions (e.g., in a multi-vend scenario). In some implementations, the transaction detail information 1062 also

Draft Only

CSC ServiceWorks - Ex. 1002
Page 920 of 1551

indicates other information related to the respective transaction such as the items dispensed by the automatic retail machine 122 and the type of transaction (e.g., coins, bills, credit card, manual mode, hands-free mode, etc.).

[00112] In some implementations, the miscellaneous information 1064 includes other information related to the payment module 124 and/or the automatic retail machine 122 to which the payment module 124 is coupled. For example, the miscellaneous information 1064 includes a verification request to the server system 108 in order to implement new firmware. In another example, the miscellaneous information 1064 includes transaction information from one or more previous interrupted transactions. In another example, the miscellaneous information 1064 includes transaction information for one or more past hard currency transactions and/or other cashless transactions (e.g., paid with a credit card or bank card at the automatic retail machine 122). In another example, the miscellaneous information 1064 includes inventory information as to one or more products of the automatic retail machine 122.

[00113] Attention is now directed towards implementations of user interfaces ("UIs") and associated processes that may be implemented on a mobile device 104 with zero or more speakers 1102, zero or more microphones 1104, and a display 1106. For example, the display 1106 is a touch screen (sometimes also herein called a "touch screen display") enabled to receive one or more contacts and display information (e.g., media content, websites and web pages thereof, and/or user interfaces for application(s) 326). Figures 11A-11G illustrate exemplary user interfaces for facilitating displaying promotional offers in accordance with some implementations.

[00114] Although some of the examples that follow will be given with reference to inputs on a touch screen (where the touch sensitive surface and the display are combined), in some implementations, the device detects inputs on a touch-sensitive surface that is separate from the display. In some implementations, the touch sensitive surface has a primary axis that corresponds to a primary axis on the display. In accordance with these implementations, the device detects contacts with the touch-sensitive surface at locations that correspond to respective locations on the display. In this way, user inputs detected by the device on the touch-sensitive surface are used by the device to manipulate the user interface on the display of the device when the touch-sensitive surface is separate from the display. It should be

Draft Only

CSC ServiceWorks - Ex. 1002
Page 921 of 1551

understood that similar methods are, optionally, used for other user interfaces described herein.

[00115] Additionally, while the following examples are given primarily with reference to contacts (e.g., finger inputs such as finger contacts, finger tap gestures, finger swipe gestures, etc.), it should be understood that, in some implementations, one or more of the contacts are replaced with input from another input device (e.g., a mouse-based, stylus-based, or physical button-based input). For example, a swipe gesture is, optionally, replaced with a mouse click (e.g., instead of a contact) followed by movement of the cursor along the path of the swipe (e.g., instead of movement of the contact). As another example, a tap gesture is, optionally, replaced with a mouse click while the cursor is located over the location of the tap gesture (e.g., instead of detection of the contact followed by ceasing to detect the contact) or depression of a physical button. Similarly, when multiple user inputs are simultaneously detected, it should be understood that multiple computer mice are, optionally, used simultaneously, or a mouse and finger contacts are, optionally, used simultaneously.

[00116] Figures 11A-11G show user interface 1108 displayed on respective mobile device 104 (e.g., a mobile phone associated with a user) for an application associated with the payment processing system 100; however, one skilled in the art will appreciate that the user interfaces shown in Figures 11A-11G may be implemented on other similar computing devices. The user interfaces in Figures 11A-11G are used to illustrate the processes described herein, including the method described with respect to Figures 12A-12C. One of ordinary skill in the art will appreciate that the following user interfaces are merely examples. Moreover, one of ordinary skill in the art will appreciate that additional affordances and/or user interface elements, or that fewer affordances and/or user interface elements may be used in practice.

[00117] Figure 11A illustrates the mobile device 104 displaying a transaction initiation screen 1110 for 8th floor snack machine. In Figure 11A, the transaction initiation screen 1110 includes a sequence of indicators 1116 showing that 8th floor snack machine is one of three automatic retail machines with which the user is authorized to initiate a transaction. For example, the user of the mobile device 104 is able to access the second of the three automatic retail machines by performing a left-to-right swipe gesture on the user interface 1108 (or alternatively a right-to-left swipe gesture) and the first second the three automatic retail machines by performing a right-to-left swipe gesture on the user interface 1108 (or

Draft Only

CSC ServiceWorks - Ex. 1002
Page 922 of 1551

alternatively a left-to-right swipe gesture). The user of the mobile device 104 is able to access settings and/or a home screen of the application by selecting affordance 1112 (e.g., with a tap gesture), and the user of the mobile device 104 is able to refresh the transaction initiation screen 1110 by selecting affordance 1114 (e.g., with a tap gesture).

[00118] Figure 11A also shows that the user of the mobile device 104 has a prepaid balance of $100.00. The user of the mobile device 104 is able to initiate a transaction with the 8th floor snack machine by performing an upward swipe gesture originating from region 1120 of the transaction initiation screen 1110. The user of the mobile device 104 is able to access special promotional offers by selecting "Special Offers" region 1122 (e.g., with a tap gesture), and the user of the mobile device 104 is able to "like" or favorite the 8th floor snack machine by selecting affordance 1124 (e.g., with a tap gesture). Figure 11A also illustrates the mobile device 104 detecting contact 1140 at a location corresponding to "Special Offers" region 1122.

[00119] Figure 11B illustrates the mobile device 104 displaying a special offers screen 1130 for the 8th floor snack machine. In Figure 11B, the special offers screen 1130 includes: a first region that corresponds to "Offer A" 1152 on product A accompanied by image A of product A; a second region that corresponds to "Offer B" 1154 on product A accompanied by image A of product A; and a third region that corresponds to "Offer C" 1156 on product B accompanied by image B of product B. The special offers screen 1130 also includes refresh affordance 1151, which, when activated (e.g., via a tap gesture), causes the special offers screen 1130 to be refreshed. In Figure 11B, none of Offers A, B, C are currently selected. The user of the mobile device 104 is able to select "Offer A" 1152 by performing a gesture (e.g., a tap gesture) on selection affordance 1153. Similarly, the user of the mobile device 104 is able to select "Offer B" 1154 by performing a gesture (e.g., a tap gesture) on selection affordance 1155 or "Offer C" 1156 by performing a gesture (e.g., a tap gesture) on selection affordance 1157. The user of the mobile device 104 is also able to dismiss or delete any of Offers A, B, or C by performing a right-to-left swipe gesture (or a left-to right swipe gesture in other implementations) in a corresponding region. Figure 11B also illustrates the mobile device 104 detecting a right-to-left swipe gesture within the second region corresponding to "Offer B" 1154 with contact 1160 moving from a first location 1162-a to a second location 1162-b.

[00120] In some implementations, the special offers screen 1130 further includes a fourth region corresponding to "No Selected Offer." For example, the user of the mobile

Draft Only

CSC ServiceWorks - Ex. 1002
Page 923 of 1551

device 104 may view the promotional offers on the special offers screen 1130 but not wish to apply any of them to a future transaction with the 8th floor snack machine. As such, the user of the mobile device 104 may select the "No Selected Offer" region (e.g., with a tap gesture), and, in response, the mobile device 104 re-displays the transaction initiation screen 1110 as shown in Figure 11A.

[00121] Figure 11C illustrates the mobile device 104 displaying delete affordance 1164 within the second region corresponding to "Offer B" 1154 in response to detecting the right-to-left swipe gesture in Figure 11B. The delete affordance 1164, when activated, (e.g., via a tap gesture), causes "Offer B" 1154 to be deleted from the special offers screen 1130. Figure 11C also illustrates mobile device 104 detecting contact 1166 at a location corresponding to delete affordance 1164.

[00122] Figure 11D illustrates the mobile device 104 ceasing to display "Offer B" 1154 within the special offers screen 1130 in response to detecting selection of delete affordance 1164 in Figure 11C. Figure 11D also illustrates mobile device 104 detecting contact 1168 at a location corresponding to selection affordance 1153 for "Offer A" 1152. Alternatively, in some implementations, the user of the mobile device may not wish to apply any of the offers to a future transaction with the 8th floor snack machine. As such, the user may select the affordance 1112 (e.g., with a tap gesture) or perform a predefined gesture on the special offers screen 1130 to re-display the transaction initiation screen 1110 as shown in Figure 11A.

[00123] Figure 11E shows that selection affordance 1153 is selected in response to detecting selection of selection affordance 1153 in Figure 11D. In some implementations, a transaction with the 8th floor snack machine is automatically initiated in response to detecting selection of selection affordance 1153 in Figure 11D. In other implementations, after detecting selection of selection affordance 1153 in Figure 11D, the mobile device 104 re-displays the transaction initiation screen 1110 (as shown in Figure 11A) and the transaction with the 8th floor snack machine is initiated in response to detecting upward swipe gesture originating from region 1120 of the transaction initiation screen 1110.

[00124] Figure 11F illustrates the mobile device 104 displaying a product code screen 1170, which prompts the user of the mobile device 104 to obtain the product code (e.g., UPC code, SKU, or the like) for product A so as to validate Offer A" 1152 selected in Figure 11D.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 924 of 1551

The product code screen 1170 also includes a product code scanner window 1172 for capturing an image of product A and/or scanning the product code of product A. In Figure 11F, UPC code 1174 (e.g., the product code) of product A (e.g., a candy bar), which is in the field of view of a camera of the mobile device 104, is shown within the product code scanner window 1172. For example, the user of the mobile device 104 is able to capture the image of product A (including the UPC code 1174 within the current field of view) or scan the UPC code 1174 by tapping within product code scanner window 1172, issuing an audible command, depressing a predetermined physical button of the mobile device 104, or the like. Figure 11F also shows that the user of the mobile device 104 has a prepaid balance of $99.00, which is $1.00 less than the amount shown in Figures 11A-11E due to purchase of product A.

[00125] Figure 11G illustrates the mobile device 104 displaying an offer validation screen 1180. In some implementations, the mobile device 104 displays the offer validation screen 1180 after the user completes the transaction with the 8th floor snack machine and the server validates the product code information (e.g., the UPC scanned in Figure 11F). In Figure 11G, the offer validation screen 1180 indicates that the "Offer A" 1152 was validated and that the user's balance was credited $0.25. Figure 11G also shows that the user of the mobile device 104 has a prepaid balance of $99.25, which is $0.25 more than the amount shown in Figure 11G due to validation of the "Offer A" 1152 and a credit of $0.25 for the "Offer A" 1152.

[00126] Figures 12A-12C illustrate a flowchart diagram of a method 1200 of providing and handling promotional offers for an automatic retail machine in accordance with some implementations. In some implementations, method 1200 is performed by a mobile device with a display, one or more processors, and memory. For example, in some implementations, method 1200 is performed by mobile device 104 (Figures 1-2) or a component thereof (e.g., the client-side module 102, Figures 1-2). In some implementations, method 1200 is governed by instructions that are stored in a non-transitory computer readable storage medium and the instructions are executed by one or more processors of the mobile device. Some operations in the method 1200 are, optionally, combined and/or the order of some operations is, optionally, changed.

[00127] In some implementations, the payment processing system 100 (Figure 1) includes the mobile device 104, which performs the method 1200, a server system 108, and a payment module 124 coupled with an automatic retail machine 122. An instance of the client-

Draft Only

side module 102 (e.g., as an application) is executed on the mobile device 104 as a foreground or background process to access and communicate with other devices (e.g., the server 108 and the payment module 124) in the payment processing system 100. The server 108 manages the payment processing system 100 and, in some cases, is associated with an entity that supplies, operates, and/or manufactures the payment module 124.

[00128] In some implementations, prior to displaying the one or more promotional offers, the mobile device (1202): obtains an information packet broadcast by a payment module coupled with a automatic retail machine, where the information packet at least includes an authorization code and a unique identifier corresponding to the payment module; send a transaction authorization request to a server, where the transaction authorization includes the authorization code and the unique identifier corresponding to the payment module; and, in response to the transaction authorization request, receive authorization information from the server that includes an authorization grant token for initiating a transaction with the automatic retail machine coupled with the payment module and the one or more promotional offers from the server. As discussed in the process 800, the mobile device 104 or a component thereof (e.g., the broadcast obtaining module 230, Figure 2) receives the information packet broadcast by the payment module 124 which at least includes an authorization code and an identifier associated with the payment module 124. Subsequently, the mobile device 104 or a component thereof (e.g., the transaction authorization module 232, Figure 2) sends the authorization code to the server 108 to pre-authorize a transaction with the automatic retail machine 122 to which the payment module 124 is coupled. In accordance with a determination that the server 108 pre-authorizes the potential transaction, the mobile device 104 or a component thereof (e.g., the transaction authorization module 232, Figure 2) receives an authorization grant token for performing a transaction with the automatic retail machine 122. In some implementations, the mobile device 104 stores the authorization grant token (e.g., in user data 265, Figure 2) until a trigger condition for initiating the transaction with the automatic retail machine 122 is detected (e.g., by the trigger detecting module 236, Figure 2). In some implementations, the trigger condition is satisfied when the mobile device 104 detects a user input on the user interface displayed by the mobile device 104. For example, with reference to Figure 11A, a transaction is initiated between the user of the mobile device 104 and the 8th floor snack machine when the mobile device 104 detects an upward swipe gesture originating from region 1120 of the user interface 1108. In another example, with reference to Figure 11D, a transaction is

Draft Only

CSC ServiceWorks - Ex. 1002
Page 926 of 1551

initiated between the user of the mobile device 104 and the 8th floor snack machine when the mobile device 104 detects selection of Offer A 1152 with contact 1166.

[00129] In some implementations, the mobile device further includes (1204) a first transceiver associated with a short-range communication protocol and a second transceiver associated with a long-range communication protocol. The mobile device communicates with the payment module via the first transceiver, and the mobile device communicates with the server via the second transceiver. For example, the short-range communication protocol is BLE, NFC, or the like, and the long-range communication protocol is GSM, CDMA, Wi-Fi, or the like.

[00130] The mobile device displays (1206) one or more promotional offers on the display. In some implementations, the mobile device 104 only displays promotional offers for products which the user has a sufficient balance. For example, a soda costs $2.00 and there is a promotion for $0.50 off, however, the user has a balance of only $1.00. In this example, the mobile device forgoes displaying the promotion for the soda. Figure 11B, for example, shows the mobile device 104 displaying special offers screen 1130 for the 8th floor snack machine. In Figure 11B, the special offers screen 1130 includes: a first region that corresponds to "Offer A" 1152 on product A accompanied by image A of product A; a second region that corresponds to "Offer B" 1154 on product A accompanied by image A of product A; and a third region that corresponds to "Offer C" 1156 on product B accompanied by image B of product B. Alternatively, in some implementations, a respective one of the one or more promotional offers is applied automatically after the user completes a transaction, and the mobile device prompts the user to provide the product code corresponding to the respective promotion. In some implementations, one or more advertisements are displayed in place of the one or more selectable promotional offers.

Draft Only

[00131] In some implementations, one of the one or more promotional offers is a "reward" for a product or service that is not associated with the automatic retail machine 122 (i.e., an out-of-band offer). For example, if the user purchases a particular product, he/she will receive a link via email for a free download (e.g., a song, video, etc.), in-app credit (e.g., $2.00 for purchases within a digital media marketplace or a $2.00 credit for in-app purchases for a game), or the like. This may or may not require validation of product. For example, buy any product now from this machine and get a link to a $1.00 off coupon via email or text for a case of soda from a retail store. In some implementations, the offer might be an "additional

sale" this is an out-of-band offer. For example, purchase XYZ Cola now, and get a case of XYZ Cola from a store for only $1.50 with a coupon to be mailed to your email address. In another example, purchase ABC Chips now, and get a special discount offer to buy a cool T-shirt for $5.00. In this example, $5.00 is added to transaction price and the user is sent an email regarding redemption and shipping of the cool the T-shirt.

[00132] In some implementations, the user is able to dismiss or delete offers and the mobile device 104 sends this information to the server 108 for analytics purposes. In one example, Figure 11C shows the mobile device 104 displaying delete affordance 1164 within the second region corresponding to "Offer B" 1154 in response to detecting the right-to-left swipe gesture in Figure 11B. Continuing with this example, Figure 11D shows the mobile device 104 ceasing to display "Offer B" 1154 within the special offers screen 1130 in response to detecting selection of delete affordance 1164 in Figure 11C.

[00133] In some implementations, the one or more promotional offers are identified (1208) based on at least one of: a unique identifier corresponding to the payment module, at least one of the current time and date, a location of the automatic retail machine, a location of the mobile device, and a unique identifier corresponding to the user of the mobile device. In some implementations, the server 108 or a component thereof (e.g., offer determining module 328, Figure 3) determines/identifies the one or more promotional offers based on the current time/date, current location, device ID associated with the payment module, user ID associated with the user of the mobile device, and the like. In some implementations, the mobile device 104 or a component thereof (e.g., the offer(s) module 234, Figure 2) determines/identifies the one or more promotional offers from a pre-stored collection of offers based on the current time/date, current location, device ID associated with the payment module, user ID associated with the user of the mobile device, and the like. For example, the mobile device 104 identifies the one or more promotional offers from the offers database 266 which includes offers sent by the server 108 at a prior time such as a part of an update to the application.

[00134] In some implementations, the promotional offers are identified based on the products stocked in the automatic retail machine 122 or past behavior (e.g., previous offers selected by the user, previous offers deleted by the user, previous offers not selected by the user, etc.). For example, side-by-side are separate snack and soda vending machines. The user buys a soda first. Then, when the user goes to transact with the snack machine, the user is presented with an offer for a particular product (e.g., to enable cross promotions between

Draft Only

CSC ServiceWorks - Ex. 1002
Page 928 of 1551

soda and snack distributors). Alternatively, the offers could be based on what a user did not select from the soda machine or offers that were actively deleted before.

[00135] In some implementations, the provider of the server 108 and payment module 124 manages a promotion marketplace to facilitate placing of promotional offers by manufacturers and distributors of products and to also facilitate competition between various product manufacturers and distributors. For example, a distributor or manufacturer of a product may place a promotional offer for $0.25 off on a particular item in all applicable community colleges in California on Thursdays between 2:00 and 4:00 PM PDT. In another example, a distributor or manufacturer of a product may place a promotional offer for 50% off on the product on the day the product expires (e.g., to sell perishable sandwiches or the like) for all applicable automatic retail machines. In some implementations, cross-promotional offers or complex promotional offers may also be placed whereby a user gets a credit (e.g., a rebate) for purchasing a particular drink and snack combination where each are manufactured or distributed by different entities.

[00136] In some implementations, a promotional offer on all items in automatic retail machines on a entity's campus (essentially a subsidy) is only available to select users. For example, all attorneys and staff at a law firm are given a subsidized rate on snacks but cleaning persons do not benefit from said subsidized rate. In another example, all full-time employees are given a subsidized rate on snacks but temporary workers do not benefit from said subsidized rate.

[00137] In some implementations, variable pricing is enacted whereby the base price of items changes and promotion offers may be added in addition to the variable pricing scheme. For example, a distributer wishes to decrease the price on all items in applicable machines during the off-peak hours (e.g., 9:00 PM – 6:00 AM). Therefore, after a transaction is completed, the server 108 will only charge a user the decreased price, and, after the server processes and accounts for the transaction, transaction acknowledgment information displayed at the mobile device 104 will indicate that the user was only charged the decreased price and not the price shown at the automatic retail machine 122.

[00138] The mobile device detects (1210) a user input selecting a respective promotional offer of the one or more promotional offers. For example, the user input is a touch input, voice input, or the like. Figure 11D, for example, shows the mobile device 104

Draft Only

CSC ServiceWorks - Ex. 1002
Page 929 of 1551

detecting selection of selection affordance 1153 for "Offer A" 1152, and Figure 11E shows that selection affordance 1153 is selected in response to detecting selection of selection affordance 1153 in Figure 11D. In some implementations, the respective promotional offer is a negative one, such as a donation to AIDS research, that adds a selected amount to the user's next transaction. Alternatively, in some implementations, the respective promotional offer is a negative one whereby the transaction is rounded up to the nearest dollar, where additional amount is donated to a Cancer research foundation.

[00139] The mobile device initiates (1212) performance of a transaction with an automatic retail machine coupled with a payment module, where the transaction corresponds to purchase of a product stocked by the automatic retail machine. In some implementations, the transaction is initiated in response to selection of the respective promotional offer (i.e., one-click transaction initiation process). For example, a transaction with the 8th floor snack machine is automatically initiated in response to detecting selection of selection affordance 1153 in Figure 11D. In other implementations, after the user selects an offer the user performs an action to initiate a transaction with the automatic retail machine (i.e., a two-step transaction initiation process). For example, after detecting selection of selection affordance 1153 in Figure 11D, the mobile device 104 re-displays the transaction initiation screen 1110 (as shown in Figure 11A) and the transaction with the 8th floor snack machine is initiated in response to detecting upward swipe gesture originating from region 1120 of the transaction initiation screen 1110.

[00140] In some implementations, performance of the transaction with the automatic retail machine coupled with the payment module is initiated (1214) by sending the authorization grant token to the payment module, where the authorization grant token includes the authorization code included in the broadcast information packet. In some implementations, initiating performance of the transaction includes the mobile device 104 or a component thereof (e.g., the transaction initiating module 238, Figure 2) sending the stored authorization grant token to the payment module 124 for payment and the user manually selects a product using the user interface of the automatic retail machine 122. As such, the automatic retail machine 122 knows nothing about the selected promotional offer – it only knows that the user sent it a payment. For example, the automatic retail machine 122 returns transaction and product information that is passed to the mobile device 104 by the payment module 124 but it cannot determine or state in any way if it is a product that corresponds to

Draft Only

CSC ServiceWorks - Ex. 1002
Page 930 of 1551

the offer. For example, the transaction completion notification indicates "I vended E3 for $1.00".

[00141] The mobile device receives (1216) a transaction completion notification from the payment module, where the transaction completion notification indicates that the product corresponding to the selected respective promotional offer was vended by the automatic retail machine. In some implementations, the mobile device 104 or a component thereof (e.g., the transaction completion notification receiving module 240, Figure 2) receives transaction completion notification (e.g., the transaction status information, the transaction detail information, the other miscellaneous information regarding the respective payment module 124 and/or the automatic retail machine 122 to which the respective payment module 124 is coupled, and/or the like) from the payment module 124 after the user manually selects a product using the user interface of the automatic retail machine 122. In some implementations, the transaction completion notification includes the good/service associated with the transaction, the current inventory of the automatic retail machine 122, information associated with one or more previous cash transactions, information associated with one or more interrupted transactions handled by the payment module 124, and/or other information associated with the automatic retail machine 122 such as error or maintenance states. In some implementations, the payment module 124 sends an error message in place of the transaction completion notification when the transaction is aborted or an error occurs during the transaction such as unavailability of a requested good/service or a vending jam.

[00142] In response to receiving the transaction completion notification, the mobile device provides (1218) a prompt to the user of the mobile device to obtain a product code for the vended product to validate the respective promotional offer. In some implementations, the mobile device 104 or a component thereof (e.g., the product code processing module 242, Figure 2) displays a scanning interface for capturing the product code of the vended item after receiving the transaction completion notification. Figure 11F, for example, shows the mobile device 104 displaying a product code screen 1170, which prompts the user of the mobile device 104 to obtain the product code (e.g., UPC code, SKU, or the like) for product A so as to validate Offer A" 1152 selected in Figure 11D. The product code screen 1170 also includes a product code scanner window 1172 for capturing an image of product A and/or scanning the product code of product A. In Figure 11F, the UPC code 1174 of product A (e.g., a candy bar), which is in the field of view of a camera of the mobile device 104, is

Draft Only

shown within the product code scanner window 1172. For example, the user of the mobile device 104 is able to capture the image of product A (including the UPC code 1174 within the current field of view) or scan the UPC code 1174 by tapping within product code scanner window 1172, issuing an audible command, depressing a predetermined physical button of the mobile device 104, or the like.

[00143] In other implementations, the mobile device 104 or a component thereof (e.g., the product code processing module 242, Figure 2) displays a pop-up message or banner notification on the display prompting the user of the mobile device 104 to manually enter or otherwise obtain the product code of the vended item. In other implementations, the mobile device 104 or a component thereof (e.g., the product code processing module 242, Figure 2) provides an audible tone, a vocal prompt, or a sequence of tactile/haptic vibrations prompting the user of the mobile device 104 to enter or otherwise obtain the product code of the vended item.

[00144] The mobile device obtains (1220) the product code for the vended product. For example, the user enters the barcode character-by-character, scans the barcode, or simply captures an image of the barcode. In some implementations, the mobile device 104 or a component thereof (e.g., the product code processing module 242, Figure 2) receives the product code.

[00145] In some implementations, obtaining the product code further comprises (1222): capturing an image of the product that includes the product code; and extracting the product code from the captured image. In some implementations, obtaining the product code further comprises (1224): scanning the product code of the product with a scanner unit of the mobile device. For example, the user of the mobile device 104 is able to access a product code capture plug-in from within the application associated with the payment processing system 100 (e.g., the product code processing module 242, Figure 2) which enables the user to capture an image of the product with the product code in the field of view or scan the product code of the product. In this example, the mobile device 104 extracts the product code from the captured image and sends the extracted product code to the server 108 or, alternatively, the mobile device 104 sends the captured image to the server 108 where the product code is extracted. In another example, the user of the mobile device 104 is able to manually enter the product code from within the application (e.g., via a virtual keypad) or via a website associated with the payment processing system 100.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 932 of 1551

[00146] After obtaining the product code, the mobile device transmits (1226) the product code to the server. In response to transmitting the product code, the mobile device: receives promotion validation information from the server; and displays the promotion validation information on the display, where the promotion validation information indicates whether the respective promotion offer was validated. In some implementations, the mobile device 104 or a component thereof (e.g., the product code processing module 242, Figure 2) either validates the obtained product code or sends the obtained product code to the server 108 for validation. In some implementations, the mobile device 104 or a component thereof (e.g., the information relaying module 244, Figure 2) sends the transaction completion notification or a portion thereof to the server 108 regardless of whether the user follows the prompt and the mobile device 104 ultimately obtains the product code. In some implementations, the server 108 determines whether conditions for the respective promotional offer have been based on the transaction and the product code. For example, the server 108 determines whether the proper product code was obtained for the respective promotional offer, whether the respective promotional offer has expired, whether the user has fulfilled a buy N items get one free condition, whether the user has fulfilled cross-promotion condition, and/or the like. In some implementations, the offer is validated and applied by the server 108 to the user's account.

[00147] In some implementations, the mobile device 104 of a component thereof (e.g., the offer validation module 246, Figure 2) receives and displays the promotion validation information. For example, the promotion validation information indicates whether the offer was validated and an updated user balance/transaction listing. Figure 11G, for example, shows the mobile device 104 displaying an offer validation screen 1180, which indicates that the "Offer A" 1152 was validated and that the user's balance was credited $0.25. Figure 11G also shows that the user of the mobile device 104 has a prepaid balance of $99.25, which is $0.25 more than the amount shown in Figure 11G due to validation of the "Offer A" 1152 and a credit of $0.25 for the "Offer A" 1152. For example, when the user gets a fifth purchased product free and the product that was the subject of the instant transaction was only the first item purchased, the promotion validation information indicates that the user must buy 3 more of the product before he/she gets a free product. In some implementations, the promotion validation information includes a coupon for a product or service that is not associated with the automatic retail machine 122 For example, the user is emailed a coupon for $5 off an amusement park for purchasing a soda.

Draft Only

[00148] In some implementations, after obtaining the product code, the mobile device determines (1228) whether a predetermined time period has expired. In accordance with a determination that the time period has expired, the mobile device provides a notification to the user of mobile device indicating that the respective promotional offer has expired. In accordance with a determination that the time period has not expired, the mobile device transmits the product code to the server. In some implementations, the predetermined time period corresponds to the time between (A) initiating performance of the transaction or prompting for the product code, (B) obtaining the product code or some other time period. For example, the mobile device 104 must receive the product code within 5 minutes of the prompt or within 5 minutes of initiation of the transaction. In some implementations, this may occur hours or even days later. In some implementations, a predetermined proximity between a first location where the transaction was initiated and a second location where the product code was obtained is used in addition to or in place of the predetermined time period.

[00149] In some implementations, the application associated with the payment processing system 100 has a coupon plug-in whereby the user of the mobile device 104 is able to scan a coupon after completing a transaction for a product and also scan the product code of the product to get a post hoc rebate for the transaction.

[00150] In some implementations, the promotion validation information indicates (1230) the price of the product after the application of the respective promotional offer. For example, the mobile device 104 displays the total deducted from the user's account or charged to the user's linked bank card after application of the promotional offer to the base purchase price included in the notification completion information. Figure 11G, for example, shows that the user of the mobile device 104 has a prepaid balance of $99.25, which is $0.25 more than the amount shown in Figure 11G due to validation of the "Offer A" 1152 and a credit of $0.25 for the "Offer A" 1152.

[00151] In some implementations, the mobile device transmits (1232) the transaction completion notification to the server. In some implementations, the mobile device 104 or a component thereof (e.g., the information relaying module 244, Figure 2) sends the transaction completion notification (e.g., the transaction status information, the transaction detail information, the other miscellaneous information regarding the respective payment module 124 and/or the automatic retail machine 122 to which the respective payment module 124 is coupled, and/or the like) or a portion thereof to the server 108 prior to sending the product

Draft Only

code or along with the product code. In some implementations, the transaction completion notification or a portion thereof is sent to the server 108 regardless of whether the user follows the prompt and the mobile device ultimately obtains the product code.

[00152] It should be understood that the particular order in which the operations in Figures 12A-12C have been described is merely exemplary and is not intended to indicate that the described order is the only order in which the operations could be performed. One of ordinary skill in the art would recognize various ways to reorder the operations described herein. Additionally, it should be noted that details of other processes described herein with respect to other methods and/or processes described herein (e.g., the processes 800 and 900) are also applicable in an analogous manner to method 1200 described above with respect to Figures 12A-12C.

[00153] While particular implementations are described above, it will be understood it is not intended to limit the application to these particular implementations. On the contrary, the application includes alternatives, modifications and equivalents that are within the spirit and scope of the appended claims. Numerous specific details are set forth in order to provide a thorough understanding of the subject matter presented herein. But it will be apparent to one of ordinary skill in the art that the subject matter may be practiced without these specific details. In other instances, well-known methods, procedures, components, and circuits have not been described in detail so as not to unnecessarily obscure aspects of the implementations.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 935 of 1551

WHAT IS CLAIMED IS:

1. A method, comprising:

at a mobile device including a display, one or more processors, and memory:

displaying one or more promotional offers on the display;

detecting a user input selecting a respective promotional offer of the one or more promotional offers;

initiating performance of a transaction with an automatic retail machine coupled with a payment module, wherein the transaction corresponds to purchase of a product stocked by the automatic retail machine;

receiving a transaction completion notification from the payment module, wherein the transaction completion notification indicates that the product corresponding to the selected respective promotional offer was vended by the automatic retail machine;

in response to receiving the transaction completion notification, providing a prompt to the user of the mobile device to obtain a product code for the vended product to validate the respective promotional offer;

obtaining the product code for the vended product;

after obtaining the product code, transmitting the product code to the server; and,

in response to transmitting the product code:

receiving promotion validation information from the server; and

displaying the promotion validation information on the display, wherein the promotion validation information indicates whether the respective promotion offer was validated.

2. The method of claim 1, wherein the one or more promotional offers are identified based on at least one of: a unique identifier corresponding to the payment module, at least one of a current time and date, a location of the automatic retail machine, a location of the mobile device, and a unique identifier corresponding to the user of the mobile device.

3. The method of any one of claims 1-2, further comprising:

prior to displaying the one or more promotional offers:

obtaining an information packet broadcast by the payment module coupled with the automatic retail machine, wherein the information packet at least includes an authorization code and a unique identifier corresponding to the payment module;

Draft Only

CSC ServiceWorks - Ex. 1002
Page 936 of 1551

sending a transaction authorization request to a server, wherein the transaction authorization includes the authorization code and the unique identifier corresponding to the payment module; and,

in response to the transaction authorization request, receiving authorization information from the server that includes an authorization grant token for initiating a transaction with the automatic retail machine coupled with the payment module and the one or more promotional offers from the server.

4. The method of claim 3, wherein performance of the transaction with the automatic retail machine coupled with the payment module is initiated by sending the authorization grant token to the payment module, wherein the authorization grant token includes the authorization code included in the broadcast information packet.

5. The method of claim 1, wherein obtaining the product code further comprises:
capturing an image of the product that includes the product code; and
extracting the product code from the captured image.

6. The method of claim 1, wherein obtaining the product code further comprises:
scanning the product code of the product with a scanner unit of the mobile device

7. The method of any one of claims 1, 2, and 4-6, wherein the promotion validation information indicates the price of the product after the application of the respective promotional offer.

8. The method of any one of claims 1, 2, and 4-6, further comprising:

after obtaining the product code, determining whether a predetermined time period has expired;

in accordance with a determination that the time period has expired, providing a notification to the user of mobile device indicating that the respective promotional offer has expired; and,

in accordance with a determination that the time period has not expired, transmitting the product code to the server.

9. The method of any one of claims 1, 2, and 4-6, further comprising:
transmitting the transaction completion notification to the server.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 937 of 1551

10. The method of any one of claims 1, 2, and 4-6, wherein the mobile device further includes a first transceiver associated with a short-range communication protocol and a second transceiver associated with a long-range communication protocol.

11. A mobile device, comprising:

a display;

one or more processors; and

memory storing one or more programs to be executed by the one or more processors, the one or more programs comprising instructions for performing the method of any one of claims 1-10.

12. A non-transitory computer readable storage medium storing one or more programs, the one or more programs comprising instructions, which, when executed by a mobile device with a display and one or more processors, cause the computing device to perform the method of any one of claims 1-10.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 938 of 1551

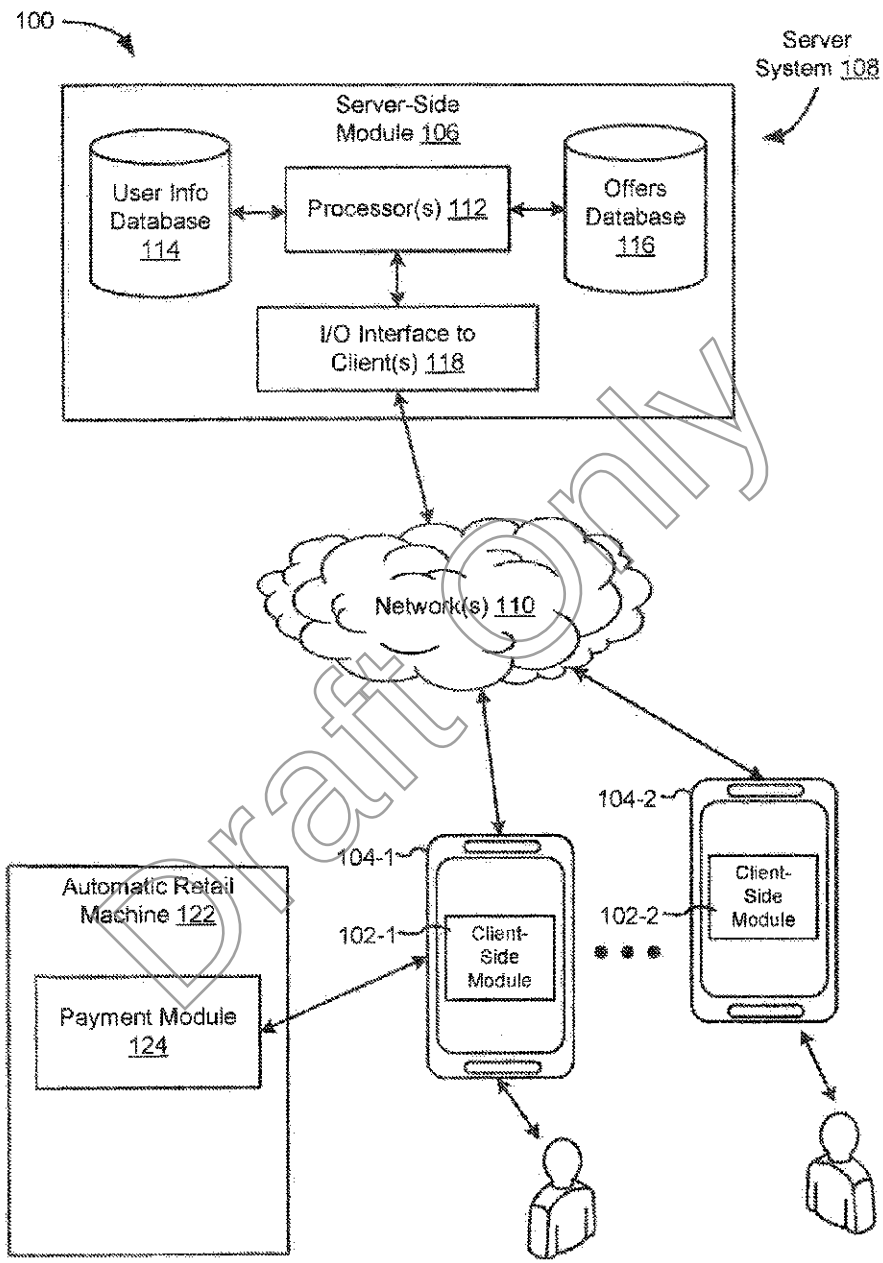


Figure 1

Draft Only

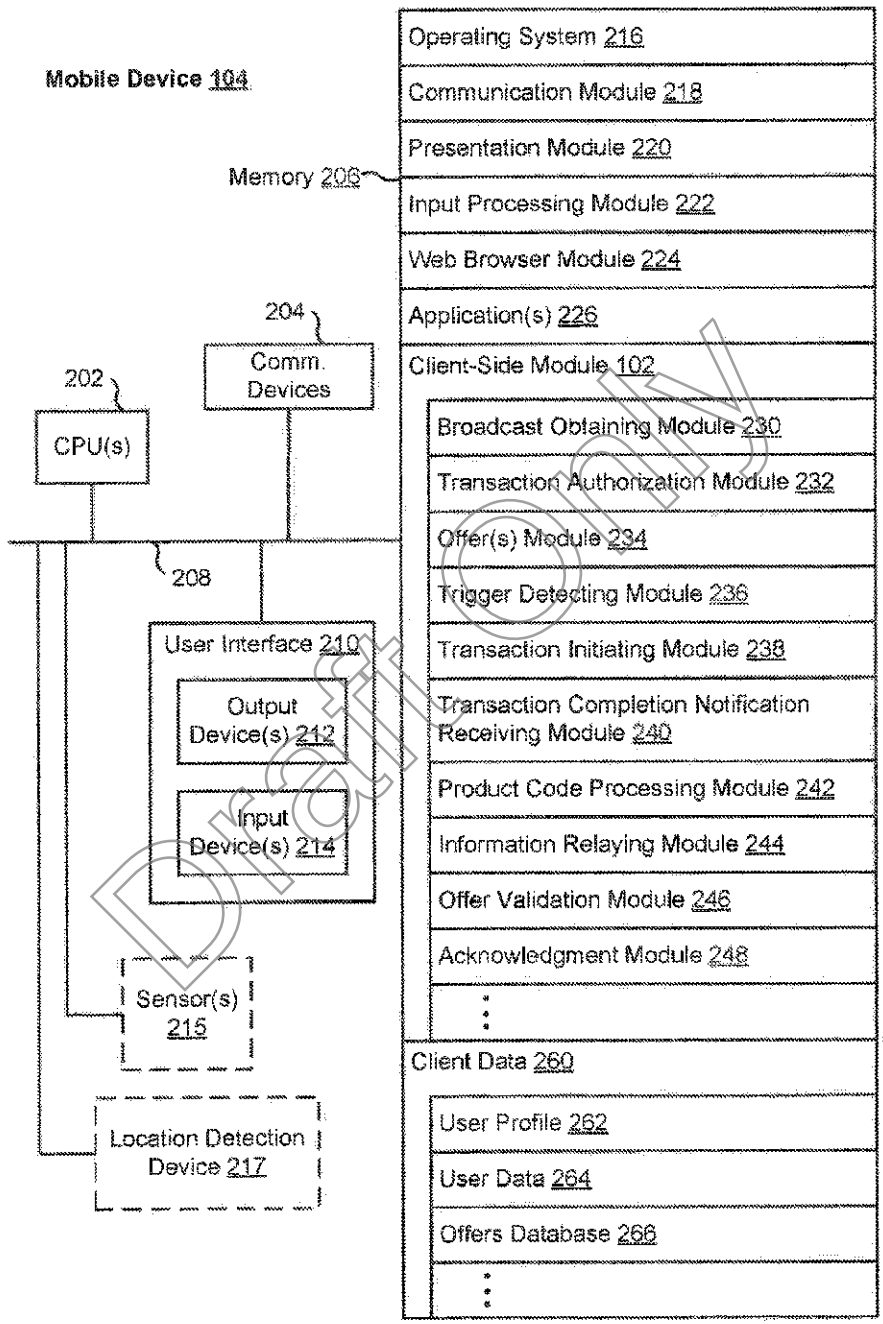
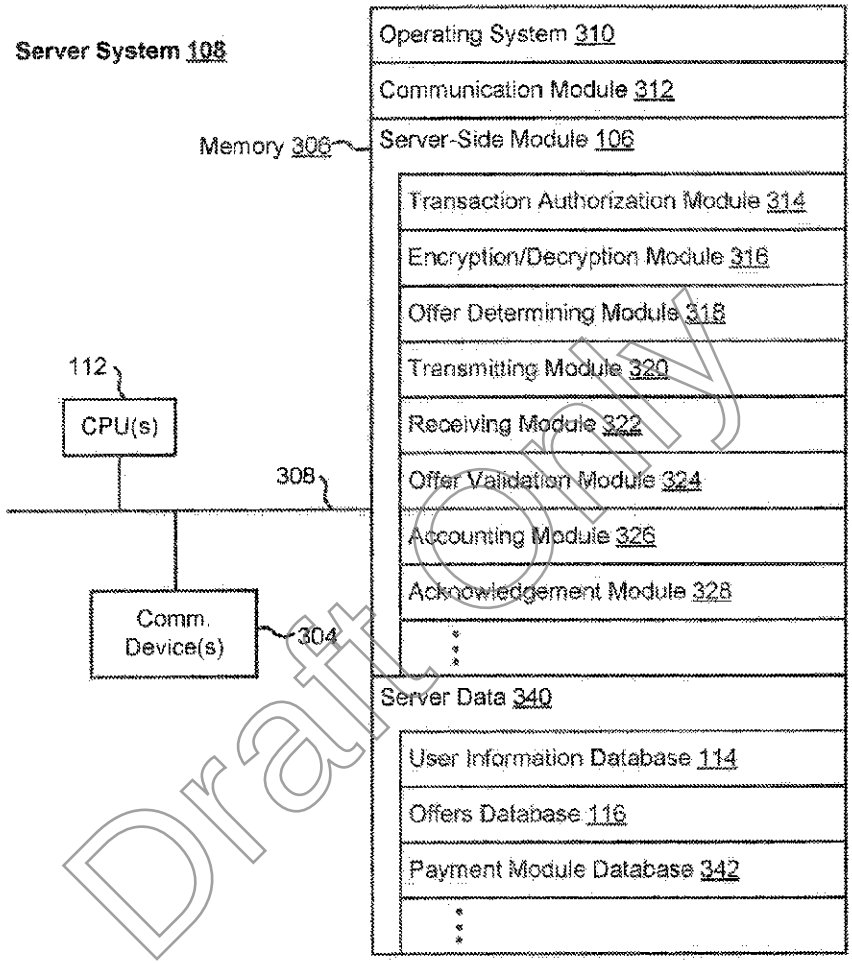


Figure 2

Draft Only



Draft only

Figure 3

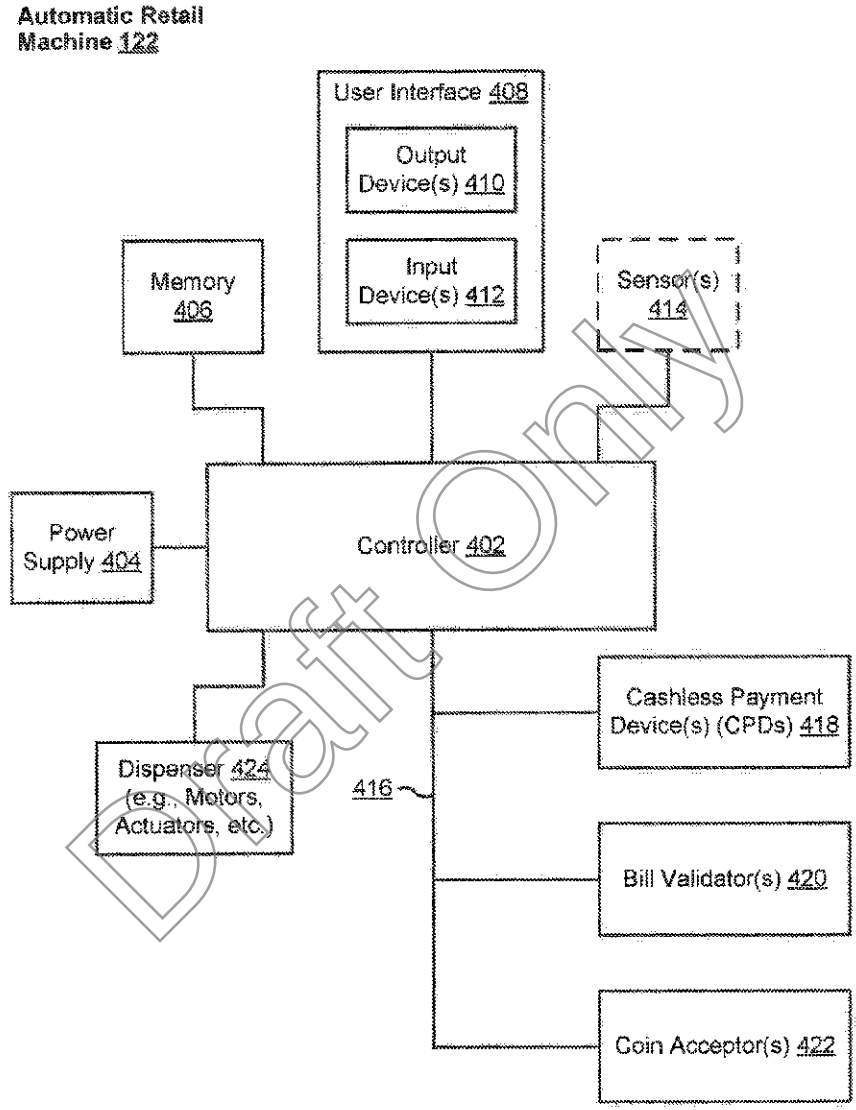
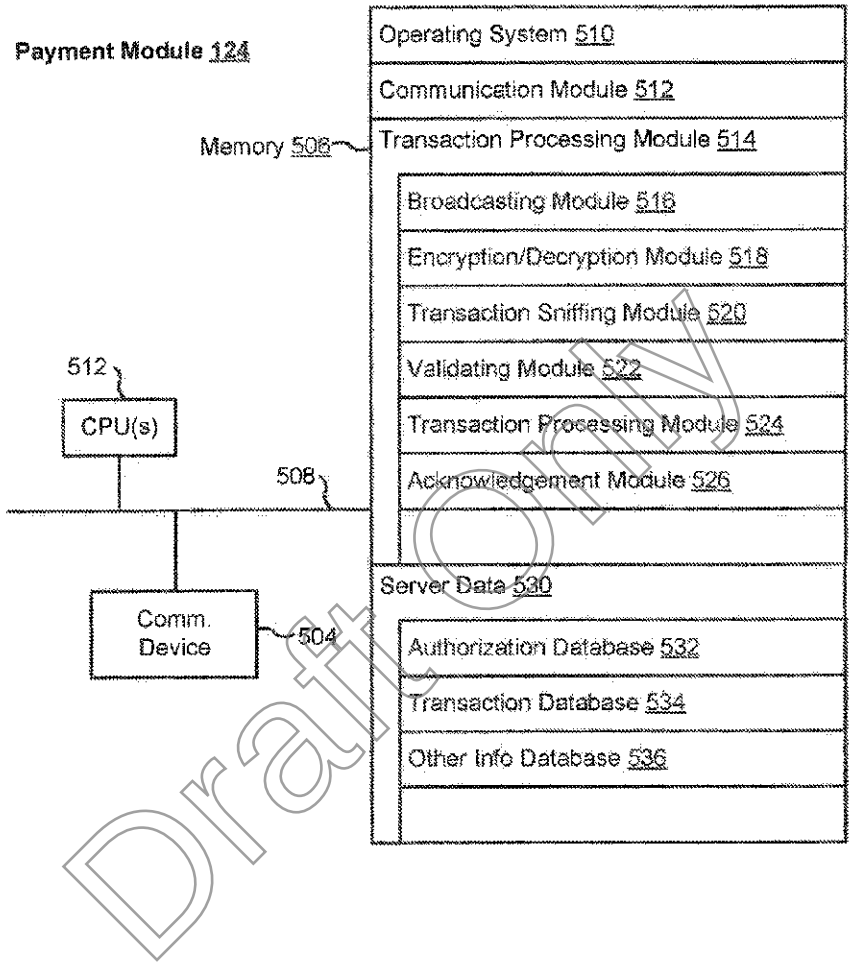


Figure 4

Draft Only



Draft Only

Figure 5

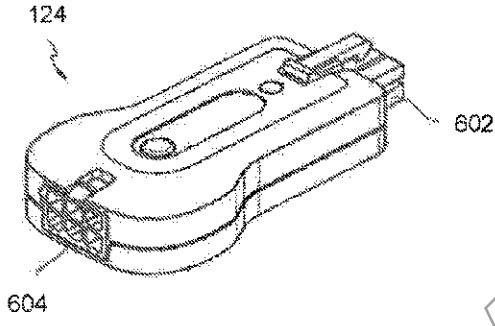


Figure 6A

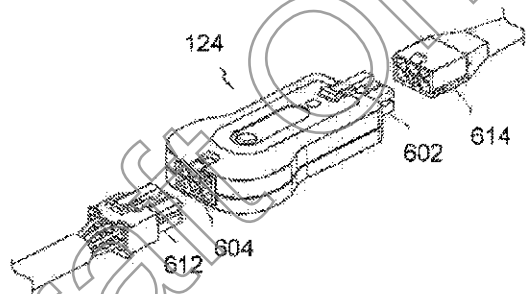
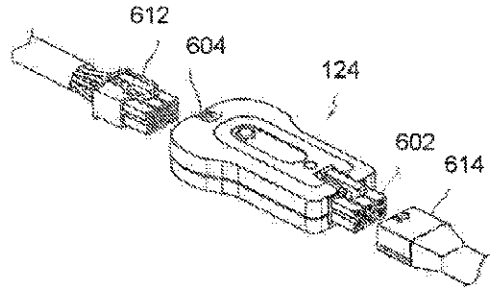
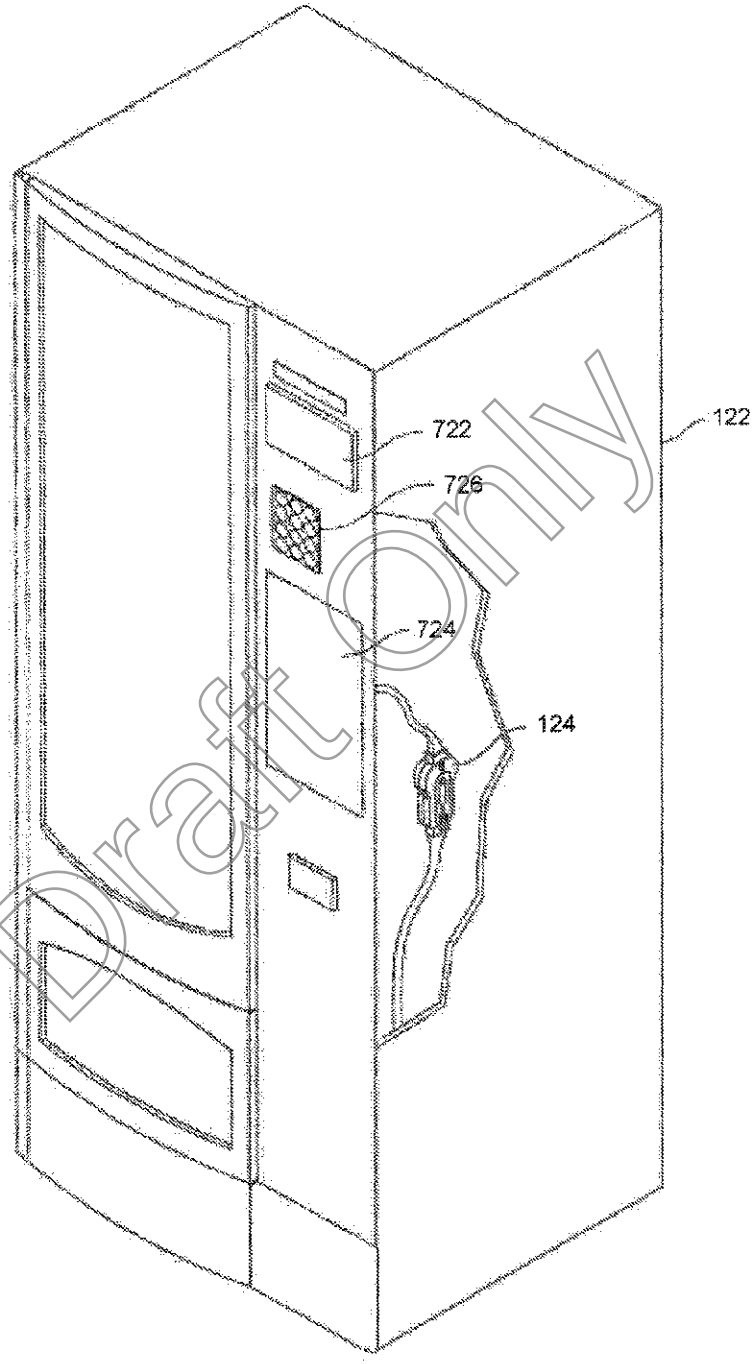


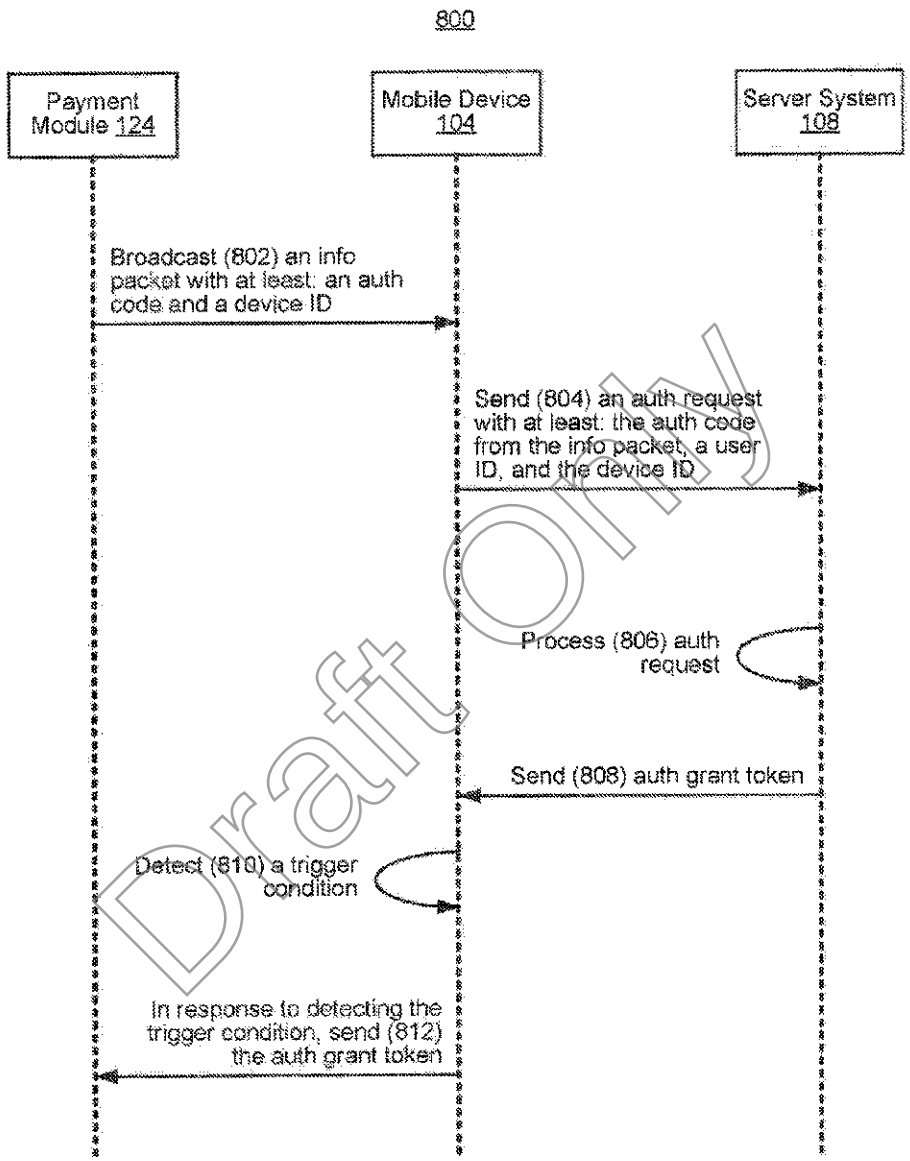
Figure 6B



Draft Only

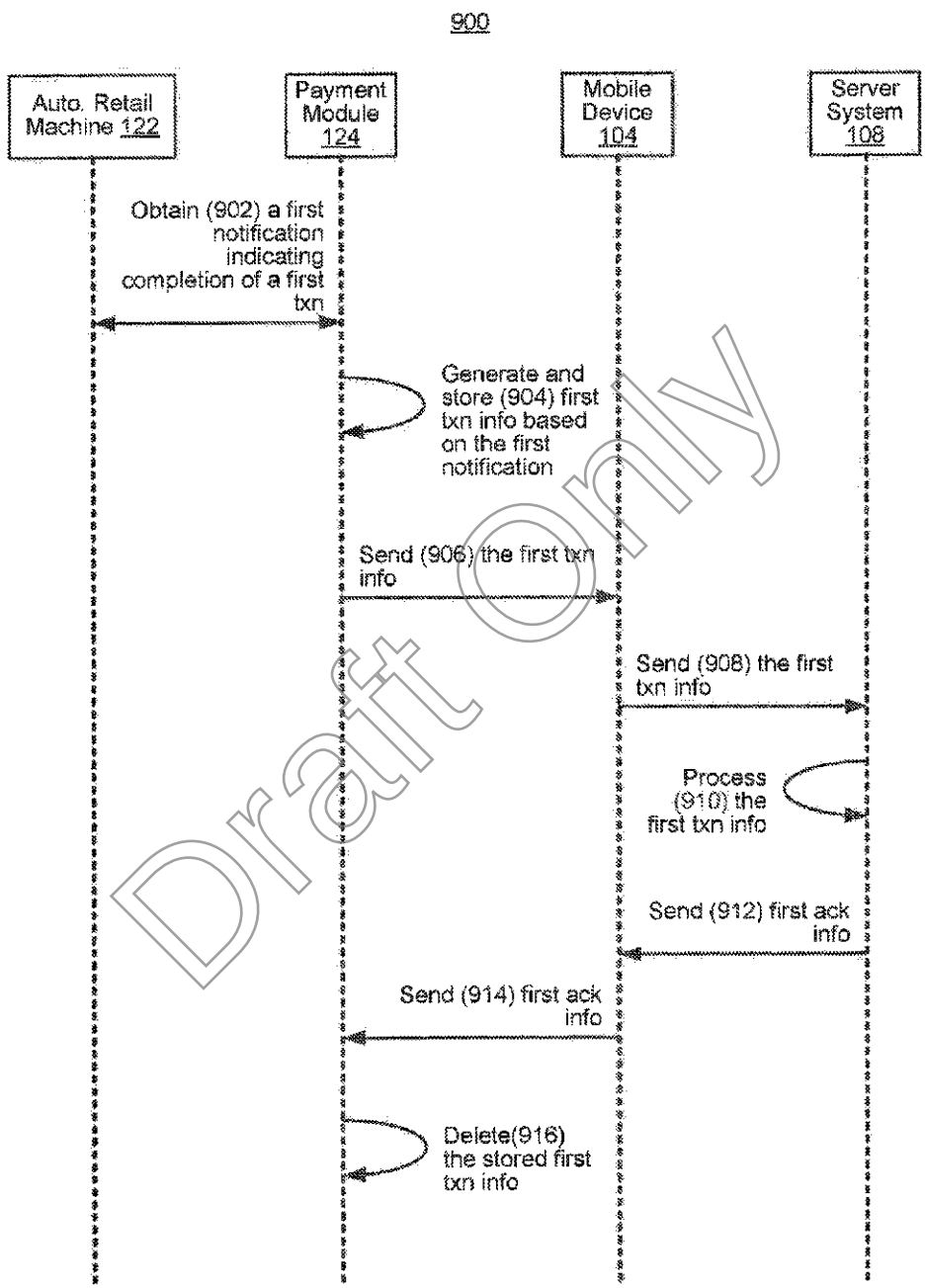


Draft Only



Draft Only

Figure 8



Draft Only

Figure 9

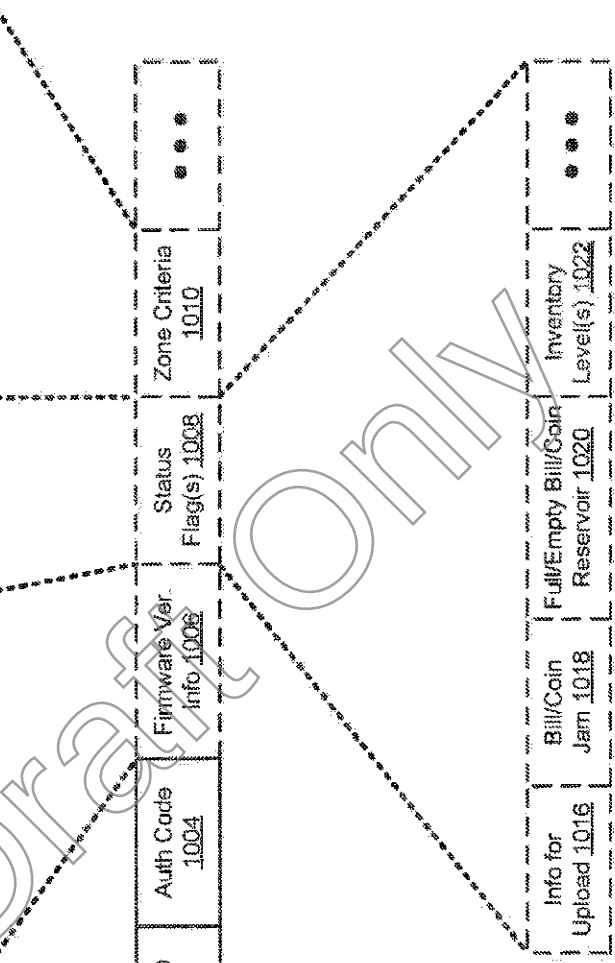


Figure 10A

Draft Only

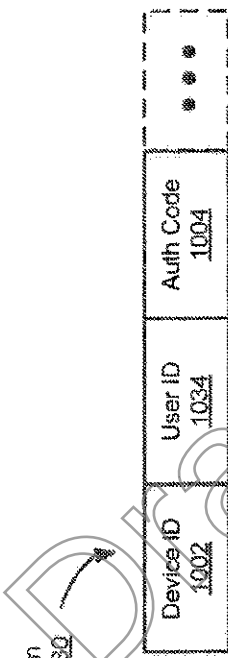


Figure 10B

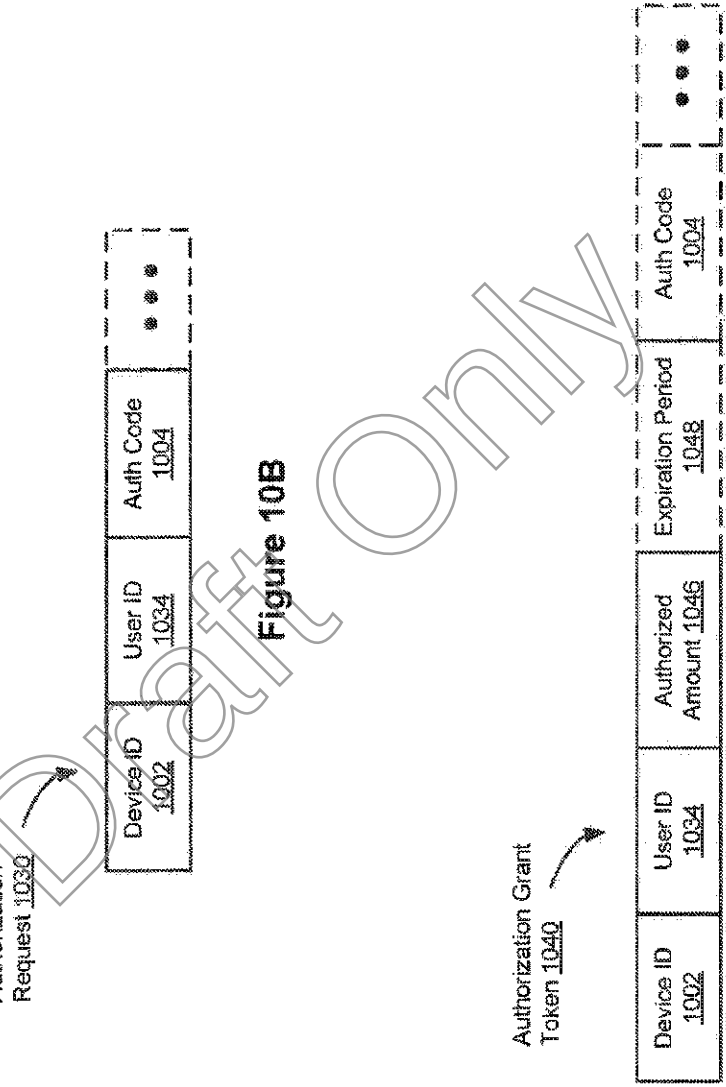


Figure 10C

Draft Only

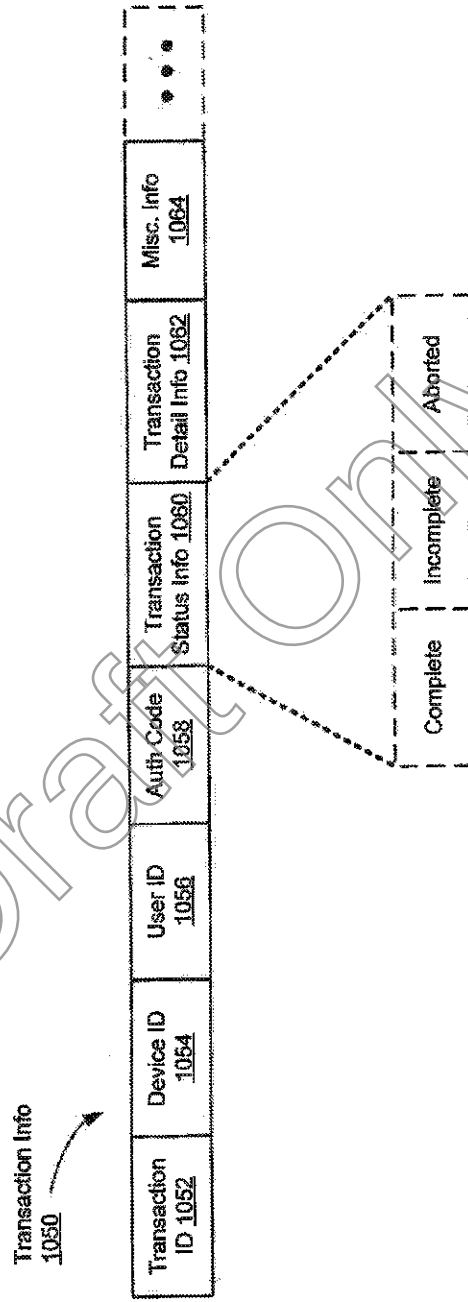
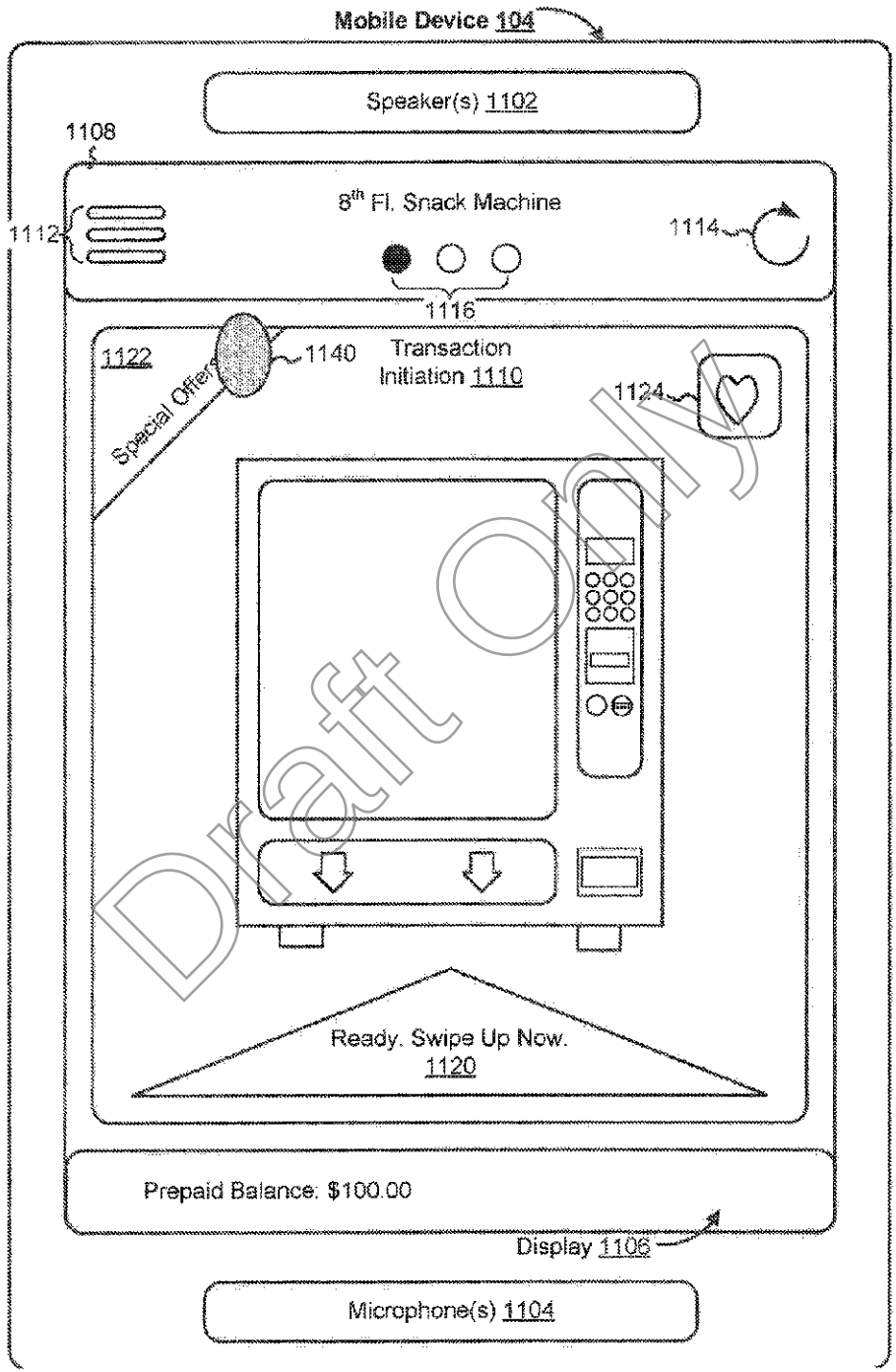
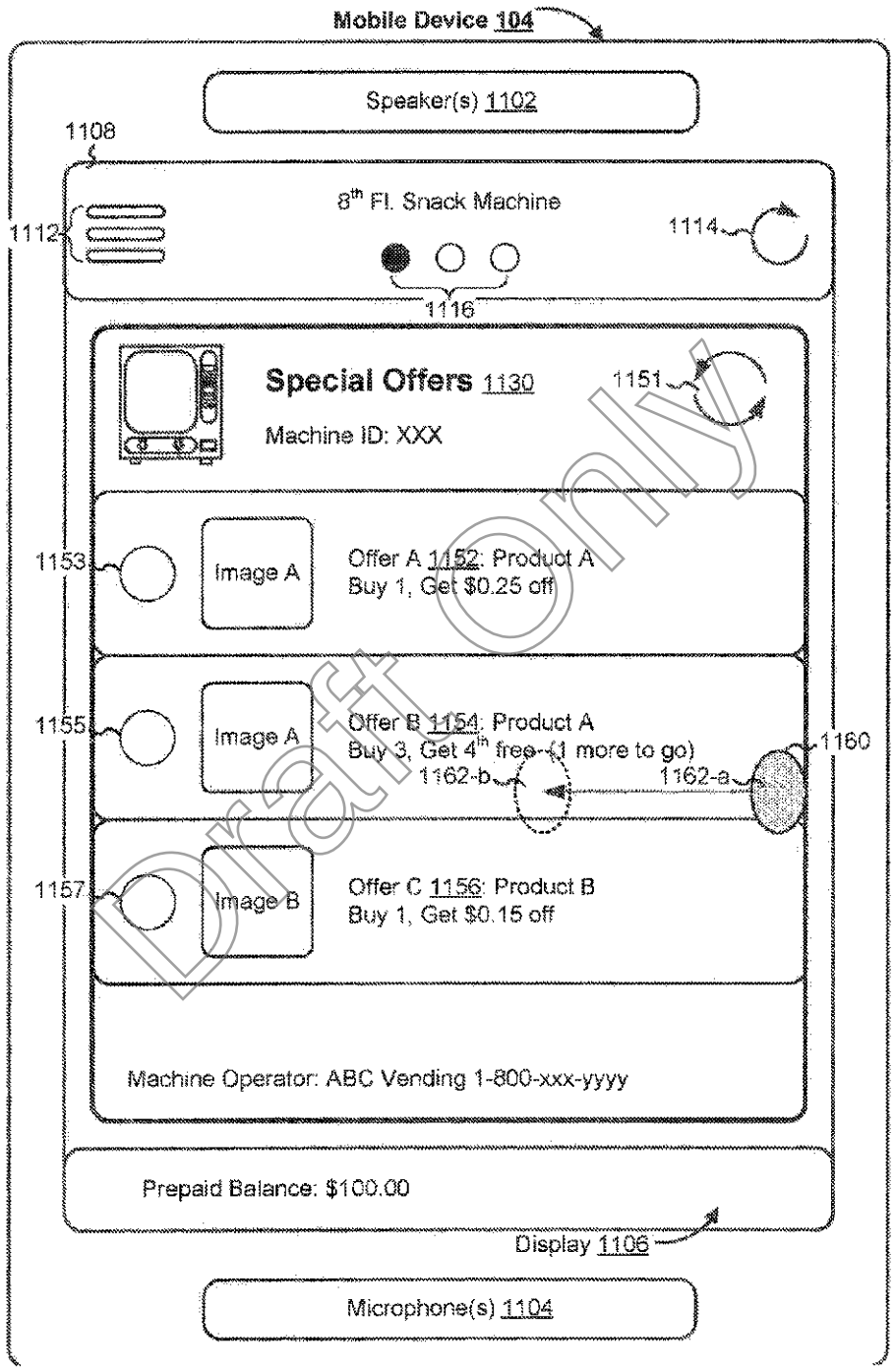


Figure 10D

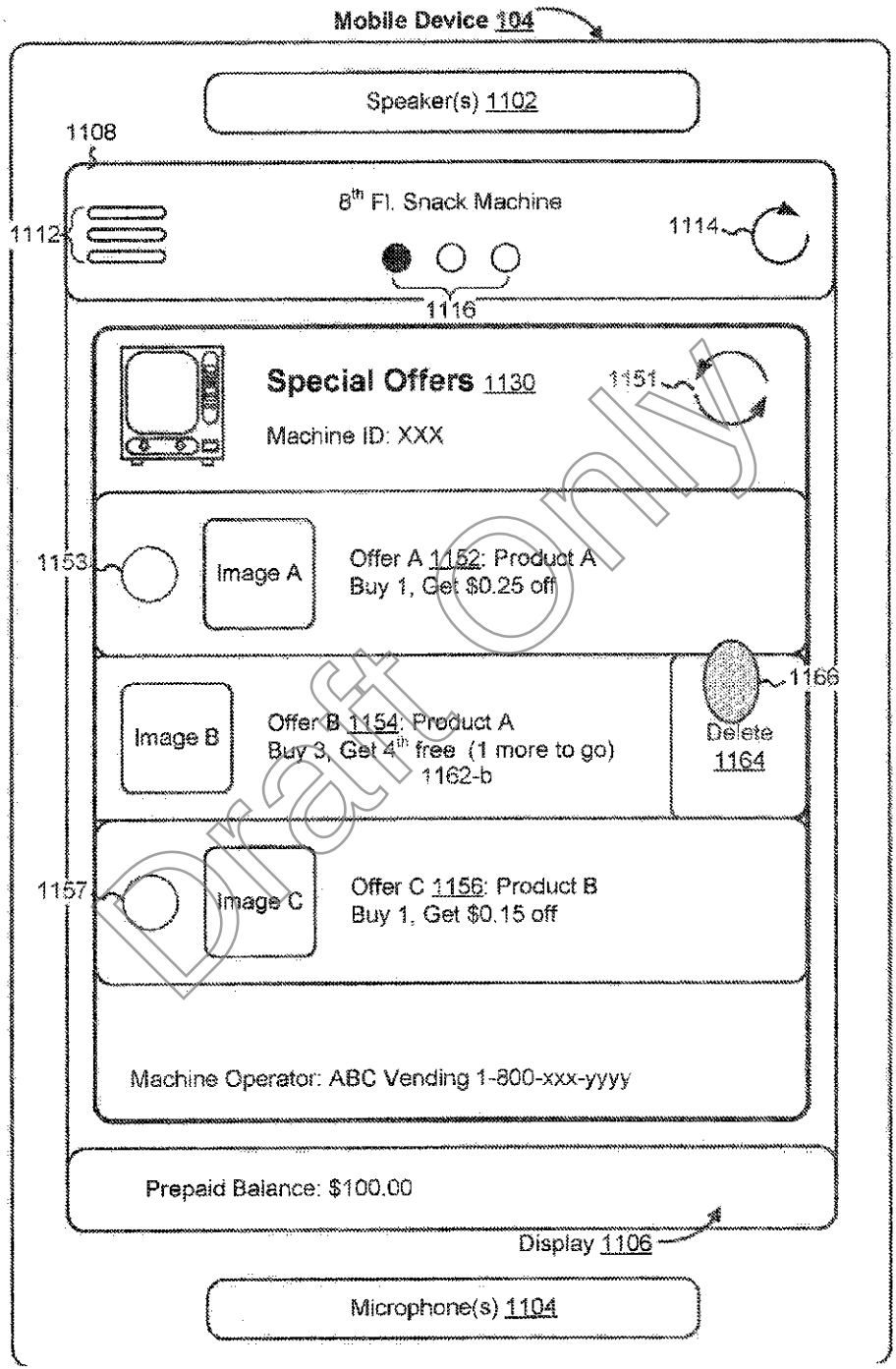
Draft Only


Mobile Device 104
Speaker(s) 1102
1108
8th Fl. Snack Machine
1112
1114
1116
1122
1140
Transaction Initiation 1110
Special Offer
1124
Ready. Swipe Up Now.
1120
Prepaid Balance: $100.00
Display 1106
Microphone(s) 1104

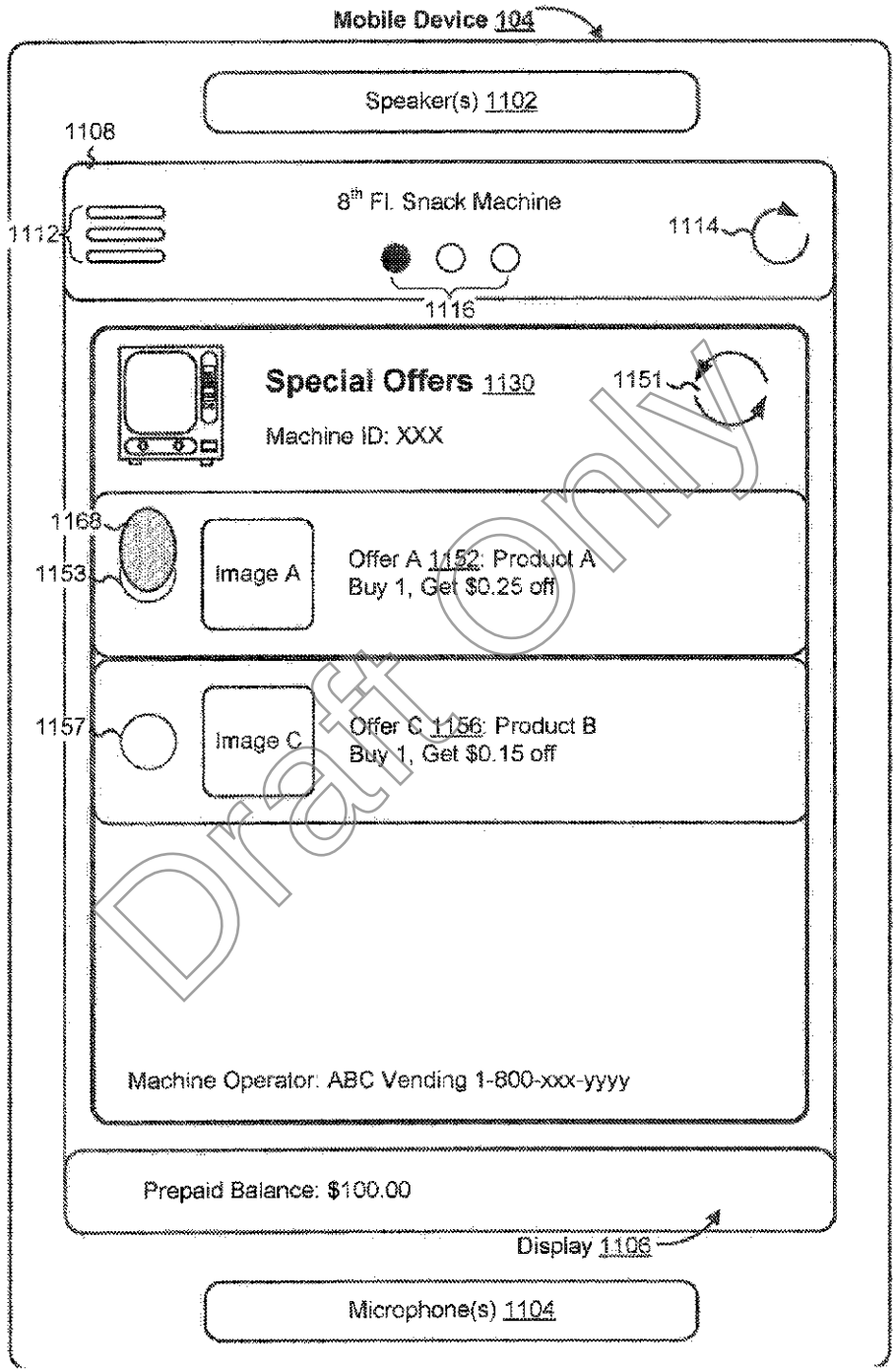
Draft Only


Mobile Device 104
Speaker(s) 1102
1108
8th Fl. Snack Machine
1112
1114
1116
Special Offers 1130
1151
Machine ID: XXX
1153
Image A
Offer A 1152: Product A
Buy 1, Get $0.25 off
1155
Image A
Offer B 1154: Product A
Buy 3, Get 4th free-(1 more to go)
1160
1162-b
1162-a
1157
Image B
Offer C 1156: Product B
Buy 1, Get $0.15 off
Machine Operator: ABC Vending 1-800-xxx-yyyy
Prepaid Balance: $100.00
Display 1106
Microphone(s) 1104

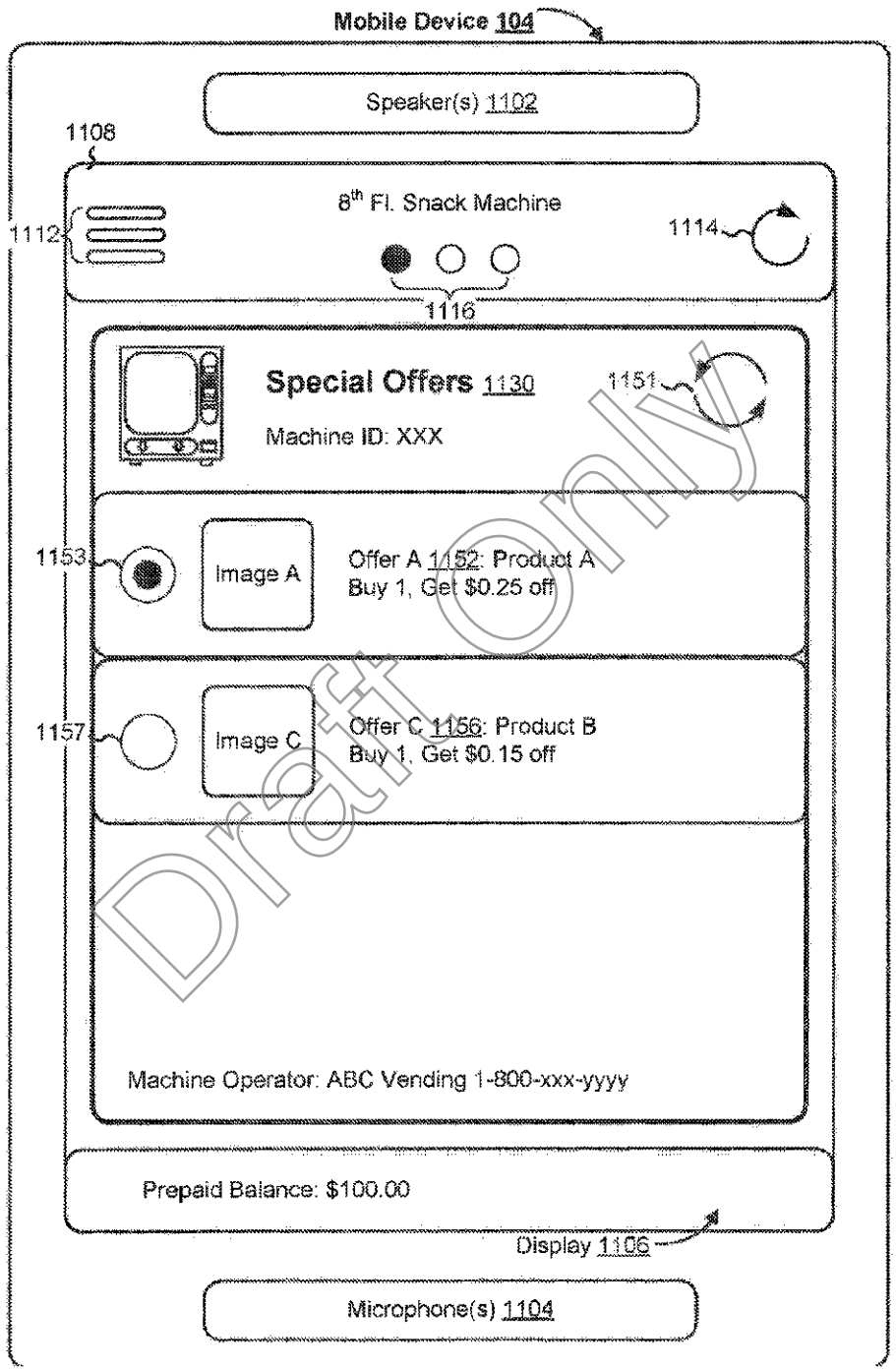
Draft Only


Mobile Device 104
Speaker(s) 1102
1108
8th Fl. Snack Machine
1112
1114
1116
Special Offers 1130
1151
Machine ID: XXX
1153
Image A
Offer A 1152: Product A
Buy 1, Get $0.25 off
1166
Image B
Offer B 1154: Product A
Buy 3, Get 4th free (1 more to go)
1162-b
Delete
1164
1157
Image C
Offer C 1156: Product B
Buy 1, Get $0.15 off
Machine Operator: ABC Vending 1-800-xxx-yyyy
Prepaid Balance: $100.00
Display 1106
Microphone(s) 1104

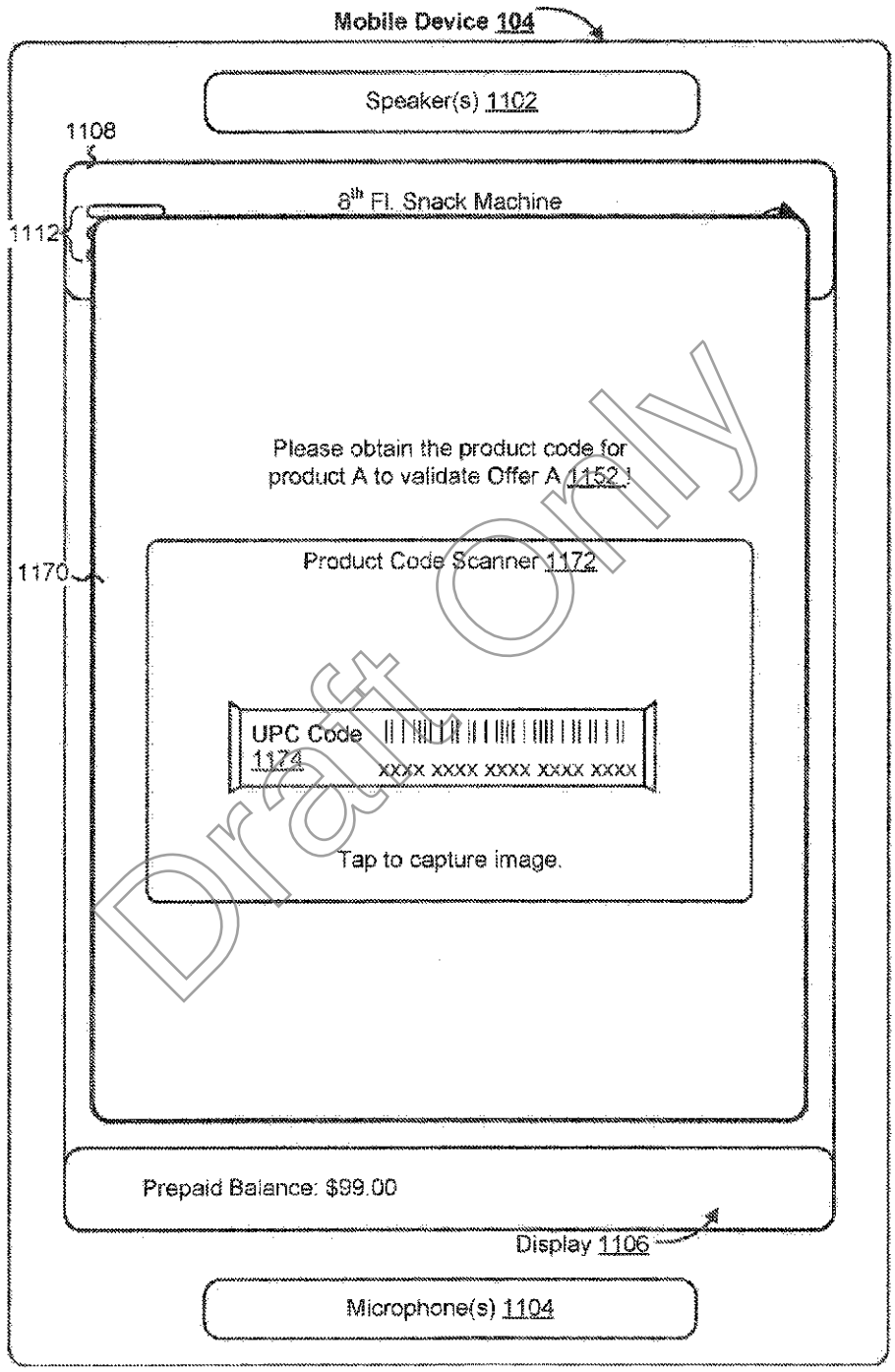
Draft Only


Mobile Device 104
Speaker(s) 1102
1108
8th Fl. Snack Machine
1112
1114
1116
Special Offers 1130
1151
Machine ID: XXX
1168
1153
Image A
Offer A 1152: Product A
Buy 1, Get $0.25 off
1157
Image C
Offer C 1156: Product B
Buy 1, Get $0.15 off
Machine Operator: ABC Vending 1-800-xxx-yyyy
Prepaid Balance: $100.00
Display 1106
Microphone(s) 1104

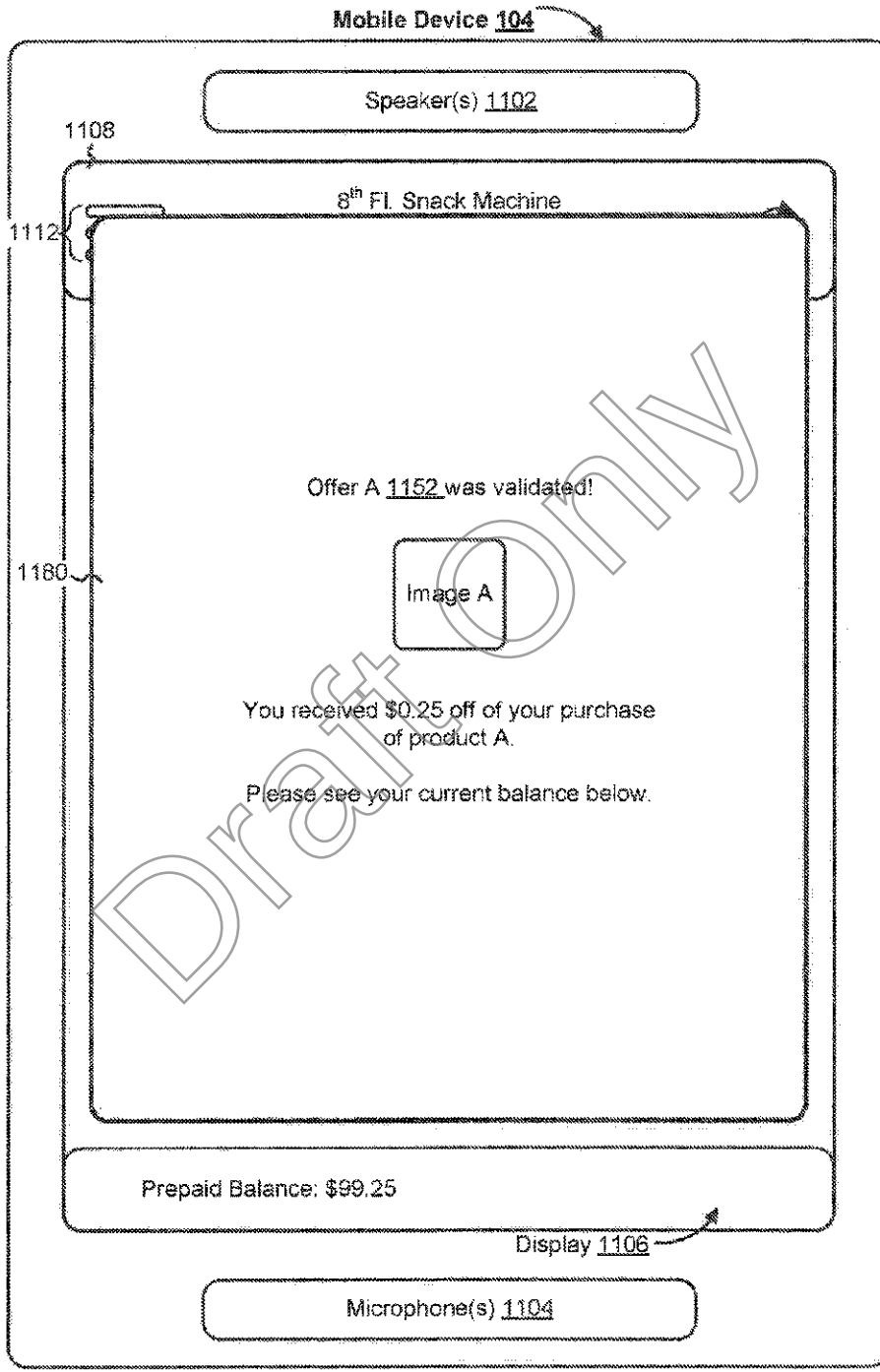
Draft Only


Mobile Device 104
Speaker(s) 1102
1108
8th Fl. Snack Machine
1112
1114
1116
Special Offers 1130
1151
Machine ID: XXX
1153
Image A
Offer A 1152: Product A
Buy 1, Get $0.25 off
1157
Image C
Offer C 1156: Product B
Buy 1, Get $0.15 off
Machine Operator: ABC Vending 1-800-xxx-yyyy
Prepaid Balance: $100.00
Display 1106
Microphone(s) 1104

Draft Only


Mobile Device 104
Speaker(s) 1102
1108
8th Fl. Snack Machine
1112
Please obtain the product code for product A to validate Offer A 1152!
1170
Product Code Scanner 1172
UPC Code 1174
xxxx xxxx xxxx xxxx xxxx
Tap to capture image.
Prepaid Balance: $99.00
Display 1106
Microphone(s) 1104

Draft Only


Mobile Device 104
Speaker(s) 1102
1108
8th Fl. Snack Machine
1112
Offer A 1152 was validated!
1180
Image A
You received $0.25 off of your purchase of product A.
Please see your current balance below.
Prepaid Balance: $99.25
Display 1106
Microphone(s) 1104

Draft Only

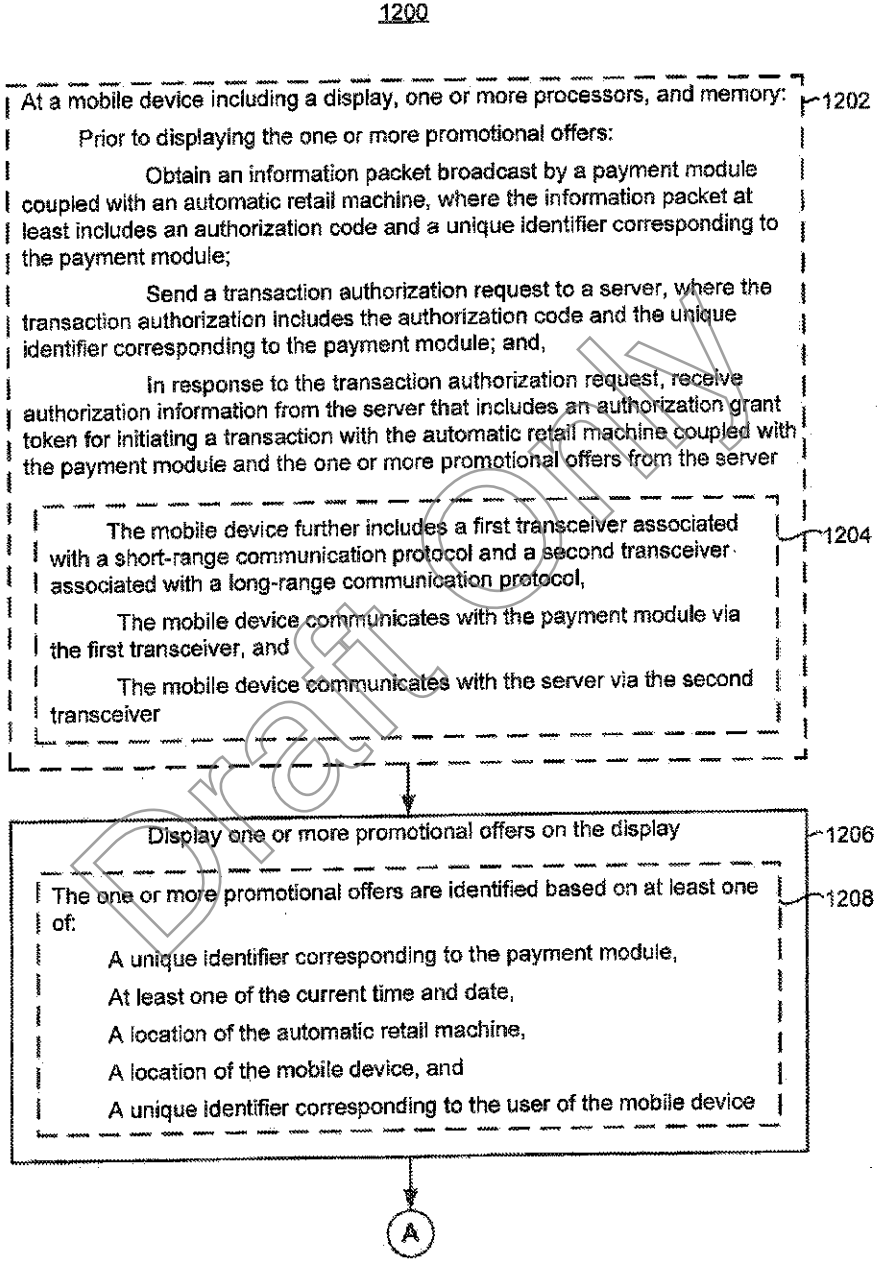
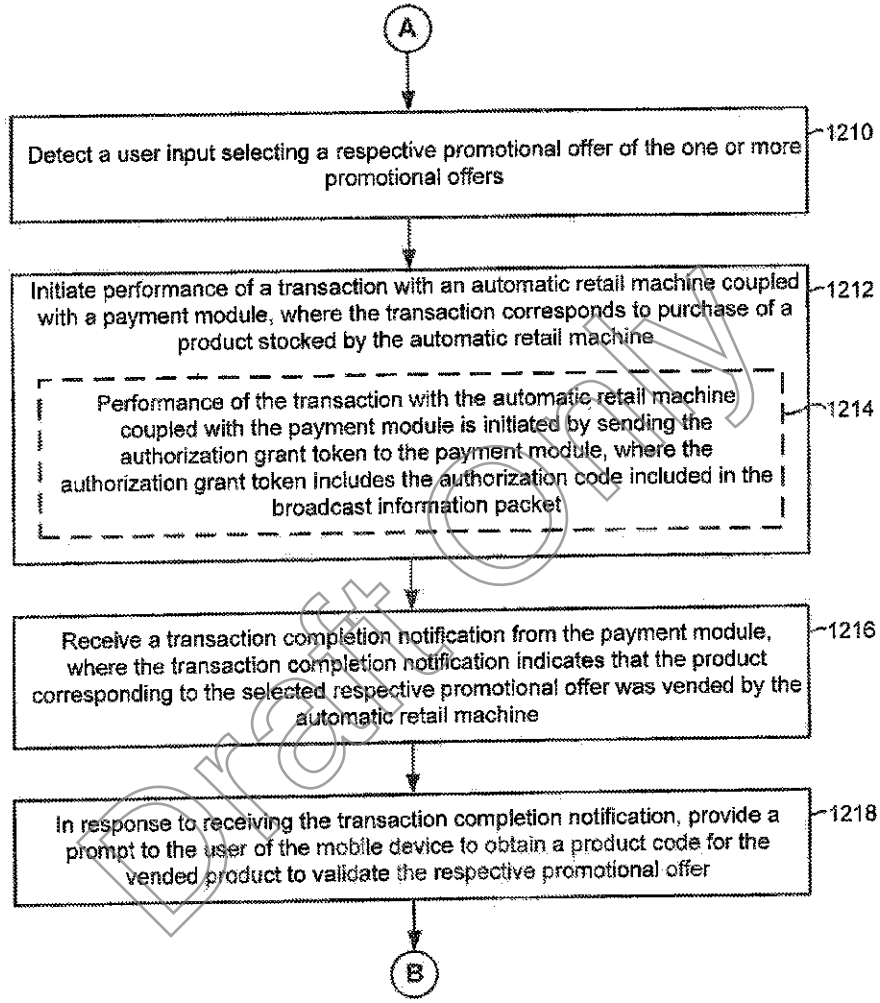


Figure 12A

Draft Only



Draft Only

Figure 12B

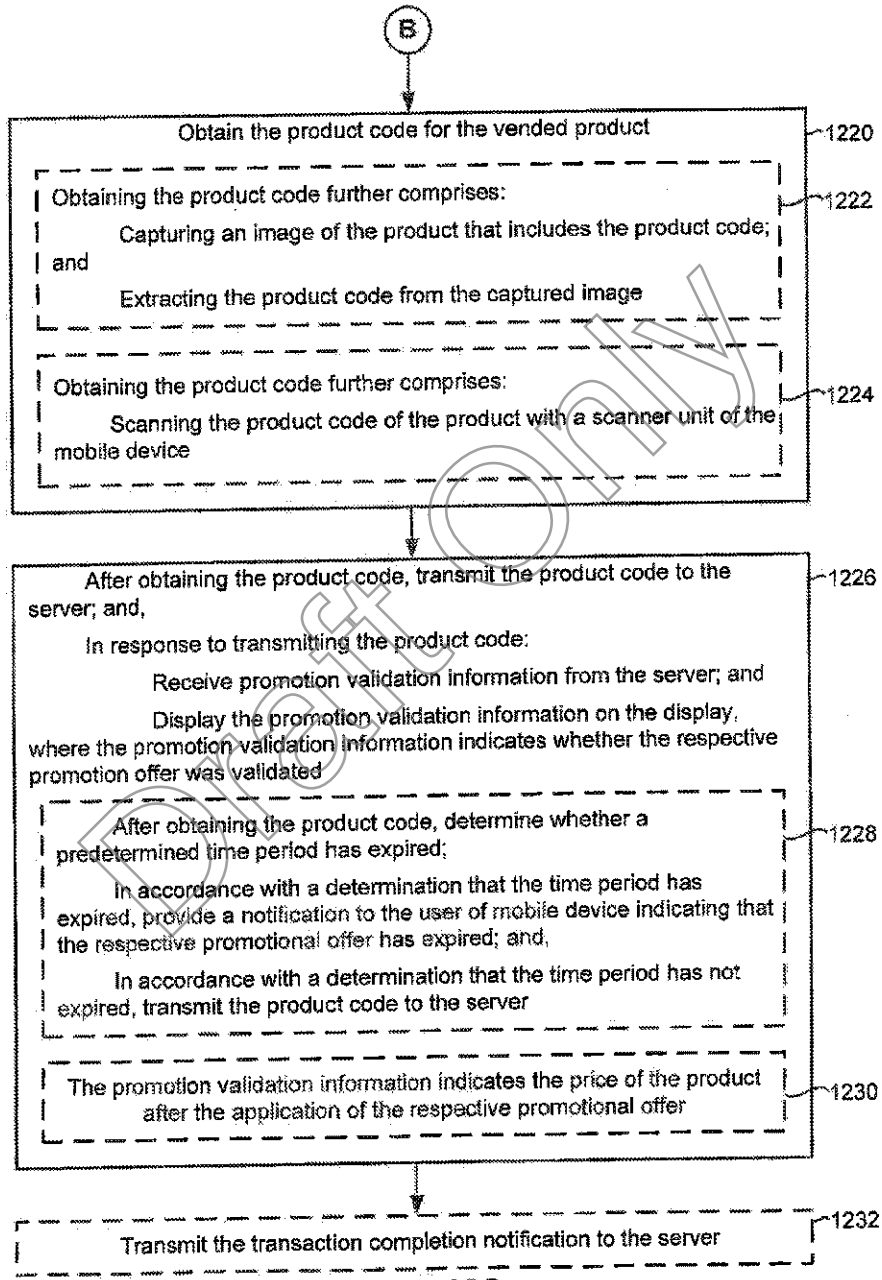


Figure 12C

Draft Only

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/015763

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q30/02 G06Q20/18 G06Q30/06
ADD.

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)
G06Q

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)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 8 856 045 B1 (PATEL PARESH K [US] ET AL) 7 October 2014 (2014-10-07) abstract figure 7 figure 10A figure 10C column 3, line 46 - line 64 column 10, line 38 - line 51 column 12, line 15 - line 51 column 14, line 53 - line 65 column 23, line 17 - line 25 column 28, line 52 - line 67 column 29, line 53 - line 60	1-12
A	US 2014/136301 A1 (VALDES JUAN [US]) 15 May 2014 (2014-05-15) abstract paragraph [0045] - paragraph [0061] paragraph [0062] - paragraph [0067]	1-12

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* 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
30 March 2016	08/04/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040,	Mesma Dajmud

Draft Only

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2016/015763

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 8856045 B1	07-10-2014	US 8856045 B1	07-10-2014
		US 2015170130 A1	18-06-2015
		US 2015227928 A1	13-08-2015
		WO 2015095599 A1	25-06-2015
US 2014136301 A1	15-05-2014	NONE	

Draft Only

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 June 2014 (19.06.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/093857 A1

(51) International Patent Classification:
G06Q 20/20 (2012.01)

(21) International Application Number:
PCT/US2013/075077

(22) International Filing Date:
13 December 2013 (13.12.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/737,409 14 December 2012 (14.12.2012) US

(71) Applicant: **MEI INC.** [US/US]; 3222 Phoenixville Pike, Suite 200, Malvern, PA 19355 (US).

(72) Inventors: **ANDERSON, Thomas**; 422 Brandham Way, Downingtown, PA 19335 (US). **TEDDER, Bradford, Reams**; 2528 Drew Valley Rd, Atlanta, GA 30319 (US). **HADDON, Douglas, Brian**; 3000 Georgetown Road, Cinnaminson, NJ 08077 (US).

(74) Agents: **MIRABITO, Jason, A.** et al.; Mintz Levin Cohn Ferris Glovsky And Popeo, PC., One Financial Center, Boston, MA 02111 (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, BN, BR, BW, BY, BZ, CA, CH, CL, 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, IR, IS, JP, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

[Continued on next page]

(54) Title: POINT OF SALE PLATFORM FOR CONSUMER MEDIA INTERACTION

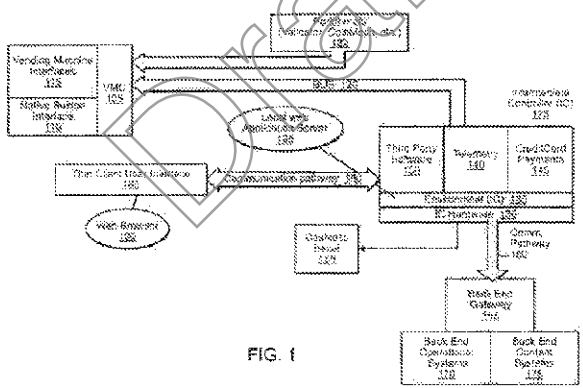


FIG. 1

(57) Abstract: A point of sale system includes a host, an intermediate controller, a user interface device, and one or more peripheral devices. The intermediate controller includes an operating environment and is in communication with the host. The user interface device is associated with and in communication with the intermediate controller. The user interface includes a web browser and the intermediate controller includes a webserver, the webserver hosting one or more applications for interaction with a customer. The one or more peripheral devices are coupled to at least the intermediate controller via a bus. Related apparatus, systems, techniques, and articles are also described.

Draft Copy

WO 2014/093857 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

Draft Only

Point of Sale Platform for Consumer Media Interaction

RELATED APPLICATIONS

[0001] This application claims priority to U.S. Provisional Patent Application No. 61/737409 filed December 14, 2012, the entire contents of which are hereby incorporated by reference herein.

TECHNICAL FIELD

[0002] The subject matter described herein relates, in general, to electronic transaction systems and, in particular, to a dynamic consumer-interactive vending platform.

BACKGROUND

[0003] Electronic transaction systems, such as vending machines, typically utilize Digital Exchange (DEX) and Multi-Drop Bus (MDB) protocols. A DEX file is an electronic audit file having information such as sales, cash in bill validators, pricing, etc. A vending machine controller (VMC) generally stores the information on a timely basis and transmits it in DEX format as a DEX file as and when requested. MDB can provide an interface between the vending machine and different peripheral devices, such as coin acceptors, bill acceptors, credit-card acceptors, etc. Additionally, the VMC can recognize and enable the peripheral devices for operation, after which the device and the VMC can communicate. The communication enables components of the system to work in concert to perform the functions of the vending machine, such as accepting payment, vending product, logging transactions, and transmitting transactional information to an external server.

[0004] However, conventional vending machines pre-configure to work with a specific set of peripheral devices and require replacement to support additional devices. Thus,

Draft Only

CSC ServiceWorks - Ex. 1002
Page 965 of 1551

the VMC is an integrated component that supports a specific set of functionalities and may require cost consuming replacements or extensions to offer additional functionalities. As an example, conventional VMC's only enable the following operations: receive a vending request; accept cash or credit to process the request; and process the vending request after receiving the intended amount. Furthermore, consumer interaction is limited to a static set of interface components, typically buttons. Prior attempts to expand vending machine functionality focuses on configuration changes with the VMC, thereby suggesting and requiring replacement of the VMC. However, replacing the VMC can be cost-prohibitive and undesirable.

SUMMARY

[0005] In one aspect, a point of sale system includes a host, an intermediate controller, a user interface device, and one or more peripheral devices. The intermediate controller includes an operating environment and is in communication with the host. The user interface device is associated with and in communication with the intermediate controller. The one or more peripheral devices are coupled to at least the intermediate controller via a bus.

[0006] The intermediate controller can be an embedded personal computer control board. The intermediate controller operating environment can include an operating system and file system. The intermediate controller can receive data from a remote server. The user interface device and intermediate controller can be coupled via an Ethernet communication connection.

[0007] The intermediate controller can further include a telemetry module to configure alarms and notifications for instances such as door open, jammed item, temperature control, etc. The intermediate controller can further include one or more application modules, for example third party software applications. Further, at least one application module can be

Draft Only

CSC ServiceWorks - Ex. 1002
Page 966 of 1551

accessed by the user interface device. The application modules can support additional and enhanced functionalities. For example, the intermediate controller can include an application module, e.g. a web server module, to run a web browser on the user interface device. The user interface device thus hosts one or more applications for interaction with a customer. Furthermore, in one implementation, the web server module can be associated with a remoter server via a network (not shown). In this configuration, the web server module requests information pertaining to the customer, such as customer profiles, loyalty information, rewards, coupons, discounts, etc., and displays the information on the user interface device. The user can make further selections on the user interface module through the web browser, thus allowing the user to dynamically interact with the point of sale system. The web server can be HTTP compliant and the web server can be an HTTP application server.

[0008] In another example, the application module can include a multiple vend selection module, which supports the selections and vending of multiple items in a single transaction. In yet another example, the application module is a monitoring module configured to monitor and record details of the point of sale systems that request a specific application module. The application modules can also be associated with license numbers making it easier to track the updates and installations.

[0009] In one implementation, the application module can be a diet information module configured to store nutritional information for each of the vend items. Additionally or optionally, the diet information module may have access to the inventory and specific information on items. Further, the diet information module stores the selections made by the customer in each transaction with the nutritional information. The diet information module can provide suggestions and recommendations based on the customer purchasing history.

[0010] The point of sale system can further include a cashless bezel coupled to the intermediate controller. The intermediate controller can further include a cashless module for

Draft Only

CSC ServiceWorks - Ex. 1002
Page 967 of 1551

enabling cashless transactions. The bus, communicatively coupled with the intermediate controller and the host, can be a multi-drop data bus (MDB). Additionally, the peripheral devices can be communicatively coupled, directly or indirectly, to the host and the intermediate controller via the bus. The host can be a vending machine controller (VMC). The VMC can include a vending machine interface and one or more native button interfaces. Conventionally, the VMC is designed to be the master controller that controls all the peripheral devices through the bus. However, in one embodiment, the intermediate controller is assigned the peer role by controlling the application modules and/or peripheral devices and translating instructions into a language understood by the VMC. In another embodiment, the intermediate controller controls one or more peripheral devices through the bus, except the peripheral devices that are hardwired to the VMC. In this manner, the "master" role switches between the intermediate controller and the VMC based on the functionality.

[0011] In another aspect, a point of sale system includes a host, an intermediate controller, a user interface and one or more peripheral devices. The intermediate controller is in communication with the host and includes one or more third party applications utilizing an application interface to control components of the point of sale system according to predefined functions. The user interface device is associated with and in communication with the intermediate controller. The one or more peripheral devices are coupled to at least the intermediate controller via a bus.

[0012] In another aspect, a point of sale system includes an intermediate controller including an operating environment, a user interface device and one or more peripheral devices coupled to at least the intermediate controller via a bus. The user interface is associated with and in communication with the intermediate controller. The user interface includes a web browser and the intermediate controller includes a webserver, the webserver hosting one or more applications for interaction with a customer.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 968 of 1551

[0013] One or more of the following features can be included. For example, the components of the point of sale system can include one or more of mechanical, electrical, or software components. The components of the point of sale system can include one or more of the peripheral devices coupled to the intermediate controller. The components of the point of sale system can include the host. The components of the point of sale system can include the user interface device. A telemetry unit can be included and can be in communication with a remote licensing server. The user interface can include a web browser and the intermediate controller can include a webserver, the webserver hosting one or more of the third party applications for interaction with a customer. The one or more third party applications can have been installed on the point of sale system using a remote back end server to select the one or more third party applications for installation. The point of sale system can be in communication with a host remote from the point of sale system.

[0014] Computer program products are also described that comprise non-transitory computer readable media storing instructions, which when executed by at least one data processors of one or more computing systems, causes at least one data processor to perform operations herein. Similarly, computer systems are also described that may include one or more data processors and a memory coupled to the one or more data processors. The memory may temporarily or permanently store instructions that cause at least one processor to perform one or more of the operations described herein. In addition, methods can be implemented by one or more data processors either within a single computing system or distributed among two or more computing systems.

[0015] The subject matter described herein provides many advantages. For example, a customer's purchasing history can be tracked and they can be rewarded according to pre-defined rules. Using the current subject matter, a customer can dynamically interact with the point of sale machine creating a unique and individualized consumer experience.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 969 of 1551

The subject matter described herein can be implemented in existing point of sale machines in a cost-effective manner with minimal software and hardware modifications. In other words, the current subject matter enables an inexpensive retrofit of existing vending machines that does not require replacement of the VMC. Further, the current subject matter can integrate into existing machines and the capabilities are modular and can be expanded based upon need. This allows retrofit integration across many different and often disparate technologies, which many prior integrated solutions do not provide.

[0016] The current subject matter enables a point-of-sale machine to support advanced media functionality, for example social media interactivity, targeted advertisement, and personalized point-of-sale machine experience.

[0017] The details of one or more variations of the subject matter described herein are set forth in the accompanying drawings and the description below. Other features and advantages of the subject matter described herein will be apparent from the description and drawings, and from the claims.

DESCRIPTION OF DRAWINGS

[0018] FIG. 1 is a system block diagram illustrating components of an example embodiment of a point of sale machine, including an intermediate controller;

[0019] FIG. 2 is a system block diagram illustrating components of another example embodiment of a point of sale machine, including intermediate controller;

[0020] FIG. 3 is a block diagram illustrating the layers of an example operating system in an exemplary intermediate controller environment;

[0021] FIG. 4 is a block diagram illustrating the application module controlling loyalty information of customers, according to an embodiment of the present subject matter; and

Draft Only

CSC ServiceWorks - Ex. 1002
Page 970 of 1551

[0022] FIG.5 is a block diagram illustrating the sharing of the bus between the intermediate controller and the VMC according to an embodiment of the present subject matter.

[0023] Like reference symbols in the various drawings indicate like elements.

DETAILED DESCRIPTION

[0024] The current subject matter described herein supports additional functionalities to a point of sale system. In one implementation, the additional functionalities can be provided as a retrofit solution with little or no hardware modifications. Examples of point of sale systems include, but are not limited to, a vending machine, gaming machines, automated teller machines, banking machines, kiosks, bill pay machines, or any other host machine configured to accept payment in exchange for products and/or services. Such systems can dynamically interact with a variety of peripheral devices and provide additional functionalities. Additional functionalities include providing advertising, loyalty rewards, discounts, coupons, multiple vend items, social media interaction, mobile device or mobile wallet interaction, etc. Further, the point of sale machine can support dynamic engagement through a user interface, for example a touch screen. Existing point of service machines can be retrofit with the current subject matter, which will reduce cost associated with replacing an entire system. In addition, the device is configured to dynamically track and control software licenses and updates by interacting with a back end server or remote server or enterprise controller.

[0025] FIG. 1 is a block diagram illustrating components of an example embodiment of a point of sale system 100. In this embodiment, a VMC 105 is coupled to native button user interfaces 110 and other vending machine interfaces 115. The VMC 105 can connect via a bus 120 to a number of optional peripherals 125. The bus 120 can include an MDB bus or other suitable communications pathway such as Executive, BDV,

Draft Only

CSC ServiceWorks - Ex. 1002
Page 971 of 1551

micromech, cctalk, and Electromechanical. The optional peripherals 125 are peripherals that enable vending machine functionality. For example, a bill validator and coin validator are optional peripherals 122. Example bill validators and coin validators can include those described in, e.g., U.S. Patent No. 6,390,269, the content of which is expressly incorporated by reference, in its entirety.

[0026] The VMC 105 also connects via bus 120 to an intermediate controller (IC) 125. The IC 125 is an embedded computing platform with unique hardware architecture and software framework that provides for flexible, expandable, and dynamic point of sale functionality. In one embodiment, the IC 125 is an embedded PC control board that provides multi-purpose hardware architecture, operating system, run time environments, with expandable hardware and software capability, and further includes industry standard interfaces. The IC 125 is connected via a communications pathway 180 to a thin client user interface 185. In one embodiment, the communications pathway 180 can be hardwired, such as an Ethernet, serial, USB, or similar connection. The thin client user interface 185 can be a standalone computing device that includes at least a graphical display that presents to a customer. The thin client interface 185 can include a display system that can function as a medium of consumer input (e.g., the display system can be an LCD touch screen). In general, the thin client user interface 185 provides access to applications running on the IC 125. In one embodiment, the thin client user interface 185 includes a web browser 190 that operates as a client in a client-server relationship with a web server 195 running on the IC environment 135 of the IC 125. Communication can occur between the thin client user interface 185 and the IC 125 through TCP/UDP protocol. In this embodiment, web server 195 is capable of serving graphics, media, video, audio and any other MIME type (i.e. standard content format under HTML standards) to the thin client user interface 185.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 972 of 1551

[0027] The IC 125 includes IC hardware 130 (e.g., an embedded PC control board) supporting an IC environment 135 (e.g., an operating system, file system, runtime environments, and other associated software applications). Optionally, the IC 125 can be powered via the bus 120. The IC 125 can also include a telemetry 140 module, a credit card payment 145 module, and third party software 150. The telemetry 140 module allows the point of sale machine to communicate with a back end or remote server, such as gateway 165. The telemetry 140 module provides for exchange of transactional and/or operational information (e.g., logging/audit, inventory information, etc.) between the point of sale machine and any backend services as well as deployment of software upgrades and additions to the point of sale machine. The telemetry 140 module can include dedicated communications hardware and associated software (e.g., for cellular, WiMax, WAN, LAN, etc.).

[0028] The credit card payment 145 module provides support for and controls a cashless bezel 155. The cashless bezel 155 is linked to the IC 125 and accepts credit card information through, e.g., magnetic swipe, contactless, chip card, IC Card, smartcard, EMV, and RFID tag interfaces. From the perspective of the VMC 105, the cashless bezel 155 is a cascaded peripheral that is controlled by the IC 125, but ultimately transactions that include the cashless bezel 155 will result in the IC 125 sending a credit message to the VMC to enable the transaction. The cashless bezel 155 can include those described in, e.g., U.S. Patent No. 8,157,167, the contents of which is herein expressly incorporated by reference, in its entirety.

[0029] The IC 125 is connected via a communications pathway 160 (e.g., a wireless APN utilizing cellular technology or other suitable mode of communications) to a backend gateway 165. The backend gateway 165 includes backend operational systems 170 and backend content systems 175. In addition to supporting credit transaction, the back end

Draft Only

gateway 165 can provide access for third parties to communicate with the point of sale machine (possibly to the third party software they have installed). In one example use, a customer can swipe a rewards or loyalty card and the IC 125 can communicate with a third party server to determine and/or receive information regarding the customer's loyalty account including any discounts, credits, or free purchases that the customer may be entitled to.

[0030] Additionally, the IC 125 may be allowed access to customer preferences and profiles stored on the third party server. The IC 125 then enables the thin client user interface 185 to support advanced media functionality, for example social media interactivity, targeted advertisement, personalization of a customer transaction experience, and e-commerce like customer experiences. In some embodiments, the thin client user interface 185 can be configured to display still images, stored video files, dynamic content and interactive content to a user. The current subject matter provides a rich consumer media and social networking experience. Further, the user may utilize multiple payment methods to make a purchase at the point of sale machine.

[0031] The IC 125, upon validating a coupon, rewards club benefit, or other discount, can send a message to the VMC 105 to add a credit for the benefit amount. Thus, from the VMC's 105 perspective, the IC 125 is another peripheral 122 such as a coin mechanism that is accepting payment from the customer and providing a credit notice to the VMC 105. Since the IC 125 can host third party software 150, the third party software 150 can instruct the IC 125 to send a credit message to the VMC 105 for a broad range of reasons, as desired by the third party software.

[0032] In one embodiment, the VMC 105 is designated as the master controller, which controls peripheral devices including optional peripherals 122 and IC 125 through the bus 120. However, in another embodiment as shown in FIG. 2, the optional peripherals 122 cascade from the IC 125. In this configuration, the IC 125 intercepts normal communication

Draft Only

CSC ServiceWorks - Ex. 1002
Page 974 of 1551

between the VMC 105 and optional peripherals 122 and acts as a master controller and instructs or tricks the VMC 105 with respect to newly defined functionalities; with the exception of vend requests. The IC 125 can "trick" the VMC into performing desired operations that the VMC is not designed to handle. For example, a customer could input a rewards club loyalty identification, coin, and bill value and the IC 125 could, in order to provide a discount, send the VMC 105 a message indicating a total credit input by the customer, even though the customer has not input sufficient funds (but in fact is receiving a discount). In this configuration, the VMC 105 continues to handle vend requests.

[0033] In another embodiment, with reference again to FIG. 1, the intermediate controller 125 acts as a peer to the VMC 105 rather than a master and peripheral configuration. In this embodiment, the IC 125 can query the VMC 105 and transmit a message that there is credit. In this case, the IC 125 translates the additional functionalities into vend requests, which can then be interpreted by the VMC 105 as legitimate requests with credit.

[0034] In another embodiment, the IC 125 and VMC 105 may work in a "shared environment," that is, sharing functionalities. The VMC 105 can be configured to support at least a portion of newly defined functionalities. Thus, the "master" role is dynamic and switches between IC 125 and the VMC 105 based on a given functionality.

[0035] Functionalities supported include, but are not limited to: Multi Vend Selection (e.g. selection of multiple products or services within a single transaction), Discounts, Coupons, Advertisements, Recommendations/Suggestions based on customer profiling, Tracking and controlling software updates/licenses, other customer engagement. Examples of vending protocols include: Executive, MDB, BDV, Electromechanical.

[0036] Additionally or optionally, the gateway 165 may be associated with a monitoring module (not shown) within the IC 125. The gateway 165 interacts with a

Draft Only

CSC ServiceWorks - Ex. 1002
Page 975 of 1551

monitoring server designed to control the licenses downloaded on the point of sale machines coupled to the gateway 165. Such information is passed onto the monitoring module via the gateway 165. Thus, the monitoring module tracks software updates on the point of sale machines. This, in turn, helps in better management and handling of application modules stored on the point of sale machines.

[0037] The IC 125 provides for flexible expansion. For example, in one embodiment, a basic embedded computing platform can expand by adding to or improving the computing device (e.g., memory, hard drive, CPU, connectors, power supply, other third party removable component), onboard machine interfaces (e.g., USB 2.0, USB 3.0, MDB, EXEC, VCCS, Serial), expansion card (e.g., WAN Modem, CDMA, Ethernet, Bluetooth, Wifi, Memory Card, SD Card, Graphics Card, Secure Storage Card, Audio Card), software infrastructure (e.g., advanced data collection, distributed computing interfaces, VDI or other Data Exchange, VPN, DNS Utilization, Web/Application Server, Python, etc.), and any software application (e.g. a third party application).

[0038] Application Programming Interfaces (API) remove the need for point-of-sale machine specific designs thereby supporting and promoting development and use of third party applications that improve or control point-of-sale machine functionality. A standard interface (to mechanical, electrical, or software components of the point-of-sale machine) allows a third party (as distinguished from the original equipment manufacturer (OEM)) to create a third party application to utilize the point-of-sale machine (and, e.g., components thereof, including the IC 125, host, thin client user interface 185, and peripherals 122) according to pre-defined functions. For example, a web service interface that implements a device to server VDI standard can allow a third party to leverage the web service in developing a third party application.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 976 of 1551

[0039] For a given point-of-sale machine, a machine manager can access a defined set of available services and interfaces. This allows third party components (e.g., mechanical, electrical, and/or software) to operate within the boundaries of that point-of-sale machine. The effect is a flexible point-of-sale machine that a manager can tailor to a specific use (e.g., for selling a specific product, selling a product in a specific region or country, etc.). For example, a third party application can deploy on the IC 125 and operate alongside the telemetry 140 module to provide enhanced capabilities for tracking consumer purchasing behavior or enhanced advertisement capability.

[0040] Third party software distribution can be managed by a library of existing and available third party or OEM software components. A point-of-sale machine manager can view the application through, for example, a web application on the back end, and select the software that the manager would like installed on the point-of-sale machine. The point-of-sale machine can download an upgrade package from a backend server and install or update the software. Licensing and version control can be applied on a point-of-sale machine level, and point-of-sale managers are able to customize their machines.

[0041] Using the current subject matter, a customer can, for example, present a form of identification (e.g., credit card or loyalty club rewards card) to the point of sale machine. The point of sale machine can then remotely access a backend or remote server that includes information specific to that customer and download preferences, targeted advertisements, account information (e.g. point balances), and other individualized information and present the information to the customer via a display device. The information can be dynamic and does not need to be stored locally at the point of sale machine. The customer can interact with the dynamic information in order to complete a transaction. Such functionality of the point of service machine can be controlled, upgraded, changed, etc.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 977 of 1551

through use of applications (third party or OEM). The functionality can be modified remotely, without having to install new hardware or have a technician service the machine.

[0042] FIG. 3 is a block diagram illustrating the layers of an example operating system in an IC environment 135.

[0043] A point of service machine that includes an intermediate device 125 and thin user client 185 can present advertisements or other media. For example, the machine can be in an idle state and display one set of advertisements (e.g., static images or video). When a customer initiates a transaction, the machine can accept or determine identification of the customer. The IC 125 can then download targeted advertisement or other information for display by the thin client user interface 185.

[0044] The current subject matter can enable a point of sale machine, more specifically, a vending machine, to perform multiple vend operations using a single payment through say the multi product vend module (not shown). As an example, a customer can swipe a credit card. The IC 125 can validate the credit card for a predetermined amount (e.g., enough for three vends of product). The IC 125 can send three separate credit messages to the VMC 105 to enable a multi-vend procedure. For example, a customer swipes a credit card, authorization is performed, the VMC 105 is informed by the IC 125 that credit sufficient for a single product vend has been input, the customer selects the product using the native button interface 110, the VMC is again informed by the IC 125 that credit sufficient for a single product vend has been input (without additional customer input), and the customer can select the desired product using the native button interface 110. This process can be repeated for any number of vends (i.e., a multi-vend). Further, the MDB driver, shown in IC 125, allows the application modules to interact with the bus 120. In essence, the MDB driver acts as a translator between the application modules and the bus 120, ensuring that the protocol is followed. The IC 125 may also include a modem (not shown) to display content on external

Draft Only

CSC ServiceWorks - Ex. 1002
Page 978 of 1551

devices such as cellular phones via cellular network or any other network know in the art. Thus, in one implementation, a user may receive nutritional information or balance information on his cell phone.

[0045] FIG. 4 is a block diagram illustrating the application module controlling loyalty information of customers, according to an embodiment of the present subject matter. Loyalty information can be stored on a loyalty system in the back-end system. A S1 Gateway can interface with the loyalty system and provide consumer loyalty information to the controller. The controller can act as a bridge between the Bezel and the Gateway and can control a transaction.

[0046] FIG.5 is a block diagram illustrating the sharing of the bus between the intermediate controller and the VMC according to an embodiment of the present subject matter. The intermediate controller (or ASK) can provide credit amount from cash and the credit available to the thin client interface. When a consumer is ready to check out, the intermediate controller can cause a vend to occur without having further consumer interaction.

[0047] Various implementations of the subject matter described herein may be realized in digital electronic circuitry, integrated circuitry, specially designed ASICs (application specific integrated circuits), computer hardware, firmware, software, and/or combinations thereof. These various implementations may include implementation in one or more computer programs that are executable and/or interpretable on a programmable system including at least one programmable processor, which may be special or general purpose, coupled to receive data and instructions from, and to transmit data and instructions to, a storage system, at least one input device, and at least one output device.

[0048] These computer programs (also known as programs, software, software applications or code) include machine instructions for a programmable processor, and may be

Draft Only

CSC ServiceWorks - Ex. 1002
Page 979 of 1551

implemented in a high-level procedural and/or object-oriented programming language, and/or in assembly/machine language. As used herein, the term "machine-readable medium" refers to any computer program product, apparatus and/or device (e.g., magnetic discs, optical disks, memory, Programmable Logic Devices (PLDs)) used to provide machine instructions and/or data to a programmable processor, including a machine-readable medium that receives machine instructions as a machine-readable signal. The term "machine-readable signal" refers to any signal used to provide machine instructions and/or data to a programmable processor.

[0049] To provide for interaction with a user, the subject matter described herein may be implemented on a computer having a display device (e.g., a CRT (cathode ray tube) or LCD (liquid crystal display) monitor) for displaying information to the user and a keyboard and a pointing device (e.g., a mouse or a trackball) by which the user may provide input to the computer. Other kinds of devices may be used to provide for interaction with a user as well; for example, feedback provided to the user may be any form of sensory feedback (e.g., visual feedback, auditory feedback, or tactile feedback); and input from the user may be received in any form, including acoustic, speech, or tactile input.

[0050] Although a few variations have been described in detail above, other modifications are possible. For example, the logic flow depicted in the accompanying figures and described herein do not require the particular order shown, or sequential order, to achieve desirable results. Other embodiments may be within the scope of the following claims.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 980 of 1551

WHAT IS CLAIMED IS:

1. A point of sale system comprising:

a host;

an intermediate controller including an operating environment and in communication with the host;

a user interface device associated with and in communication with the intermediate controller, wherein the user interface includes a web browser and the intermediate controller includes a webserver, the webserver hosting one or more applications for interaction with a customer; and

one or more peripheral devices coupled to at least the intermediate controller via a bus.

2. The point of sale system of claim 1, wherein the web browser is HTTP and the webserver is an HTTP application server.

3. The point of sale system of claim 1, wherein the intermediate controller further includes a telemetry module.

4. The point of sale system of claim 1, wherein the intermediate controller further includes a cashless module.

5. The point of sale system of claim 1, wherein the intermediate controller further includes one or more third party software applications.

6. The point of sale system of claim 5, wherein the third party software applications are accessible by the user interface device.

7. The point of sale system of claim 1, wherein the bus is a multi-drop data bus (MDB).

8. The point of sale system of claim 1, wherein the host is a vending machine controller (VMC) or a PC control board.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 981 of 1551

9. The point of sale system of claim 1, further comprising a cashless bezel coupled to the intermediate controller and wherein the intermediate controller further includes a cashless module for enabling cashless transactions.

10. The point of sale system of claim 1, wherein the intermediate controller is an embedded personal computer control board.

11. The point of sale system of claim 1, wherein the intermediate controller operating environment includes an operating system and file system.

12. The point of sale system of claim 1, wherein the user interface device and intermediate controller are coupled via an Ethernet communication connection.

13. A point of sale system comprising:

a host;

an intermediate controller in communication with the host and including one or more third party applications utilizing an application interface to control components of the point of sale system according to predefined functions;

a user interface device associated with and in communication with the intermediate controller; and

one or more peripheral devices coupled to at least the intermediate controller.

14. The system of claim 13, wherein the components of the point of sale system include one or more of mechanical, electrical, or software components.

15. The system of claim 13, wherein the components of the point of sale system includes one or more of the peripheral devices coupled to the intermediate controller via a bus.

16. The system of claim 13, wherein the components of the point of sale system includes the host.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 982 of 1551

17. The system of claim 13, wherein the components of the point of sale system includes the user interface device.

18. The system of claim 13 further comprising a telemetry unit in communication with a remote licensing server.

19. The system of claim 13, wherein the user interface includes a web browser and the intermediate controller includes a webserver, the webserver hosting one or more of the third party applications for interaction with a customer.

20. The system of claim 13, further comprising a telemetry unit and wherein the one or more third party applications have been installed on the point of sale system using a remote back end server to select the one or more third party applications for installation.

21. A point of sale system comprising:

an intermediate controller including an operating environment;

a user interface device associated with and in communication with the intermediate controller, wherein the user interface includes a web browser and the intermediate controller includes a webserver, the webserver hosting one or more applications for interaction with a customer; and

one or more peripheral devices coupled to at least the intermediate controller via a bus.

22. The point of sale system of claim 21, wherein the point of sale system is in communication with a host remote from the point of sale system.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 983 of 1551

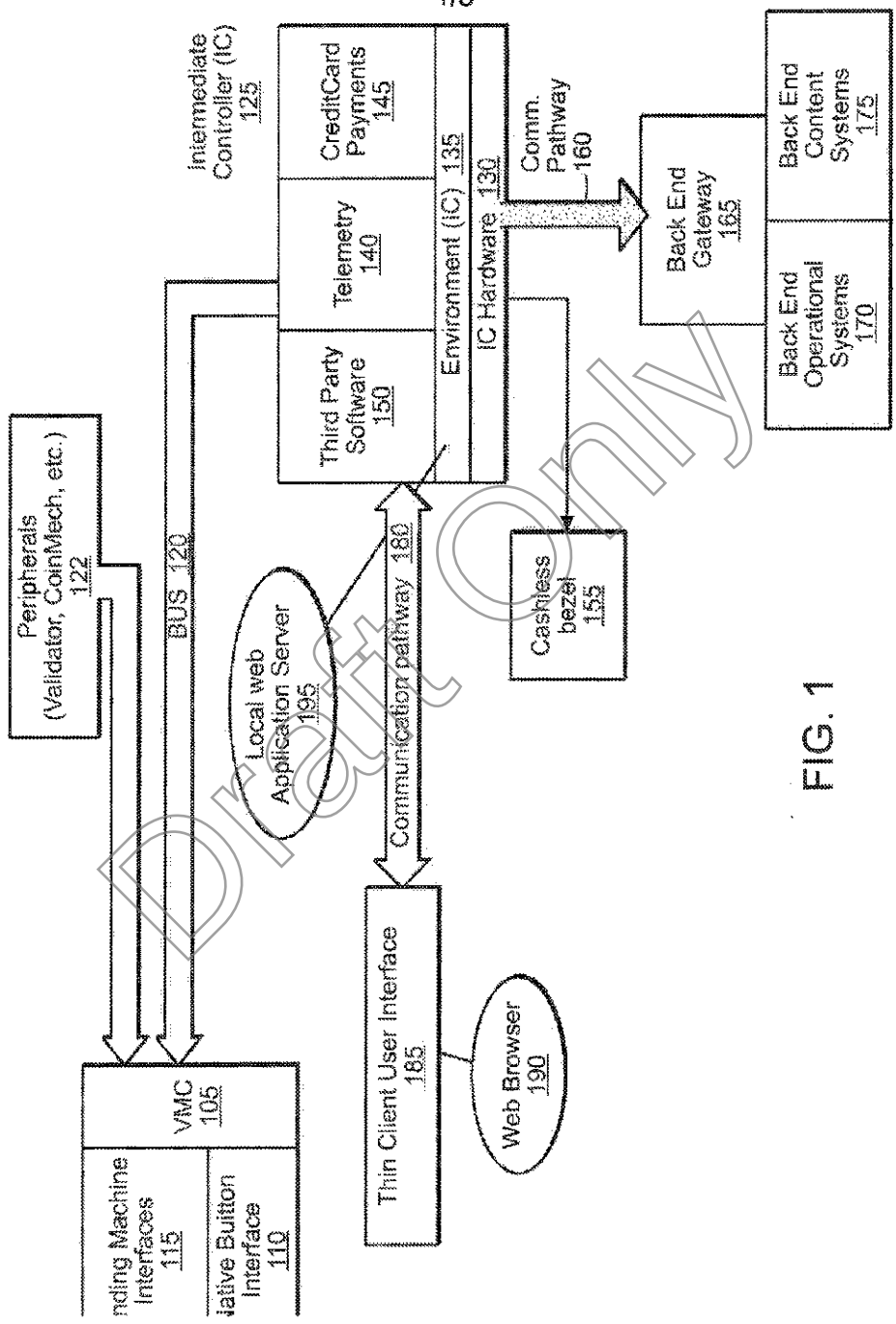


FIG. 1

Draft Only

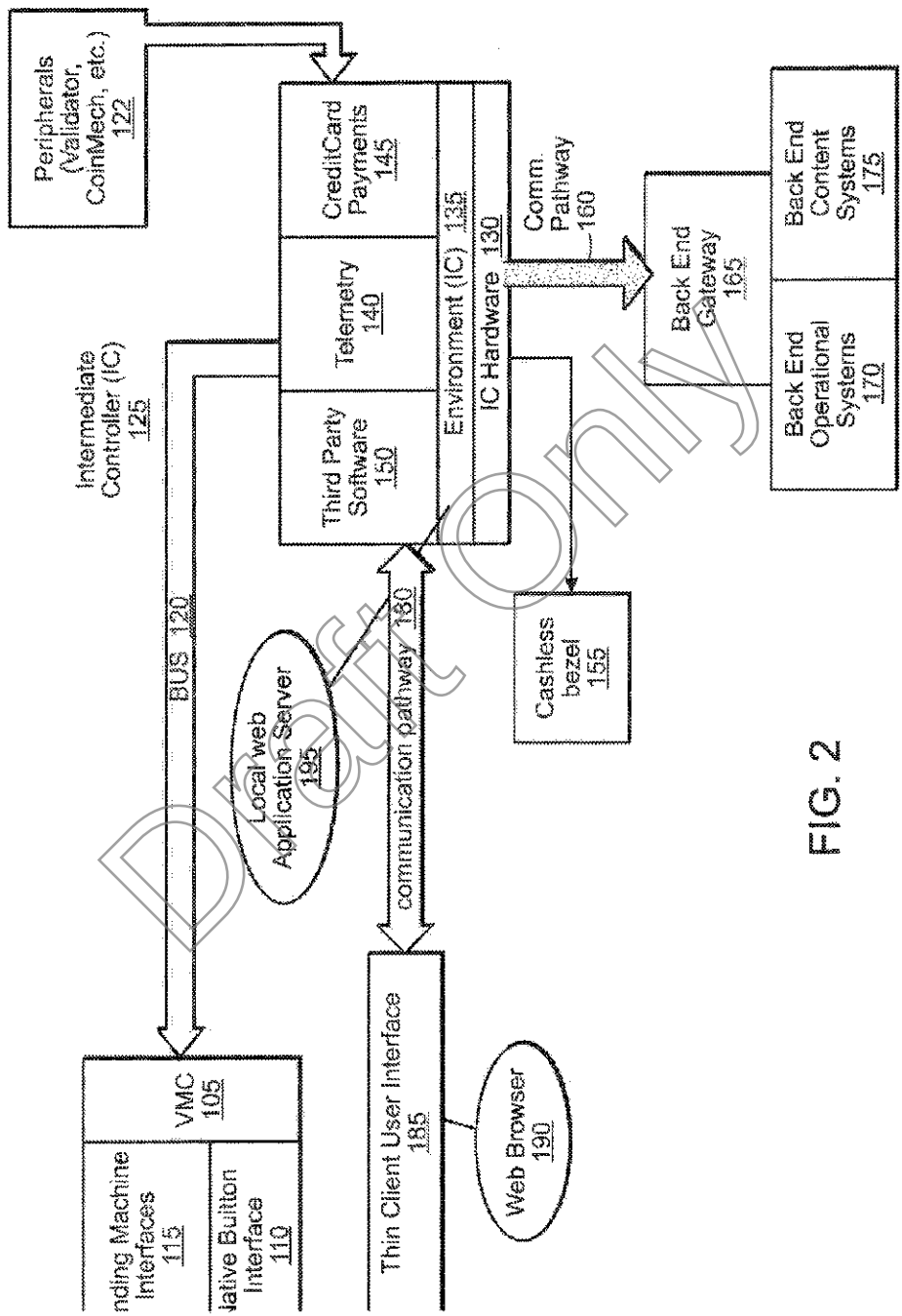


FIG. 2

Draft Only

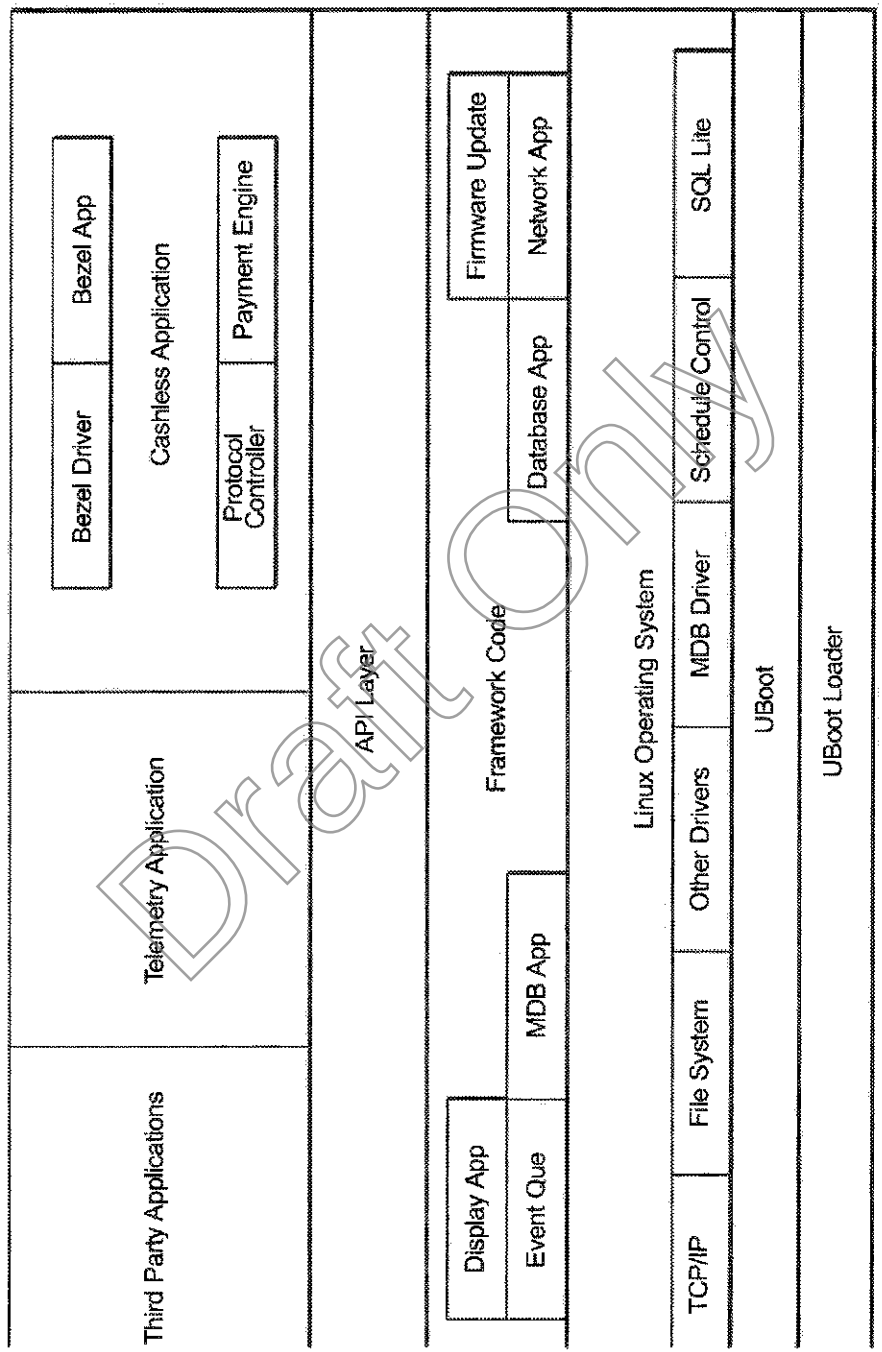


FIG. 3

Draft Only

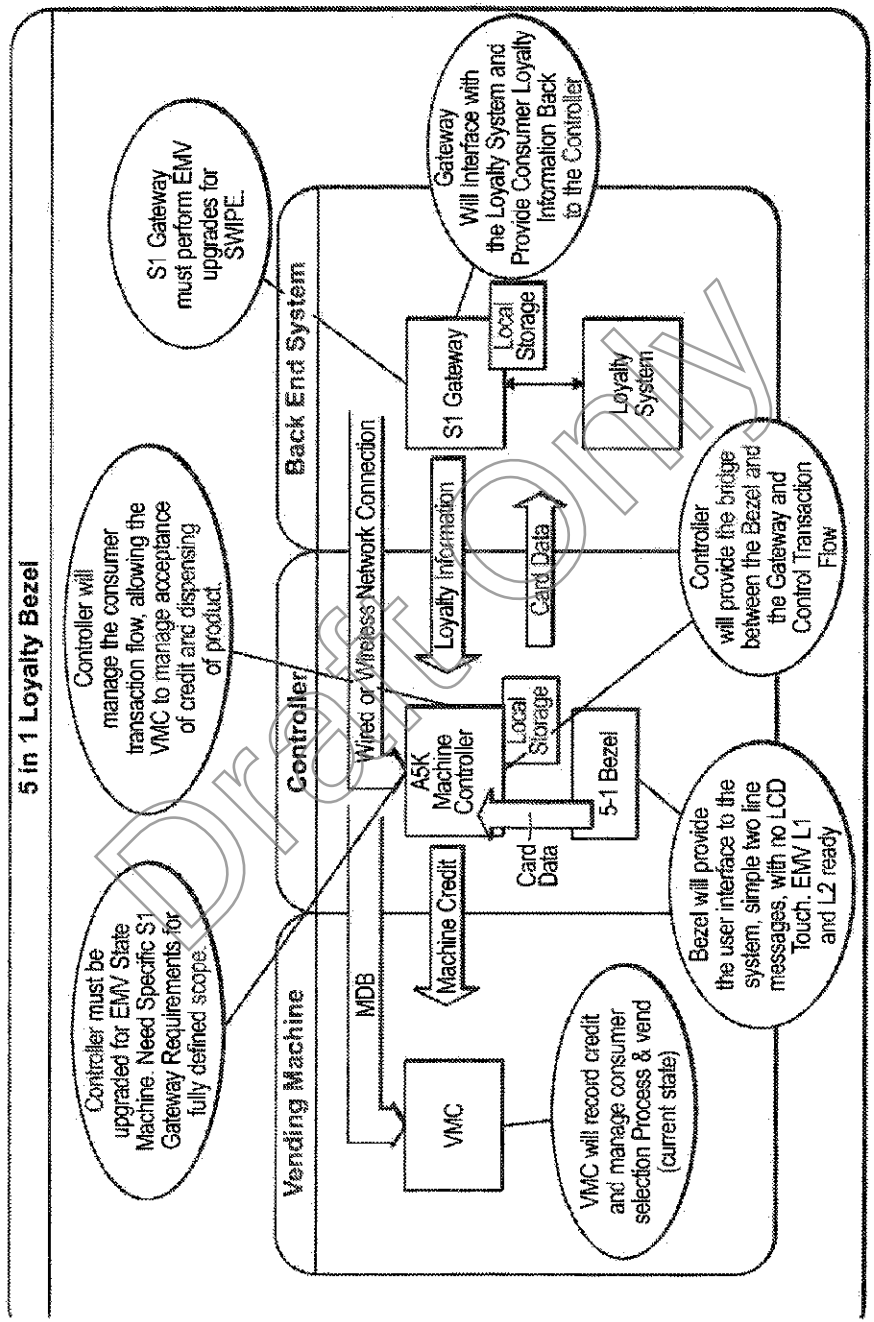


FIG. 4

Draft Only

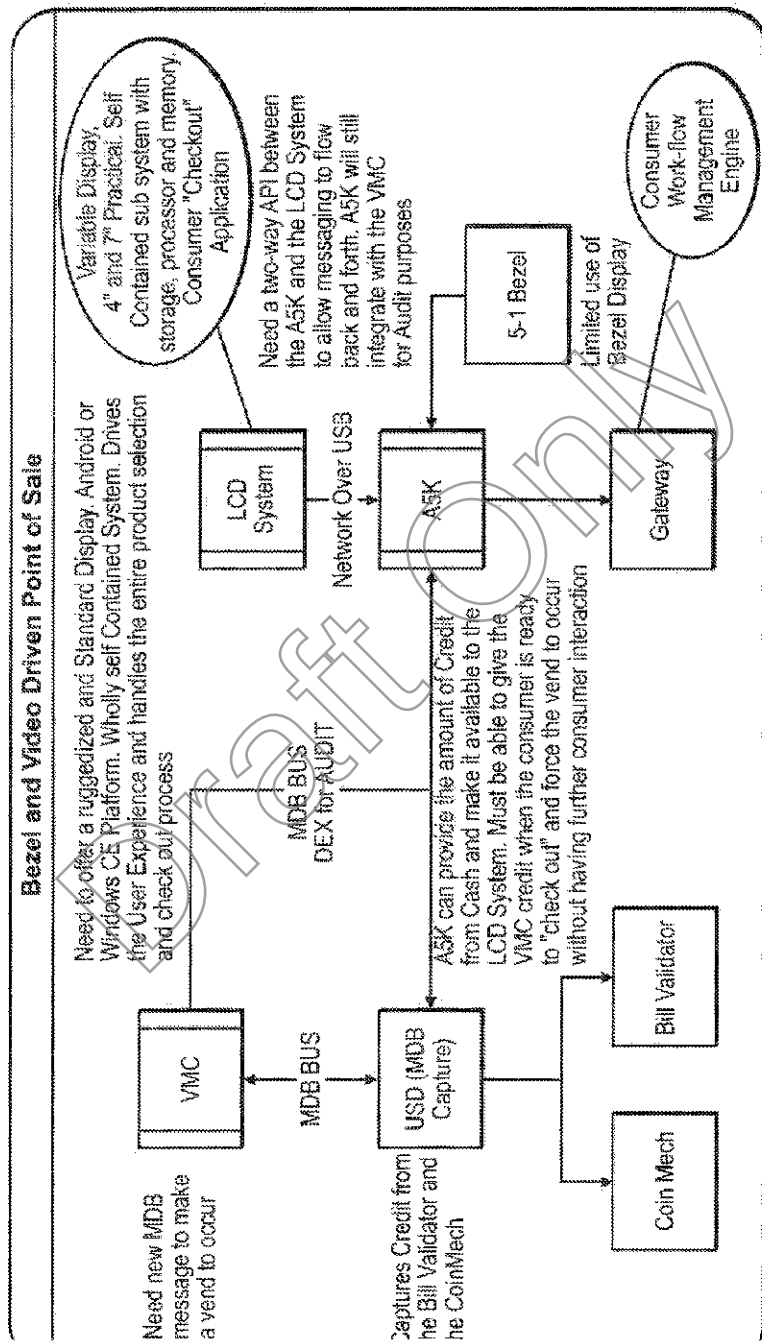


FIG. 5

Draft Only

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/075077

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 20/20 (2014.01)
USPC - 705/16
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) - G06Q 20/20, 30/06 (2014.01)
USPC - 700/214; 705/16

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
CPC - G06Q 20/20, 30/0613, 30/0641 (2014.02)

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2009/0013028 A1 (CANTER et al) 08 January 2009 (08.01.2009) entire document	1-22
Y	US 2006/0252523 A1 (WALKER et al) 09 November 2006 (09.11.2006) entire document	1-22
A	WO 2011/120104 A1 (FELICIJE) 06 October 2011 (06.10.2011) entire document	1-22
A	US 2002/0194387 A1 (DEFOSSE) 19 December 2002 (19.12.2002) entire document	1-22
A	US 2009/0076650 A1 (FAES) 19 March 2009 (19.03.2009) entire document	1-22
A	US 2007/0170249 A1 (RADEMACHER) 26 July 2007 (26.07.2007) entire document	1-22

Draft Only

☐ 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
02 April 2014	16 APR 2014
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) (July 2009)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 August 2016 (04.08.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/123545 A1

(51) International Patent Classification:
G06Q 30/02 (2012.01) *G06Q 30/06* (2012.01)
G06Q 20/18 (2012.01)

(21) International Application Number:
PCT/US2016/015763

(22) International Filing Date:
29 January 2016 (29.01.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14/611,065 30 January 2015 (30.01.2015) US
14/614,336 4 February 2015 (04.02.2015) US

(71) Applicant: **PAYRANGE, INC.** [US/US]; 700 NE Multnomah Street, Suite 1400, Portland, OR 97232 (US).

(72) Inventor: **PATEL, Paresh, K.**; 700 NE Multnomah Street, Suite 1400, Portland, OR 97232 (US).

(74) Agents: **CRISMAN, Douglas J.** et al.; Morgan Lewis & Bockius LLP, 2 Palo Alto Square, 3000 El Camino Real, Suite 700, Palo Alto, CA 94306 (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, BN, BR, BW, BY, BZ, CA, CH, CL, 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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report (Art. 21(3))*

(54) Title: METHOD AND SYSTEM FOR PROVIDING OFFERS FOR AUTOMATED RETAIL MACHINES VIA MOBILE DEVICES

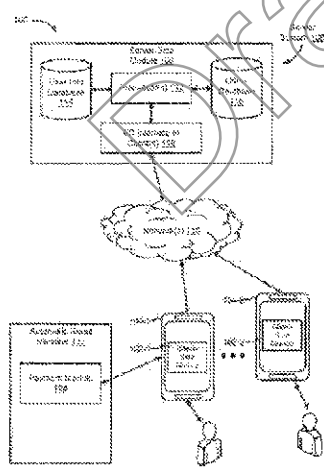


Figure 1

(57) Abstract: A mobile device with a display, processor(s), and memory: displays promotional offers; detects a user input selecting one of the promotional offers; and initiates performance of a transaction with an automatic retail machine to purchase a product stocked by the automatic retail machine. The mobile device also: receives a transaction completion notification from the payment module indicating that the product corresponding to the selected promotional offer was vended by the automatic retail machine; and, in response to receiving the transaction completion notification, provides a prompt to the user of the mobile device to obtain a product code for the vended product to validate the promotional offer. The mobile device further: obtains the product code for the vended product; transmits the product code to the server; and, in response: receives promotion validation information from the server; and displays the promotion validation information indicating whether the respective promotion offer was validated.

Draft Only

WO 2016/123545 A1

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 November 2013 (28.11.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/177416 A2

(51) International Patent Classification:
G06Q 20/32 (2012.01)

(21) International Application Number:
PCT/US2013/042455

(22) International Filing Date:
23 May 2013 (23.05.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/651,276	24 May 2012 (24.05.2012)	US
61/772,260	4 March 2013 (04.03.2013)	US
61/794,545	15 March 2013 (15.03.2013)	US

(71) Applicant: **JVL VENTURES, LLC** [US/US]; 230 Park Avenue, Suite 2829, New York, NY 10169-0005 (US).

(72) Inventors: **BUSH, Larry, L.**; 13637 N. 12th Way, Phoenix, AZ 85022 (US). **TOMCZAK, Christopher, J.**; 1319 Lochness Drive, Allen, TX 75013 (US).

(74) Agents: **BERSCHADSKY, Jonathan** et al.; Fitzpatrick, Cella, Harper & Scinto, 1290 Avenue Of The Americas, New York, NY 10104-3800 (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, BN, BR, BW, BY, BZ, CA, CH, CL, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

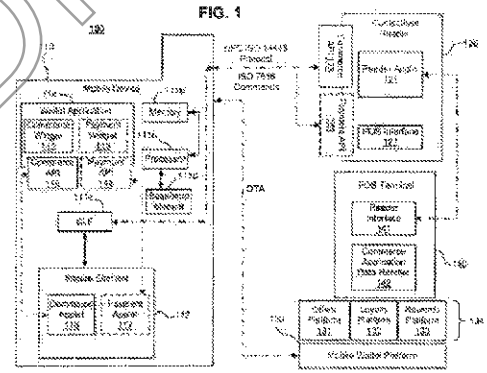
Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

Draft Only

(54) Title: SYSTEMS, METHODS, AND COMPUTER PROGRAM PRODUCTS FOR PROVIDING A CONTACTLESS PROTOCOL

FIG. 1



(57) Abstract: Systems, methods and computer program products are provided for managing contactless transactions. A first tap is performed when a system is placed within a predetermined proximity to a payment terminal. A first select command including an AID corresponding to a first application is received from the payment terminal. A first response based on the first select command is transmitted to the payment terminal. A data request including information indicating supported data types is received from the payment terminal. A second response based on the data request and including transaction data is transmitted to the payment terminal.

WO 2013/177416 A2

SYSTEMS, METHODS, AND COMPUTER PROGRAM PRODUCTS FOR PROVIDING A CONTACTLESS PROTOCOL

Draft Only

BACKGROUND

Field

[0001] Example aspects described herein relate generally to contactless protocols and more particularly to systems, methods, and computer program products for providing a contactless protocol allowing interoperation between mobile devices, near field communication (NFC) readers, and point of sale (POS) systems.

Related Art

[0002] NFC technology is a standards-based wireless communication technology that allows data to be exchanged between devices that are positioned within a certain proximity, generally less than ten centimeters apart. One use of such NFC technology is for making contactless transactions, including those for payment,

access and ticketing. For example, an NFC-enabled mobile device can be provisioned with a payment application and payment account information (*i.e.*, credentials associated with a financial instrument such as credit or debit card) issued by a consumer's financial institution. Each payment application can store and manage multiple sets of commerce data associated with multiple merchants, manufacturers or brands on a secure element. The application and payment account information are typically encrypted and stored in a secure area in the mobile device. The mobile device can, in turn, use the NFC technology to communicate with NFC-enabled point of sale (POS) systems at attended locations such as stores and unattended locations such as vending machines. To pay, the consumer simply brings the mobile device to within approximately ten centimeters of a contactless payment-capable POS system and the transaction occurs. The process is typically the same as that used by the contactless credit and debit cards.

[0003] Placing the mobile device or contactless credit or debit card near an NFC-enabled reader so that they can be communicatively coupled is sometimes referred to as a "wave" or "tap". An application for a mobile device that allows consumers to "tap to pay" at a NFC-enabled POS systems is generally referred to as a "wallet application" or "mobile wallet client application." An application related to payments is generally referred to as a "payment" application. Common contactless payment applications are facilitated using any of the following technologies: American Express® "ExpressPay," Discover® "ZIP," Mastercard® "PayPass" or Visa® "PayWave".

[0004] NFC can also be used to read information about products or receive special offers, loyalty or rewards information from, for example, NFC tags, smart posters or smart billboards. An application related to offers, loyalty and rewards is generally referred to herein as a "commerce" application.

[0005] One technical challenge associated with utilizing payment and commerce technologies cooperatively involves the ability to allow the same tap event that sends payment information to include additional information associated with merchant loyalty cards, offers, rewards, and the like. To this end, messaging technologies in existing NFC readers or NFC-enabled payment POS terminals

Draft Only

stand to be upgraded to effectively support a messaging technology that retrieves and/or receives both payment credentials (using the aforementioned payment protocols) and additional commerce data (loyalty, offers, rewards, etc.) from mobile devices used to perform the transactions. Yet another technical challenge involves publishing commerce elements (*e.g.*, offers, loyalty card credentials, rewards, and the like) into a mobile device such that those commerce elements may, in turn, be presented as part of a typical POS transaction (*e.g.*, a purchase).

BRIEF DESCRIPTION

[0006] The example embodiments presented herein meet the above-identified needs by providing systems, methods and computer program products for providing a contactless protocol.

[0007] In one embodiment, a system for managing contactless transactions includes at least one memory operable to store commerce data and financial instrument data, and at least one processor coupled to the at least one memory. A first tap is performed, the first tap occurring when the system is placed within a predetermined proximity to a payment terminal. A first select command including an AID corresponding to a first application is received from the payment terminal. A first response based on the first select command is transmitted to the payment terminal. A data request including information indicating supported data types is received from the payment terminal. A second response based on the data request and including transaction data is transmitted to the payment terminal. The transaction data includes at least a portion of the commerce data stored in the at least one memory.

[0008] In another embodiment, a method for managing contactless transactions includes: performing a first tap, the first tap occurring when a mobile device is placed within a predetermined proximity to a payment terminal; receiving from the payment terminal a first select command including an AID corresponding to a first application; transmitting to the payment terminal a first response based on the first select command; receiving from the payment terminal a data request including information indicating supported data types; and transmitting to the payment terminal a second response based on the data request, the second

Draft Only

response including transaction data. The transaction data includes at least a portion of commerce data stored in at least one memory.

[0009] In another embodiment, a non-transitory computer-readable medium has sequences of instructions stored thereon for causing one or more processors to: perform a first tap, the first tap occurring when a mobile device is placed within a predetermined proximity to a payment terminal; receive from the payment terminal a first select command including an AID corresponding to a first application; transmit to the payment terminal a first response based on the first select command; receive from the payment terminal a data request including information indicating supported data types; and transmit to the payment terminal a second response based on the data request, the second response including transaction data. The transaction data includes at least a portion of commerce data stored in at least one memory.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The features and advantages of the example embodiments of the invention presented herein will become more apparent from the detailed description set forth below when taken in conjunction with the following drawings.

[0011] FIG. 1 is a graphical representation of a platform architecture in accordance with an exemplary embodiment.

[0012] FIG. 2 illustrates a single tap timing diagram according to an exemplary embodiment.

[0013] FIG. 3 shows a timing diagram illustrating a commerce process flow including a double tap and post transaction data transmission according to an exemplary embodiment.

[0014] FIG. 4 shows a timing diagram illustrating a commerce process flow including a double tap, and post transaction data and payment transmissions according to an exemplary embodiment.

[0015] FIG. 5 illustrates an exemplary multi-block data flow according to an example embodiment.

Draft Only

[0016] FIG. 6 illustrates windows or screen shots generated by the graphical user interface for a wallet application in accordance with an example embodiment of the present invention.

[0017] FIG. 7 illustrates a flow diagram illustrating an exemplary instant offer implementation according to an embodiment of the present invention.

[0018] FIG. 8 is a collaboration diagram of functional modules deployed on a computer system in accordance with an example embodiment of the present invention.

DETAILED DESCRIPTION

[0019] The example embodiments presented herein are directed to systems, methods and computer program products for providing a contactless protocol, which are now described herein in terms of an example merchant transaction. This description is not intended to limit the application of the example embodiments presented herein. In fact, after reading the following description, it will be apparent to one skilled in the relevant art(s) how to implement the following example embodiments in alternative embodiments (*e.g.*, involving mass transit transactions requiring a wireless communications connection between a mass transit terminal and a mobile device).

[0020] The terms "application," "applet," "widget," and/or the plural form of these terms are used interchangeably herein to refer to an application (functioning independently or in conjunction with other applications) or set or subset of instructions or code, which when executed by one or more processors (*e.g.*, in a mobile device, card reader, terminal, point of sale (POS) system, or server) causes the processor(s) to perform specific tasks. For example, a wallet application can be used to conduct transaction- or interface-related functions such as storing, processing, accessing or transmitting financial, loyalty, offer, membership, or account data. A wallet application may also incorporate or interact with one or more payment applications, such as ExpressPay from American Express®, Discover® Network Zip℠, MasterCard® PayPass™ and Visa payWave™ payment applets.

Draft Only

[0021] Generally, commerce-related services are made available through a suite of applications available on several different platforms. The first application (or suite of applications) exists onboard a server within a mobile commerce (MoCom) platform. The MoCom platform is responsible for the management of consumer data, including loyalty accounts and offers. In addition, the MoCom platform serves as a campaign manager for offers, providing a remote data store for offers made available to the consumer via the available merchant portals within a wallet application.

[0022] A second application exist onboard a mobile device in the form of a wallet application. The wallet application provides the consumer's primary user interface (UI) and additional commerce application services through which the wallet application may access additional resources onboard a secure element (SE) of a mobile device.

[0023] A third application exists onboard a secure element of a mobile device in the form of JavaCard applet. This applet stores commerce-related data such as loyalty and offer data and provides an interface through which the data may be managed. The applet is accessible through the use of Application Protocol Data Unit (APDU) commands as defined in International Standards Organization (ISO) 7816-4.

[0024] The fourth application exists onboard an NFC-enabled reader (referred to herein simply as a "reader"). The reader can be either a stand-alone device or attached to (and managed by) a point of sale (POS) terminal. This application facilitates or provides access to the interface with a secure element on a mobile device, performing specific tasks that optimize the APDU command/data exchange tasks. For example, it includes the reading of loyalty or offer information following the placement of a mobile device in proximity of a reader (*i.e.*, a "tap").

[0025] A fifth application (or suite of applications) exists onboard a merchant POS system, including a POS terminal and any additional merchant-specific hardware/software. These applications manage the data related to payment/loyalty/offers/rewards received from a secure element on a mobile

Draft Only

device via a reader. In most cases, this data will then be forwarded to a corresponding MoCom or merchant specific platform(s).

[0026] FIG. 1 is a graphical representation of a platform architecture in accordance with an exemplary embodiment. As shown in FIG. 1, system 100 includes a mobile device 110 communicatively coupled to a contactless (*e.g.*, proximity or NFC) reader 120 and a mobile wallet platform 130. Reader 120 also is communicatively coupled to a POS terminal 140. POS terminal 140 may be within the same housing as reader 120. Alternatively, POS terminal 140 and reader 120 are communicatively coupled with each other but each of these components is housed separately.

[0027] Mobile device 110 may be, for example, a cellular phone or the like, and includes a processor 111a, memory 111b, a contactless frontend (CLF) 111c, a baseband modem 111d, and a user interface such as a display (not shown). Baseband modem 111d is a digital modem that is used for mobile network communications. CLF 111c is circuitry which handles the analog aspect of contactless or NFC communications and the communication protocol layers of a contactless transmission link. CLF 111c also is used to exchange data between reader 120 and a secure element (or SE) 112 contained in mobile device 110, for example, to execute contactless transactions.

[0028] Secure element 112 may be implemented as a Universal Integrated Circuit Card (UICC), embedded SE card, secure micro secure digital (microSD) card, and the like. Secure element 112 is generally considered secure because it is a self-contained system, including dedicated memory, and is protected by hardware and software hardening techniques that are verified by independent testing.

[0029] Secure element 112 includes (*e.g.*, stored thereon) one or more commerce applets 113. Each commerce applet 113 is associated with a commerce service and an account issued by a commerce service provider (SP). A service provider is a company, organization, entity, or the like, that provides services to customers or consumers. Examples of service providers include account-issuing entities such as banks, merchants, card associations, marketing companies, and transit authorities. A service may be an activity, capability, functionality, work, or use

Draft Only

that is permitted or provided by a service provider, such as a payment service, credit, debit, checking, gift, offer or loyalty service, transit pass service, and the like.

[0030] A commerce service provider can provision (or have provisioned) onto secure element 112 one or more separate commerce applets 113. In addition, other independent service providers can provision (or have provisioned) onto secure element 112 their own commerce applet(s) 113. Generally, a commerce applet 113 stores both loyalty and offers related data, providing an APDU interface through which this data can be managed. Commerce applet 113 operates as a generic storage container, allowing multiple loyalty/offers services to share mechanisms (*e.g.*, secure element, mobile device) for loyalty/offer data management. If memory restrictions and performance requirements limit the amount of loyalty/offers data that can be stored on secure element 112, additional data can be stored in mobile device memory 111b and managed by the consumer via commerce widget 115. For example, any graphic images related to an offer can be stored in memory 111b in order to optimize secure element memory allocation. Loyalty/offers data management can be handled by the corresponding offer platform 131, loyalty platform 132, or rewards platform 133.

[0031] Commerce applet 113 includes a cached merchant data table enabling the storage/management of all data related to a given merchant. This allows the commerce data for a given merchant to be pre-loaded in secure element 112 or mobile device 110 by a wallet application. Exemplary commerce elements (and their corresponding tag values used during Tag Length Value (TLV) encoding) that are included in the cached merchant data table are defined below. This data is stored in a record oriented data buffer. In an exemplary embodiment, a merchant identifier (Merchant Identifier) is used as the key field for search/retrieval tasks. Optionally, an index (or hash table) may be created to improve performance.

[0032] One or more commerce applets 113 can be loaded onto the secure element 112, for example, during manufacture and/or configuration of the secure element 112 and may be personalized to enable its use to conduct commerce transactions. A commerce applet 113 interfaces with reader 120 via a commerce

Draft Only

application programming interface (API) 123. In an exemplary embodiment, a commerce applet 113 is in the form of a JavaCard applet and is accessible through the use of APDU commands as defined in ISO 7816-4. Particularly, commerce applet 113 communicates commerce elements to reader 120 via secure element 112 using ISO 7816 commands over the NFC ISO 14443 protocol.

[0033] Secure element 112 can also include one or more payment applets 117 where each payment applet 117 is associated with a payment service and an account issued by a payment service provider. One or more payment applets 117 also can be loaded onto the secure element 112, for example, during manufacture and/or configuration of the secure element 112 and may be personalized to enable its use to conduct payment transactions. A payment applet 117 interfaces with reader 120 via API 124. In an exemplary embodiment, payment applet 117 is in the form of a JavaCard applet and is accessible through the use of APDU commands as defined in ISO 7816-4. Payment applet 113 also communicates payment elements to reader 120 via secure element 112 using ISO 7816 commands over the NFC ISO 14443 protocol.

[0034] It should be understood that other communications between the aforementioned devices may include communications with or through other intervening systems, hardware, and/or software, and such communications may include receiving, transferring, and/or managing data.

[0035] A wallet application 114 stored on mobile device 110 includes instructions which, when executed by the processor of the mobile device 110, cause the mobile device 110 to act as an instrument, for example, for processing transactions such as contactless commerce and/or payment transactions. Wallet application 114 communicates, through the use of APDU commands as defined in ISO 7816-4, with the commerce applet 113 via commerce API 116 and to payment applet 117 via payment API 118.

[0036] Commerce widget 115 is a component of the wallet application 114 that provides an interface for consumers to manage commerce elements (*e.g.*, loyalty card credentials, offers and rewards), for example, through interactions with the display or user interface of a mobile device. Commerce widget 115 maintains, for example, a master list of commerce elements present on the handset in a

Draft Only

memory of the mobile device (*e.g.*, 111b). A subset of offers that have been identified as ready to be used are, in turn, moved to secure element 112 to be communicated to contactless reader 120 and POS terminal 140. Sensitive information, such as loyalty account identifiers can be stored on secure element 112.

[0037] Payment widget 119 is a component of the wallet application 114 that provides an interface for consumers to manage payment elements (*e.g.*, credit or debit card credentials), for example, through interactions with the display or user interface of a mobile device.

[0038] Reader 120 includes a reader commerce application 121 (referred to herein simply as a "reader application") and a POS interface 122. Reader 120 manages two interfaces: one interface is with the secure element 112 in the mobile device 110 and the other interface is with POS terminal 140 which includes a reader interface 141 and a commerce application data handler 142. The functionality of reader 120 is the same whether reader 120 is standalone and connected to a payments terminal or merchant POS, or is integrated therein. Contactless payment functionality is also contained in reader 120 but is not shown.

[0039] Mobile device 110 is further communicatively coupled to a mobile wallet platform 130, which in turn is communicatively coupled to offers platform 131, loyalty platform 132 and rewards platform 133. Collectively, offers platform 131, loyalty platform 132 and rewards platform 133 can be referred to as a mobile commerce (MoCom) platform 134 and are implemented on one or more servers, referred to herein individually and collectively as a MoCom server (now shown).

[0040] In one embodiment, a customer may use mobile device 110 to conduct a contactless transaction at a POS equipped with reader 120. The customer places the mobile device 110 within a predetermined required proximity of the contactless reader 120 (*i.e.*, taps) causing CLF 111c of the mobile device 110 to communicate with reader 120 using, for example, NFC ISO 14443 protocols. Reader 120 also communicates with wallet application 114, commerce applet

Draft Only

113, and/or payment applications on the mobile device 110 to execute contactless transactions.

[0041] A secure element employs a Proximity Payment System Environment (PPSE) that serves as a directory of available credentials currently stored in secure element 112. Each credential is assigned a corresponding application identifier (AID) associated with a payment application and stored in the PPSE. When an NFC enabled-mobile device containing secure element 112 is placed in the vicinity of an NFC-enabled contactless reader, the contactless reader reads the credential and completes the transaction. Before doing so, however, the reader is initialized.

[0042] On mobile device 110, PPSE is an application used to maintain a list of payment applications stored on secure element 112, and provides accessibility to each payment application stored on the mobile device 112 by making them visible or not visible (*i.e.*, accessible) to systems or devices.

Reader Initialization

[0043] Initialization of the reader 120 will now be described in more detail. In one embodiment, reader 120 implements a function referred to as an Entry Point Manager (EPM) to control which application in a mobile device is selected. In this embodiment, EPM controls whether reader 120 sends a command to mobile device 110 to select an application that performs a commerce transaction or a command that performs a payment transaction. A command to select a commerce application is referred to herein as "Select Commerce." A command to select a payment application is referred to herein as "PPSE Select."

[0044] EPM also controls the start mode for the reader 120 and subsequent application switching during a checkout process. EPM thus facilitates switching (at reader 120) between the Select Commerce command for a commerce transaction and the PPSE Select command for payment transactions.

Commencing a Commerce Transaction on a Reader

[0045] A reader can be configured to initiate a commerce transaction on a reader according to several modes, which are described below in further detail. In one mode, referred to as "auto start", reader application 121 is the default application

Draft Only

on the reader 120. Being the default application allows reader application 121 to be available to the consumer as a first tap option (*i.e.*, upon an initial coupling communication between the mobile device 110 and contactless reader 120).

[0046] Another mode, referred to as "manual start," allows manual intervention to be used to initiate reader commerce application 121. Manual intervention can be in the form of a command from POS terminal 130 (*e.g.*, initiated by using a POS terminal interface) or from a consumer selecting a commerce application on a mobile device by using commerce widget 115.

[0047] Another mode, referred to as "payment with post transaction data," involves controlling how payments are handled in an activity stream. If a merchant supports the provisioning of post transaction data, for example, then payment and receipt of merchant data can be accomplished by the same tap event, such as after the final total for a transaction has been calculated.

[0048] Another mode is referred to as "payment first." The payment first option works in conjunction with the auto start mode and/or the manual start mode to initiate a PPSE Select command for payment and then a Select Commerce command to obtain commerce data (*e.g.*, loyalty data, offer data, reward data, and the like). Commerce data is interchangeably referred to herein as "commerce elements."

Auto Start Mode

[0049] Referring to FIG. 1, auto start mode provides commerce functionality on reader 120 at the beginning of a POS checkout process. When mobile device 110 taps reader 120, reader application 121 causes reader 120 to send a "Select Commerce" message to mobile device 110 including the AID corresponding to the commerce application to be used to execute a contactless transaction. If the message is accepted by mobile device 110 it sends a positive response message in return. Next, reader 120 sends mobile device 110 a "Get Commerce Data" command. The Get Commerce Data command contains merchant specific data that secure element 112 uses to perform a commerce transaction. Also, control passes to the mobile device 110 upon successful completion of the Get Commerce Data transaction. If reader 120 receives a negative response to "Select Commerce" message it passes control back to the EPM.

Draft Only

Manual Start Mode

[0050] Referring still to FIG. 1, in manual startup mode, reader 120 starts reader application 121 in response to a request from either the consumer or the POS terminal 140. In this manual start mode, at the beginning of a checkout process, reader 120 is in a PPSE select state. For a consumer initiated commerce transaction, the consumer selects the commerce application at the customer facing device (*e.g.*, commerce widget 115). The customer facing device then sends a command to reader 120 to start the reader application 121 via the EPM. For a POS terminal initiated commerce transaction, POS terminal 140 commands reader 120 to initialize the reader application 121. In one embodiment, this is initiated by a cashier via an interface on the POS terminal 140.

[0051] Once reader commerce application 121 has been started on reader 120, the commerce application will function as described in the auto start mode above.

Payment with Post Transaction Data

[0052] In payment with post transaction data mode, a payment transaction can be made such that post transaction data is communicated between POS terminal 140, reader 120, and secure element 112. This option allows the commerce protocol to start at the beginning of the consumer checkout, but payment is not requested by the reader 120 until the final transaction total has been calculated.

[0053] POS terminal 140 sends a "Post Transaction" command to reader 120 with, for example, a transaction identifier (ID) and redeemed coupon IDs. Reader 120 then transmits a request for a tap for payment. The tap allows reader 120 to first request payment credentials from secure element 112 and then cause the reader application 121 to send commerce data (*e.g.*, coupon data) to secure element 112. Both functions are performed in a single tap by the mobile device 110 at reader 120.

Payment First

[0054] In payment first mode, a payment can be made first, prior to a commerce transaction. This option accommodates a situation where the payment/PPSE process must precede any commerce processing. Payment first mode works in

Draft Only

conjunction with both auto and the manual start modes discussed above. Payment and commerce processing is accomplished in a single tap.

EXEMPLARY COMMERCE PROCESS FLOWS

Normal Commerce Process Flow (Single Tap)

[0055] FIG. 2 illustrates a single tap timing diagram 200 according to an exemplary embodiment. The following process flow can commence as items being purchased are being scanned at a POS. For convenience, reader 120 (FIG. 1) and POS terminal 140 (FIG. 1) are illustrated as a single component and collectively referred to as payment terminal 201. Each component (*i.e.*, reader 120 or POS terminal 140) is referred to individually when applicable.

[0056] A merchant POS system 202 can be a merchant server operated by a merchant which controls the operation of payment terminal 201. In an exemplary embodiment, merchant POS system 202 commands payment terminal 201 to activate the reader ("Activate Reader") before items are being scanned, as items are being scanned, or after the items are scanned. In each case, reader 120 requests a user (or consumer) to place a mobile device 110 in proximity of reader 120, as shown in step 250 ("Request 'tap'"). In response to a request for the user to place a mobile device 110 in proximity of reader 120 (step 250), a consumer taps mobile device 110 onto reader 120, as shown in step 251.

[0057] Once a NFC connection has been established between mobile device 110 and reader 120, the following command exchanges are initiated for service initialization and processing of both a payment transaction and a commerce transaction. Payment transaction initialization and processing exchanges between secure element 112 and reader 120 include steps 260 and commerce transaction initialization and processing exchanges between secure element 112 and reader 120 include steps 262. Steps 260 may be performed before steps 262, afterward, or substantially simultaneously.

[0058] Referring first to steps 262, after a mobile device has tapped reader 120, reader 120 sends to secure element 112 a Select Commerce command along with a particular commerce AID ("Select Commerce AID") indicating which commerce applet within secure element 112 it seeks to cooperate with (*e.g.*,

Draft Only

commerce applet 113). In response, secure element 112 sends a positive or negative response. A negative response (not shown) results in reader 120 terminating reader application 121 (FIG. 1) and passing control to the EPM (not shown). If the response is positive ("Positive Response"), then reader 120 sends a command ("Get Commerce Data") to secure element 112 specifying identifying information, such as a merchant/store identifier, and any additional loyalty, offer or reward schemes supported by that location, date and time information, the version of reader commerce application 121 supported by reader 120, and any merchant capability data.

[0059] Secure element 112 returns corresponding commerce elements (*e.g.*, loyalty data, offer data, reward data) to reader 120 ("Loyalty & Offers Data") based on the fields in the Get Commerce Data command received from reader 120. In one embodiment, commerce applet 113 builds a package containing the commerce data (*e.g.*, a buffer or set of buffers including loyalty data, offer data, or rewards data). In another embodiment, the buffer is pre-built using memory space in the secure element 112.

[0060] Referring to steps 260, in one embodiment, reader 120 begins payment processing by sending a PPSE request ("PPSE Select") to secure element 112.

[0061] If the Select Commerce AID and PPSE Select requests are successful, as shown in step 264 ("Read Success Indication"), payment terminal 201 forwards the commerce application data and payment credentials it has received to the merchant POS system 202 for processing ("Payment & Commerce Data"). Merchant POS system 202, in turn, records the loyalty identifier and offers (not shown) and applies any applicable discounts as product scanning continues as shown in step 266. This concludes the commerce application process and the payment processing proceeds.

[0062] Once scanning has completed and a transaction amount has been approved for payment, a payment authorization request to a payment platform 203 is made ("Payment Auth Request"). In turn, payment platform 203 returns an authorization result ("Authorization Result") indicating whether or not the payment has been authorized.

Draft Only

[0063] Referring again to steps 260, in one embodiment, a PPSE Select request by reader 120 to secure element 112 causes secure element 112 to return a PPSE payment AID indicating which payment applet (and hence which corresponding payment network) should be used to perform the payment transaction ("PPSE Payment AID"). In response, reader 120 sends a Select AID indicating that it supports the particular applet ("Select AID"). File control information (FCI) associated with the payment applet (*e.g.*, FIG 1, 117) is sent by secure element 112 to reader 120. Similarly, other payment and card information is sent by secure element 112 to reader 120 ("Payment/Card Data").

[0064] FIG. 3 shows a timing diagram 300 illustrating a commerce process flow including a double tap and post transaction data transmission according to an exemplary embodiment. This embodiment can be used when a merchant has data to communicate back to a mobile device. For convenience, reader 120 (FIG. 1) and POS terminal 140 (FIG. 1) are illustrated as a single component and collectively referred to as payment terminal 301. Each component (*i.e.*, reader 120 or POS terminal 140) is referred to individually when applicable. Generally, POS terminal 140 (FIG. 1) initiates a request for a second tap by sending a command, "Post Transaction Command", to reader 120. Reader 120, in turn requests a second tap from the consumer.

[0065] A merchant POS system 302 can be a merchant server operated by a merchant which controls the operation of payment terminal 301. In an exemplary embodiment, merchant POS system 302 commands payment terminal 301 to activate reader 120 ("Activate Reader") before items are being scanned, as items are being scanned, or after the items are scanned. In each case, reader 120 requests a user to place a mobile device 110 in proximity of reader 120, as shown in step 350 ("Request 'tap'"). In response to a request for the user to place a mobile device 110 in proximity of reader 120 (step 350), a consumer taps mobile device 110 onto reader 120, as shown in step 351.

[0066] Once a NFC connection has been established between mobile device 110 and reader 120, the following command exchanges are initiated for service initialization and processing of both a payment transaction and a commerce transaction. Payment transaction initialization and processing exchanges between

Draft Only

secure element 112 and reader 120 include steps 360 and commerce transaction initialization and processing exchanges between secure element 112 and reader 120 include steps 362. Steps 360 may be performed before steps 362, afterward, or substantially simultaneously.

[0067] Referring first to steps 362, after mobile device 110 has tapped reader 120, reader 120 sends to secure element 112 a Select Commerce command along with a particular commerce AID ("Select Commerce AID") indicating which commerce applet within secure element 112 it seeks to cooperate with (*e.g.*, commerce applet 113). In response, secure element 112 sends a positive or negative response. A negative response (not shown) results in reader 120 terminating reader application 121 (FIG. 1) and passing control to the EPM (not shown). If the response is positive ("Positive Response"), then reader 120 sends a command to the secure element 112 specifying identifying information, such as a merchant/store identifier, and any additional loyalty and offer schemes supported by that location, date and time information, the version of reader commerce application 121 supported by reader 120 and any merchant capability data ("Get Commerce Data"). Secure element 112 returns corresponding commerce elements (*e.g.*, loyalty and offers data) to reader 120 ("Loyalty & Offers Data") based on the fields in the Get Commerce Data command received from reader 120. In one embodiment, this is accomplished by commerce applet 113, which builds a package of data (essentially a buffer or set of buffers including offers and loyalty data). In another embodiment, the buffer can be pre-built using memory space in the secure element 112.

[0068] Referring next to steps 360, in one embodiment, a PPSE Select request by reader 120 to secure element 112 causes secure element 112 to return a PPSE payment AID indicating which payment applet (and hence payment network) should be used to perform the payment transaction ("PPSE Payment AID"). In response, reader 120 sends a Select AID indicating that it supports the particular applet ("Select AID"). FCI associated with the payment applet (*e.g.*, 117) is sent by secure element 112 to reader 120. Similarly, other payment and card information is sent by secure element 112 to reader 120 ("Payment/Card Data").If the Select Commerce AID and PPSE Select requests are successful, as

Draft Only

shown in step 364, payment terminal 301 forwards the commerce application data and payment credentials it has received to the merchant POS system 302 for processing ("Payment & Commerce Data"). Merchant POS system 302, in turn, records the loyalty identifier and offers (not shown) and applies any applicable discounts as product scanning continues as shown in step 366.

[0069] Once scanning has completed and a transaction amount has been approved for payment, a payment authorization request to a payment platform 303 is made ("Payment Auth Request"). In turn, payment platform 303 returns an authorization result ("Authorization Result") indicating whether or not the payment has been made.

[0070]

[0071] If there is data to send back to payment terminal 301, merchant POS system creates a command, "Post Transaction Data", with correctly formatted TLVs and forwards the data to reader 120. Upon receipt of a Post Transaction command payment terminal 301 will request a second tap from the consumer, as shown in step 368 ("Request 2nd 'tap'").

[0072] Referring to step 369 and steps 370, when the mobile device 110 is placed within proximity of reader 120 for the second time as shown in step 369, reader 120 sends a secure element 112 a Select Commerce command along with a particular commerce AID ("Select Commerce AID") indicating which commerce applet within secure element 112 it seeks to cooperate with (e.g., commerce applet 113).

[0073] If a negative response is received reader 120 terminates the reader commerce application 121. If a positive response is received, then reader 120 forwards to secure element 112 the data received in the Post Transaction Data command from the POS terminal 140 ("Post Transaction Data"). This concludes commerce processing for this transaction.

[0074] FIG. 4 shows a timing diagram 400 illustrating a commerce process flow including a double tap, and post transaction data and payment transmissions according to an exemplary embodiment. In this scenario the payment and post transaction data are processed after a basket has been totaled and all discounts

Draft Only

have been applied. Usage of this flow is controlled by a reader start mode data element with a particular bit (*e.g.*, "Payment with Post Transaction") set on.

[0075] For convenience, reader 120 (FIG. 1) and POS terminal 140 (FIG. 1) are illustrated as a single component and collectively referred to as payment terminal 401. Each component (*i.e.*, reader 120 or POS terminal 140) is referred to individually when applicable. Generally, merchant POS system 402 initiates a request for a second tap by sending a post transaction data command to reader 120. Reader 120, in turn requests a second tap from the consumer.

[0076] A merchant POS system 402 can be a merchant server operated by a merchant which controls the operation of payment terminal 401. In an exemplary embodiment, merchant POS system 402 commands payment terminal 401 to activate the reader ("Activate Reader") before items are being scanned, as items are being scanned, or after the items are scanned. In each case, reader 120 requests a user to place a mobile device 110 in proximity of reader 120, as shown in step 450 ("Request 'tap'"). In response to a request for the user to place a mobile device 110 in proximity of reader 120 (step 450), a consumer taps mobile device 110 onto reader 120, as shown in step 451.

[0077] Once a NFC connection has been established between mobile device 110 and reader 120, the following command exchanges are initiated. The command exchanges are performed for service initialization and processing of both a payment transaction and a commerce transaction. Payment transaction initialization and processing exchanges between secure element 112 and reader 120 include steps 472, and commerce transaction initialization and processing exchanges between secure element 112 and reader 120 include steps 462 and 474.

[0078] Referring first to steps 462, after a mobile device has tapped reader 120, reader 120 sends to secure element 112 a Select Commerce command along with a particular commerce AID ("Select Commerce AID") indicating which commerce applet within secure element 112 to cooperate with (*e.g.*, commerce applet 113). In response, secure element 112 sends a positive or negative response. A negative response (not shown) results in reader 120 terminating reader application 121 (FIG. 1) and passing control to the EPM (not shown). If the response is positive ("Positive Response"), then reader 120 sends a command

Draft Only

to the secure element 112 specifying identifying information, such as a merchant/store identifier, and any additional loyalty and offer schemes supported by that location, date and time information, the version of reader commerce application 121 supported by reader 120 and any merchant capability data ("Get Commerce Data"). Secure element 112 returns corresponding commerce elements (*e.g.*, loyalty and offers data) to reader 120 ("Loyalty & Offers Data") based on the fields in the Get Commerce Data command received from reader 120. In one embodiment, this is accomplished by commerce applet 113, which builds a package of data (*e.g.*, a buffer or set of buffers including offers and loyalty data). In another embodiment, the buffer can be pre-built using memory space in the secure element 112.

[0079] At step 464, reader 120 indicates to the consumer that the transaction is complete and that the handset can be removed from payment terminal 401, which causes reader 120 to forward the commerce application data to the POS terminal 140 and, in turn, merchant POS system for processing ("Loyalty & Offers Data"). A clerk may continue to process the shopping basket.

[0080] Merchant POS system 402, records the loyalty identifier and offers (not shown) and applies any applicable discounts as product scanning continues as shown in step 466. After the basket total has been calculated, merchant POS system 402 sends a request for payment to payment terminal 401 and sends post transaction data to payment terminal 401 (if data is available to send) ("Send Post Transaction Data and Payment Req").

[0081] At step 468, payment terminal 140 requests a tap for payment. Reader 120, in turn, activates the reader field. When mobile device 110 is detected in the field of reader 120, payment processing is performed as shown in steps 472. Particularly, a PPSE Select request is made by reader 120 to secure element 112 to cause secure element 112 to return a PPSE payment AID indicating which payment applet (and hence payment network) should be used to perform the payment transaction ("PPSE Payment AID"). In response, reader 120 sends a Select AID command indicating that it supports the particular applet ("Select AID"). FCI associated with the payment applet (*e.g.*, FIG. 1, 117) is sent by

Draft Only

secure element 112 to reader 120. Similarly, other payment and card information is sent by secure element 112 to reader 120 ("Payment/Card Data").

[0082] Referring to steps 474, if payment terminal 401 has received post transaction data from merchant POS system 402, reader 120 starts the commerce application 121 (FIG. 1) and sends secure element 112 the Select Commerce command along with a particular commerce AID ("Select Commerce AID") after a mobile device has tapped reader 120 a second time. The Select Commerce AID identifies which commerce applet within secure element 112 should be used to cooperate with reader 120. In response, secure element 112 sends a positive or negative response. A negative response (not shown) results in reader 120 terminating reader application 121 (FIG. 1) and passing control to the EPM (not shown). If the response is positive ("Positive Response"), then reader 120 sends post transaction data to the secure element 112 ("Post Transaction Data"), with correctly formatted TLVs. This concludes commerce processing for this transaction.

[0083] If the Select Commerce AID and PPSE Select requests are successful, payment terminal 401 forwards the payment application data and payment credentials it has received to the merchant POS system 402 for processing ("Payment/Card Data"). In turn, merchant POS system sends a payment authorization request to a payment platform 403 ("Payment Auth Request"). In turn, payment platform 403 returns an authorization result (Authorization Result) indicating whether or not the payment has been authorized.

[0084] If the commerce and payment credentials and information have been successfully read, reader 120 can provide a notification either through an interface on payment terminal 140, commerce widget 115 (FIG. 1) or payment widget 119 (FIG. 1), as shown in step 478 ("Read Success Indication").

Commerce Message Specifications

Data Encoding

[0085] In one embodiment, all command/response data is encoded using BER-TLV (ISO 7816-4 Annex D) format. In some cases, the TLV (Tag, Length, Value) may be nested (embedded TLV). Due to the flexible nature of the

Draft Only

TLV encoding format, the tagged data may be placed in any order. This is true when formatting the data for both incoming and outgoing payloads. In addition, this data is stored in record oriented tables. The order of the TLV encoded data elements stored therein is not critical; however, some data may be placed at the beginning of the record to enhance index/search performance. Thus, the record data tables provided in this document are supplied as samples for reference purposes.

[0086] A tag is encoded using a "private" tag class and a tag type representing a primitive data object encoded on one or more subsequent bytes. Therefore, the first byte (tag class) is set to 0xDF. In all cases, the data element tag is defined on a single byte. Therefore, the second tag byte has the most significant bit (b8) set to 0. This allows up to 128 valid tag values (0x00 – 0x7F).

[0087] Length encoding supports both the short or long forms. When the length is less that (<) 128 bytes, the most significant bit (b8) is set to 0 and the actual length is specified in the remaining bits (b7 – b1). When the length is greater than (>) 128 bytes, the most significant bit (b8) is set to 1 (length mask = 0x80) and the remaining bits (b7-b1) define the number of subsequent bytes in the length field. Those subsequent bytes encode an integer equal to the number of bytes in the value field.

BER-TLV Example

[0088] Assuming the incoming data uses a tag value of 0x21 (Consumer ID) with a length of 8 bytes and a value of (0x1122334455667788), the data is encoded as shown in Table 1:

TABLE 1

Tag	Length	Value
DF 21	08	11 22 33 44 55 66 77 88
DF 21	81 08	11 22 33 44 55 66 77 88
DF 21	82 00 08	11 22 33 44 55 66 77 88

[0089] TLV encoding allows for the length indicator to be expressed in multiple bytes. Preferably multi-byte length is supported. In short form, the length field consists of a single byte where bit 8 is set to 0 and bits 7 to 1 encode the number

Draft Only

of bytes in the value field. One byte can thus encode any number from zero to 127. Any number from one to 127 is encoded in the same way in BER-TLV length field as in Lc and Le fields. The encoding differs for zero, 128 and more. See, for example, the coding of data objects in the Get Commerce Data command described below.

[0090] In long form, the length field consists of two or more bytes. Bit 8 of the first byte is set to 1 and bits 7 to 1 are not all equal, thus encoding the number of subsequent bytes in the length field. Those subsequent bytes encode the number of bytes in the value field. ISO/IEC 7816 does not use the "indefinite length" specified by the basic encoding rules of ASNI ISO/IEC 7816, which supports length fields of one, two, ... up to five bytes (Table 2). In ISO/IEC 7816, the values '80' and '85' to 'FF' are invalid for the first byte of length fields.

TABLE 2 – BER-TLV length fields in ISO/IEC 7816

	1st byte	2nd byte	3rd byte	4th byte	5th byte	N
1 byte	'00' to '7F'					0 to 127
2 bytes	'81'	'00' to 'FF'				0 to 255
3 bytes	'82'	'0000' to 'FFFF'				0 to 65 535
4 bytes	'83'	'000000' to 'FFFFFF'				0 to 16 777 215
5 bytes	'84'	'00000000' to 'FFFFFFFF'				0 to 4 294 967 295

Select Commerce Applet

[0091] In one embodiment, the processing starts when reader 120 detects a mobile device 110 in the field of reader 120 and NFC communications have commenced. At that time, reader 120 sends a command to secure element 112 to select a commerce applet, particularly a "Select Commerce" command. The Select Commerce command (also referred to as a "Select Commerce Applet" command) is standardized as defined in the ISO 78016-3 specification. An example Select Commerce command structure is shown in Table 3:

TABLE 3 – Select Commerce Applet

CLA	INS	P1	P2	Lc	Data	Le
00	A4	04	00	09	A00000048510010101	00

Draft Only

[0092] Secure element 112 in mobile device 110 validates the "Select Commerce" command and sends back an appropriate response. Example responses (also referred to as "Status Codes") are shown in Table 4:

TABLE 4 – Status Codes

SW1	SW2	Description
90	00	Successful execution of command
67	00	Wrong data length
69	01	Application ID not supported
69	99	Application not available
6A	82	Application not installed

[0093] All responses other than '90 00' ("Successful execution of command") cause commerce application 121 (FIG. 1) to terminate in reader 120 and pass control to the EPM.

Get Commerce Data

[0094] Upon commencement of the reader application 121 and communications between reader 120 and secure element 112 initiating, reader 120 sends a command to mobile device 110 to obtain commerce data, "Get Commerce Data." An exemplary Get Commerce Data command is defined below in Tables 5 and 6. In this example, specific loyalty and offers data is being requested. The "Merchant Capability" field is utilized by reader 120 to determine which fields need to be present in the request and response data.

[0095] Date and time stamp information are optional. In one embodiment, the date time is in synchronization with the POS. In the event that this information is not available from the POS, the date/time from the POS terminal 140 can be used. If date and time is not available, reader 120 will not send the date time stamp data element.

[0096] In an exemplary embodiment, the data elements contained in the Get Commerce Data request are preconfigured in the reader 120 or POS terminal 140 at setup time. The data may be modified after the reader 120 has been installed and configured.

Draft Only

TABLE 5 – Get Commerce Data

CLA	INS	P1	P2	Lc	Data	Le
90	50	00	00	xx	Merchant ID/ Store ID [+ Loyalty IDs +Coupon Types + Date/Time-Stamp +Application Version + Merchant Capability]	00

TABLE 6 – Command Data

Data Element	Byte Size	Value	Req
Merchant Identifier Tag	2	0xDF 31	Y
Identifier Length	1	xx	
Merchant Identifier	xx	[MerchantID]	
MerchantStore_ID Tag	2	0xDF 32	Y
Merchant_Store_ID Length	1	xx	
Merchant_Store_ID	xx	(StoreID/Location)	
Loyalty_ID Tag #1 For Secondary loyalty	2	0xDF 41	Opt
Identifier Length #1	1	xx	
LoyaltyID #1	xx	[Loyalty ID] (Hex)	
.....			
Loyalty_IDr Tag #X For Secondary loyalty	2	0xDF 41	Opt
Loyalty Identifier Length #X	1	xx	
LoyaltyID #X	xx	Loyalty ID (Hex)	
Date_Time_Stamp Tag	2	0xDF 11	Opt
Date_Time_Stamp Length	1	0x07	
Date_Time_Stamp	7	BCD (yyyymmddhhmmss)	
Commerce_App_Version Tag	2	0xDF 12	Y
Commerce_App_Version Length	1	0x02	
Commerce_App_Version Data	2	[Major + Minor] Hex	
Merchant_Capability Tag	2	0xDF 33	Y
Merchant_Capability Length	1	0x02	
Merchant_Capability Data	2	2 Bytes Hex	
Terminal_Startup_Mode_Tag	2	0xDF 34	Opt
Terminal_Startup_Mode_Length	1	0x02	
Terminal_Startup_Mode_Data	1	1 Bytes Hex	
Total:	<var>		

[0097] Table 7 defines the possible Status Word values that may be returned by the Get Commerce Data command.

Draft Only

TABLE 7 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
61	xx	More data to follow
67	00	Wrong Data Length
69	09	Internal Error

[0098] Any response other than'61 xx' or '90 00' will result in reader 120 terminating commerce application 121 and passing control to the EPM, after recording the error and storing the data for forwarding to commerce widget 115.

[0100] If the Get Commerce Data request is correctly formatted, commerce applet 113 on secure element 112 filters the data based on the merchant identifier ("Merchant_ID"), loyalty identifier ("Loyalty_ID") and offer type code ("Offer_Type_Code") to format a response data for reader 120 based on the version number in the request. Commerce applet 113 may return more than one Loyalty ID and multiple Offers messages based on the configuration in the wallet. Table 8 lists exemplary response data:

TABLE 8 – Example Response Data

Data Element	Byte Size	Value
Consumer_ID Tag	2	0XDF21
Consumer_ID Length	1	0x10
Consumer_ID_Data	16	[Consumer ID]
Loyalty_ID_Tag #1	2	0xDF41
Loyalty_ID_Length #1	1	xx
Loyalty Identifier #1	xx	[Loyalty ID]
Loyalty_Account_Code Tag #1	2	0xDF43
Loyalty_Account_Code Length #1	1	xx
Loyalty_Account_Code #1	xx	[Acct Code]
Loyalty_ID Tag #2	2	0xDF 41
Loyalty_ID Length #2	1	xx
Loyalty_ID_Data #2	xx	[Loyalty ID]
Loyalty_Account_Code Tag #2	2	0xDF43
Loyalty_Account_Code Length #2	1	xx
Loyalty_Account_Code Code #2	xx	[Acct Code]
.....		
Offer_ID_Tag #1	2	0xDF51
Offer_ID #1 ID Length	2	X'81 xx'

Draft Only

Data Element	Byte Size	Value
Offer_ID #1 ID Value	xx	[Coupon ID]
Offer_Code #1 Code Tag	2	0xDF53
Offer_Code #1 Code Length	2	0x'81xx'
Offer_Code #1 Code Value	xx	[Coupon Code]
Offer_ID_Tag #2	2	0xDF51
Offer_ID #2 ID Length	2	0x'81xx'
Offer_ID #2 ID Value	xx	[Coupon ID]
Offer_Code #2 Code Tag	2	0xDF53
Offer_Code #2 Code Length	2	0x'81xx'
Offer_Code #2 Code Value	xx	[Coupon Code]
.....		
Total:	<var>	

[0101] The following is an exemplary response data parsing sample. The NFC reader (or POS terminal) delivers this commerce data to a POS system in a string of data that may contain consumer, loyalty and/or offer data. The merchant POS system can then parse the data to obtain the loyalty and offer data, and process the data per the merchant's specifications.

```
DF 21 10 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF DF 41 06
18 DB 6E 23 F4 0B DF 43 0D 02 31 38 44 42 36 45 32 33 46 34 30 42
DF 51 08 88 77 66 55 44 33 22 05 DF 53 09 02 42 41 31 38 37 36 35
34 DF 51 08 88 77 66 55 44 33 22 06 DF 53 0C 02 41 39 39 39 39 31
33 33 35 37 38 DF 51 08 88 77 66 55 44 33 22 07 DF 53 10 02 5A 58
31 37 39 35 36 37 35 34 38 33 31 43 46 DF 51 08 88 77 66 55 44 33
22 08 DF 53 0C 02 31 38 30 30 38 37 32 30 30 30 31 DF 51 08 88 77
66 55 44 33 22 09 DF 53 33 02 57 4B 52 50 31 32 33 34 35 36 37 38
39 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 50 57 50 57 50
57 50 57 50 57 50 57 50 57 50 57 50 57 50 40 A1

Data parsing example

DF 21 10 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
(Consumer ID)

DF 41 06 18 DB 6E 23 F4 0B            (MoCom Loyalty ID)

DF 43 0D 02 31 38 44 42 36 45 32 33 46 34 30 42
(Consumer Loyalty Code)

DF 51 08 88 77 66 55 44 33 22 05      (MoCom Offer ID)  #1

DF 53 09 02 42 41 31 38 37 36 35 34   (Merchant Offer Code)  #1

DF 51 08 88 77 66 55 44 33 22
```

Draft Only

Post Transaction Data

[0102] As explained above, a Post Transaction Data command provides a mechanism to receive data back from a merchant POS system (MPOS). This command is initiated by the merchant POS terminal 140 and preferably is supported in the merchant capability field. In an exemplary embodiment, this command consists of a single frame of data with a maximum data size of 255 bytes. The contents of the data use standard TLV formatting but may also be variable. This command enables dynamic reconciliation or post transaction data consolidation. Additional data tags may be defined for the transmission of additional data from the POS terminal/MPOS to the secure element 112 in mobile device 110. An exemplary post transaction data command ("Post Transaction Data") is illustrated in tables 9 and 10:

TABLE 9 – Post Transaction Data Command

CLA	INS	P1	P2	Lc	Data	Le
90	52	00	00	xx	<TLV Encoded Post Transaction Data>	00

TABLE 10 – Command Data

Data Element	Byte Size	Value	Req
Transaction ID	2	0x DF 61	Opt
Transaction ID Length	1	xx	
Transaction ID Data	xx	Merchant generated Transaction ID	
Offer_ID Code #1	2	0XDF 51	Opt
Offer_ID Length #1	1	xx	
Offer_ID Data #1	xx	Coupon ID	
.....			
Offer_ID Code #X	2	0xDF 51	Opt
Offer_ID Length #X	1	xx	
Offer_ID Data #X	xx	Coupon ID	
Total:	<var>		

Multi-block data handling

[0103] FIG. 5 illustrates an exemplary multi-block data flow according to an example embodiment. When secure element 112 has more than 255 bytes of data to send, a Get Response command (C0) is used to retrieve the remaining response

Draft Only

data. Particularly, this command is used to obtain the remaining data when the commerce applet 113 must send more than, for example, 255 bytes of response data.

[0104] Referring to FIG. 5, after a user taps a commerce-enabled mobile device 110 to reader 120, reader 120 sends a Select Commerce command to the secure element 112 of the mobile device 110. A positive response ('90 00') causes reader 120 to send a Get Commerce Data command. In response, secure element 112 returns loyalty and offers data. As shown in FIG. 5, the Get Commerce Data response status SW1 flag is set to '61' and the SW2 flag is set to '00'.

[0105] A Get Response command is triggered when the SW1 flag in the Get Commerce Data response is set to '61'. In this example, the SW2 flag is set to '00' because commerce applet 113 on mobile device 110 may not know how much data is left to send. The subsequent response to the Get Response command also contains an SW1 flag set to '61', causing a second Get Response command to be sent by reader 120 to mobile device 110.

[0106] This sequence will terminate when the SW1 flag of the Get Commerce Data response is set to any value other than '61'. For example, an SW1 value of '90' in response to a Get Response command as shown in FIG. 5 will indicate normal completion. Any other SW1 value can be logged as an error.

[0107] Table 11 defines exemplary settings for the Get Response Data APDU command.

TABLE 11 – Get Response Data

CLA	INS	P1	P2	Lc	Data	Le
90	C0	00	00	00	<none>	00

[0108] The actual length of the remaining data is variable. Therefore, the Le data length can be 0x00; allowing the commerce applet 113 to manage a variable length response.

[0109] Table 12 defines possible status word values ("Status Codes") that may be returned by the Get Response Data APDU command.

Draft Only

TABLE 12 – Status Codes

SW1	SW2	Description
90	00	Successful execution of command
61	xx	More data to follow
67	00	Wrong data length
69	09	Internal error

Reader Configuration Data

[0110] In one embodiment, during the installation and configuration of reader 120 certain merchant and commerce specific data are loaded and saved in reader 120. This data is used by reader 120 to fill in the Get Commerce Data command from reader 120. These data elements can be updated as new features and functions become available.

Commerce AID

[0111] As explained above, a commerce AID is sent in the Select Commerce command. If the command is accepted by mobile device 110, commerce applet 113 is started and APDU command / response flows will start between reader 120 and secure element 112. In an exemplary embodiment, the commerce AID value is A0000004851001010l. This value can be hardcoded on reader 120. In one embodiment, reader 120 is not required to support partial selection.

Merchant_ID

[0112] A merchant identifier (Merchant_ID (DF31)) can be loaded onto reader 120. Merchant ID is a value assigned by a service provider. In one embodiment, this value is assigned by the MoCom platform operator. This is required to allow commerce applet 113 to filter the loyalty and coupon data, and send the appropriate items to the reader 120.

Merchant_Store_ID

[0113] A merchant store identifier value (Merchant_store_ID (DF32)) is loaded to the reader 120 and is a value assigned by a service provider. This value can be used, for example, for reporting purposes.

Draft Only

Loyalty_ID

[0114] A loyalty identifier value (Loyalty_ID (DF41)) is used when multiple Loyalty IDs are being requested during a tap. This is accomplished by setting the Secondary Loyalty in Merchant Capabilities (DF33). This allows commerce applet 113 to return additional loyalty numbers in the response to a Get Commerce Data command. Multiple (*e.g.*, 5) additional Loyalty_IDs may be coded in the Get Commerce Data request.

Offer_Type_Codes

[0115] Offer type codes (Offer Type Codes (DF54)) are loaded onto reader 120. Values assigned to Offer Type Codes are assigned by a service provider. This value is used by the commerce applet 113 to filter offers and send only the appropriate items to reader 120. Multiple Offer_Type_Codes can be defined and sent to the secure element 112 in the Get Commerce Data command.

Commerce_Application_Version

[0116] A commerce application version number (Commerce_Application_Version) can be loaded onto reader 120 to represent the version of the commerce reader specification that the application on reader 120 is coded to and certified for.

Merchant_Capabilities

[0117] The Merchant Capabilities value represents the Commerce features supported by a particular merchant. This data element can also be used by reader 120 to format the Get Commerce Data command.

Terminal_Startup_Mode

[0118] A terminal start mode command (Terminal Start Mode (DF34)) commands reader 120 to provide the mechanism used to start commerce application 121. This data element is not sent to the secure element 112. This data element will also be used to define processing flows between reader 120 and secure element 112 on the handset.

Draft Only

Get Commerce Data Fields

[0119] Table 13 provides an exemplary definition of data required by reader 120 to format the Select Commerce and Get Commerce Services commands:

TABLE 13

Data Element	Tag	Max Size Bytes	Data Format
Commerce AID		09	Hex
Merchant ID	DF 31	8	Hex
Merchant Store ID	DF 32	32	ASCII
Loyalty Identifier #1 thru X	DF 41	8	BCD
Date and Time Stamp	DF 11	7	BCD
Specification Version (Major/Minor)	DF 12	2	Hex
Merchant Capabilities	DF 33	2	Binary
Commerce Start Mode	DF 34	2	Binary

Commerce Applet Version Format

[0120] A Commerce Applet Version value is a two-byte hex field the first byte containing the major version (xx) and the second byte contains the minor version (xx). These fields are updated in accordance to the specific version of the reader commerce technical specification that is implemented on reader 120. In an exemplary embodiment, the first official release of the commerce application 121 is 0x0100.

Merchant Capabilities

[0121] A merchant capabilities field (Merchant Capabilities Field (DF 33)) determines which commerce functions are being implemented by the merchant. Reader 120 can pass this field to mobile device 110, and mobile device 110 uses the information to build a response frame, referred to as Commerce Data Response frame. Table 14 illustrates exemplary merchant capabilities:

TABLE 14 – Merchant Capability Data

Commerce Start Mode Format

Byte	Bit	Value	NFC reader function
1	8 MSB	1=Merchant Loyalty Support	If Bit 8 is on the reader will send the required Merchant ID and optionally a

Draft Only

		0=No	Loyalty ID for the merchant
1	7	1=Secondary Loyalty 0=No	Bit 8 must be on. Additional Loyalty ID's is included in the Get Commerce Data request
1	6	1=Offers Support 0=No	Offer Type fields is included in Get Commerce Data request
1	5	1=Additional Offer support 0=No	The merchant can request additional offers in the Get Commerce request
1	4	1=Contactless Payment support 0=No	Some merchants may choose to only accept Commerce but not contactless payments. This bit setting is information only. It will not stop the PPSE process from happening.
1	3	1=Enterprise Merch ID 0=No	
1	2	1=Cloud Based Offer 0=No	Indicates that the merchant can support cloud based offers. (Future)
1	2	0	Reserved for Future Use
1	1	1=Post Transaction Data support 0=No	The reader will receive redemption data from the POS and forward it to the handset
2	8-1	0	Reserved for Future Use

Commerce Start Mode Format

[0122] A commerce start mode format value (Commerce Start Mode (DF34)) indicates to reader 120 what mechanism is to be used to start commerce application 121 on reader 120. In one embodiment, this data element is not sent to the mobile device 110 in the Get Commerce Data command. In another embodiment, this data element is optional. Table 15 illustrates exemplary start modes can be used to commence commerce application 121. In an exemplary embodiment, bits 7 and 8 are exclusive and only one bit is turned on at a time:

TABLE 15 – Commerce Start Mode

Byte	Bit	Value	Reader function
1	8 MSB	1=Auto Start 0=No	At the start of the check the reader will quest Commerce AID at the first TAP
1	7	1=Manual Start 0=No	The reader will only select Commerce AID after some user intervention.
1	6	1=Payment with	Payment and Post Transaction Data will

Draft Only

		Post Transaction Data 0=No	occur on TAP 2
1	5	Payment First	Payment PPSE will precede in Auto or Manual start modes
1	4-1	0	Reserved for Future Use
2	8-1	0	Reserved for Future Use

Reader Message Forwarding

[0123] While reading commerce application data from the mobile device 110, reader 120 forwards the data to a merchant POS system or POS application resident on a POS terminal 140. Reader 120 strips off the APDU headers and un-blocks the data from the mobile device 110. The Tagged TLV frames are then wrapped in the appropriate protocol and forwarded to the merchant POS system or POS application running on the POS terminal for processing.

Commerce Response Data Description

[0124] During a successful interaction with a reader 120, data will be returned to the POS merchant system (or POS terminal). This information will typically be composed of a consumer loyalty number and/or some number of offers that the merchant defined and loaded to the consumer's wallet.

Consumer ID

[0125] A consumer identifier (Consumer ID) is a unique identifier that is assigned to a consumer during the wallet activation process. Typically, Consumer ID will stay with a consumer even if the consumer moves her wallet to a new mobile device or different mobile network. In a preferred embodiment, Consumer ID is sent from the mobile device to the reader on every commerce-related interaction, even if the handset has no loyalty or offers data to send. The presentation of Consumer ID can be used by the merchant POS system to trigger specific actions related to a payment-only tap.

Loyalty ID

[0126] A loyalty identifier (Loyalty ID) is sent along with each consumer loyalty number requested during a tap event. Loyalty ID is a unique value assigned to

Draft Only

each merchant loyalty program assigned by the MoCom platform. In most cases the Loyalty ID received by the reader will match the Merchant ID that was configured by the Get Commerce data command. Use of this information by a merchant system is optional.

Consumer Loyalty Code

[0127] A consumer loyalty code (Consumer Loyalty Code) matches the loyalty number assigned to the consumer for a specific merchant loyalty program. Wallet application 114 allows for multiple loyalty numbers to be presented at the tap. If the system is set up for multiple consumer loyalty codes, each consumer loyalty code will be preceded by its unique loyalty ID.

Offer ID

[0128] A mobile commerce offer identifier (Offer ID) is sent along with each consumer offer number sent during a commerce-related session. The Offer ID is a unique value assigned to each offer delivered to a consumer wallet. In one embodiment, no two Offer IDs generated by the MoCom platform will have the same value.

Merchant Offer Code

[0129] A merchant offer code ("Merchant Offer Code" or "Offer Number") is generated by the merchant and loaded to the consumer's wallet application through various means. This number matches the same offer that is defined on the merchant POS system for processing. There can be multiple merchant offers (*e.g.*, 10) presented during a single commerce transaction. The merchant system parses the incoming data to extract the individual merchant offers.

Commerce Response Data Fields

[0130] Table 16 defines exemplary data elements that may be returned to the merchant POS system after a successful commerce transaction:

Draft Only

TABLE 16

Data Element	Tag	Max Size Bytes	Data Format
Consumer ID	DF 21	16	BCD
Loyalty ID	DF 41	8	Hex
Consumer Loyalty Code	DF 43	32	ASCII, Hex, BCD
Offer ID	DF 51	8	BCD
Merchant Offer Code	DF 53	48	ASCII, Hex, BCD

[0131] In one embodiment, a data element "Terminal Start Mode" is passed to reader 120 but will not be passed to the secure element 112. Reader 120 uses this information to control when Select Commerce and Select PPSE commands are sent to the secure element 112.

Reader Commerce Application Functionality

[0132] The following section provides a list of functions that the Commerce application within reader 120 performs. Some of these functions are automated, while others are triggered via an API call from the POS terminal or merchant POS.

Select Commerce AID Command

[0133] After the Commerce application is started on reader 120 and a device is detected in the field of reader 120, the first command sent is Select Commerce AID. The command will contain the RID value assigned by ISO and a PIX value generated by a commerce service provider. The Commerce AID value is A0000004851001010l. This value should be hard coded on reader 120.

Get Commerce Data Command

[0134] The Get Commerce Services Data command is a general data request to the secure element 112. The Get Commerce Data has a number of required and optional fields that communicate information to commerce applet 113. Commerce applet 113 uses this information to build the data elements that need to be sent to reader 120. Reader 120 uses the fields in the Merchant Capability records to determine which optional fields need to be included in the request to the handset.

Draft Only

Post Transaction Data

[0135] The Post Transaction Data command was created to provide a mechanism to receive data back from the MPOS. This command consists of a single frame of data with a maximum data size of 255 bytes. The contents of the data use standard TLV formatting, but the contents may be variable. Additional data tags may be defined for the transmission of additional data from the POS Terminal/MPOS to secure element 112 in mobile device 110.

NFC Error recovery

[0136] In a preferred embodiment, reader 120 is able to recover from a reader error generated when the handset is prematurely removed from the NFC field. Reader 120 signals the read error to the consumer via a failure interface such as a speaker that outputs a "beep" or display that provides an optical indication such as via lights. The consumer is asked to tap again and the transaction that was in progress during the error is restarted. In the case where multiple transactions are being processed, such as a commerce transaction and a PPSE transaction, reader 120 will try to recover the last process being executed.

Large Data block support

[0137] In an exemplary embodiment, reader 120 reads and writes multiple 255-byte blocks of data to and from mobile device 112 in a single tap process.

Date and time stamp support

[0138] When reader 120 has connectivity to the merchant POS system, the date and time can be retrieved from the POS terminal at the start of the transaction.

TLV Master Tag List

[0139] Table 17 defines the data elements and corresponding tag values and target/max byte sizes used by commerce based applications. Additional values have been provided for those elements with a limited/fixed value range.

TABLE 17 – APDU Commands

Commerce Services			
Shared Data Elements			
Data Element	Tag	Max	Description

Draft Only

		Size	
DATE_TIME_STAMP	0xDF11	7	Date/Time stamp (yyyymmddhhmmss)
COMMERCE_APP_VERSION	0xDF12	2	Supported Commerce application Version Number
Consumer Data Elements			
Data Element	Tag	Max Size	Description
CONSUMER_ID	0XDF21	16	MoCom Platform specific consumer identifier
CONSUMER_KEY	0xDF22	16	MoCom Platform generated consumer specific 3DES key
CONSUMER_CERT	0xDF23	8	MoCom Platform generated consumer signature/ certificate
Merchant Data Elements			
Data Element	Tag	Max Size	Description
MERCHANT_ID	0xDF31	8	MoCom Platform specific merchant identifier
MERCHANT_STORE_ID	0xDF32	32	MoCom Platform specific merchant store identifier ASCII character data
MERCHANT_CAPABILITY	0xDF33	2	Supported Commerce application Services
NFC READER_START_MODE	0xDF34	2	NFC enabled payment terminal startup mode (provided by Merchant POS System during initialization)
Merchant Capabilities			
Data Element	Value	Max Size	Description
MERCAP_MERCHANT_ LOYALTY	0x80	1	The Get Commerce Data request includes a valid merchant identifier used to determine the Loyalty data received by the applet.
MERCAP_ADDITIONAL_ LOYALTY	0x40	1	The Get Commerce Data request includes additional Loyalty Identifiers. Additional Loyalty data is determined by the specified Loyalty ID(s).
MERCAP_MERCHANT_ OFFERS	0x20	1	Offer type fields are included in Get Commerce Data request

Draft Only

MERCAP_ADDITIONAL_ OFFERS	0x10	1	The Get Commerce Data request includes a valid merchant identifier used to determine the offers data received by the applet.
MERCAP_PAYMENT	0x08	1	Indicates merchant supports contactless payment.
MERCAP_ENTERPRISE	0x04	1	Indicates support for Enterprise Merchant ID
MERCAP_CLOUD	0x02	1	Indicates support for cloud based offers and Loyalty
MERCAP_REDEMPTION	0x01	1	The NFC reader supports the transmission of offer redemption data (from the POS) to the applet via the Redeem Offer command.
Service Provider Platform Data Elements			
PLATFORM_SIGNATURE	0x71	8	MoCom Platform generated MAC/Signature appended to command/data originating from the platform for remote verification purposes (data integrity/ authenticity).
PLATFORM_KEY	0x72	16	MoCom Platform Key
PLATFORM_CERT	0x73	8	MoCom Platform Certificate

Loyalty			
Loyalty Data Elements			
Data Element	Tag	Max Size	Description
EMBEDDED_TLV_ LOYALTY_DATA	0xDF40	xx	Embedded TLV loyalty data tag
LOYALTY_ID	0xDF41	8	MoCom Platform specific loyalty identifier
LOYALTY_STATUS	0xDF42	1	Loyalty card/account status (see below)
LOYALTY_ACCOUNT_ CODE	0xDF43	32	Loyalty account (barcode data)
LOYALTY_MAC_ SIGNATURE	0xDF44	8	MoCom Platform specific MAC/Signature for integrity/ authenticity verification

Transaction Log			
Transaction Data Elements			
Data Element	Tag	Max	Description

Draft Only

		Size	
EMBEDDED_TLV_ TRANSACTION_LOG	0xDF60	xx	Transaction log record data tag
TRANSACTION_ID	0xDF61	16	Transaction ID (assigned by POS)
TRANSACTION_STATUS	0xDF62	3	Transaction log record data tag

Offers			
Offer Data Elements			
Data Element	Tag	Max Size	Description
EMBEDDED_TLV_ OFFER_DATA	0xDF50	xx	Embedded TLV offer data tag
OFFER_ID	0xDF51	8	MoCom Platform specific offer identifier
OFFER_STATUS	0xDF52	1	Offer status (see below)
OFFER_CODE	0xDF53	130	Offer (UPC/EPC/GS1 Databar) barcode data
OFFER_TYPE_CODE	0xDF54	9	Offer Type (see below)
OFFER_MAC_ SIGNATURE	0xDF55	8	MoCom Platform specific data security signature
OFFER_UPDATE_FLAG	0xDF56	1	Update flag (synchronization status)

[0140] Table 18 provides a master list of exemplary APDU commands supported by the Commerce Applet 113.

TABLE 18

Command	CLA	INS	P1	P2	Lc	Data	Le
Get Commerce Data	90	50	00	00	xx	Date/Time Stamp + Merchant ID + Store ID [+ Commerce application Version + Merchant Capabilities + Transaction ID + Loyalty IDs + Offer Codes]	00
Post Transaction Data	90	52	00	00	xx	<TLV-Encoded Transaction Data>	00
Get Remaining Data	90	C0	00	00	xx	None	

Draft Only

Specially Formatted Data Elements

[0141] Data elements included in the commerce data payload may include a format byte that identifies the data encoding used for that element. The data encoding is specified by the merchant to ensure compatibility at the point of sale. The formatted data value is supplied by the commerce platform to the wallet application 114. Thus, no additional interpreting/formatting is necessary between the platform 130, wallet 114, secure element 112, and reader 120/POS terminal 140 (collectively referred to as "payment terminal"). It is the role of the payment terminal (or merchant POS system) to properly interpret the data and supply it to the merchant system for processing.

[0142] In an exemplary embodiment, the following data elements include the following format value:

- Loyalty Account Code (DF 43)
- Offer Code (DF 53)

[0143] Table 19 defines possible format byte values and their corresponding encoding rule:

TABLE 19

Format Byte	Encoding Rule	Description
0x00	Hexadecimal	Each byte of data is encoded in (raw) hexadecimal format.
0x01	Binary Coded Decimal (BCD)	Each nibble represents a single digit. Thus, only decimal values are specified. A data stream containing an odd number (length) of digits includes the hex value 'F' in the first nibble of the data stream.
0x02	ASCII	Each byte represents an ACII value that is interpreted as such and handled as its corresponding CHAR value. In most cases, these data streams are converted into a String before being passed to the merchant POS system for processing.

[0144] A BCD encoded data value that includes the hexadecimal value 'F' in the first nibble shall identify a data stream containing an odd number of digits. Thus, the BCD data stream *12345* is encoded in 3 byte buffer as follows: *0xF12345*.

Draft Only

Exemplary Implementations

[0145] FIG. 6 illustrates windows or screen shots generated by the graphical user interface for a wallet application in accordance with an example embodiment of the present invention. For purposes of this exemplary implementation, the mobile device 110 has some redeemable offers and loyalty cards stored in memory 111b.

[0146] The wallet home screen 601 features a strip of merchant tiles 604. A tile is present for every merchant that has a redeemable object (*e.g.*, a redeemable offer or loyalty card) present in the mobile wallet. The user may, for example, swipe through the tiles, left and right, to find a particular merchant. Once the particular merchant is found, the tile is selected to open a merchant offer view 602. This can be done prior to making a transaction or immediately prior to making the transaction, such as while waiting in line, or earlier (*e.g.*, while browsing through a store.).

[0147] The merchant offer view 602 presents a list of redeemable offers 603 available in the wallet. Non-redeemable promotions may be presented as well. If present, a loyalty card 605 is also presented and made accessible from the merchant offer view 602.

[0148] If the selected merchant is not a commerce-enabled merchant, there is no option presented to load offers for a commerce transaction. If the merchant is a commerce-enabled merchant, however, one or more buttons or icons 606a, 606b are presented allowing offers to be loaded for a commerce transaction.

[0149] The user may select an offer (*e.g.*, 606a), and then select the "Done" bar at the bottom of the screen.

[0150] In an exemplary embodiment, a limit as to the number of offers can be enforced by secure element 112 (*e.g.*, 10 offers), and the user interface of commerce widget 115 enforces this limit while the user is activating offers. The "Done" bar is the trigger to load the selected offers into secure element 112. If there are offers from another merchant in the secure element 112, they can be removed at the same time as the new offers are loaded – this ensures that there are only offers from one merchant present in the 112 at any given time.

Draft Only

[0151] When the secure element load is complete, the user taps the mobile device 110 to reader 120. What happens next depends on a few factors. If the reader that is tapped is not capable of processing commerce elements, the selected payment card is sent, but no commerce elements (*e.g.*, offers or loyalty credentials) are sent. A post-tap message is presented through the reader interface indicating that payment credentials were sent, with no other information.

[0152] If the reader that is tapped is capable of processing commerce elements, but the merchant-ID does not match the selected merchant, offers will not be sent. Commerce applet 113 in secure element 112 can search for a loyalty card for this merchant-ID and transmit loyalty credentials, if present. A post-tap message is presented through an interface indicating that an event took place, identifying the merchant and reporting that loyalty credentials were sent (if they were available) as well as the payment credentials.

[0153] If the reader that is tapped is a commerce-enabled reader and the merchant-ID matches the selected merchant, selected offers and (if present) the loyalty card credentials for the merchant are sent. Mobile device 110 can present a post-tap message through the commerce widget 115 user interface confirming that offers and loyalty (if present) were sent, along with payments.

[0154] Following the tap, offers that were loaded into the secure element 112 are left in secure element 112 until the user removes them or selects offers from another merchant. Alternatively, if the offers expire, it is removed from the secure element 112 when wallet maintenance is performed. In an exemplary embodiment, the selected merchant will remain the "active" merchant on the wallet home page until the user selects a different merchant.

Instant Offer Implementation

[0155] FIG. 7 illustrates a flow diagram illustrating an exemplary instant offer implementation according to an embodiment of the present invention. In this embodiment, a mobile commerce (MoCom) platform can be integrated with merchant POS system to implement a mechanism for users to select offers by using a wallet application and/or instant offers merchants make available to consumers.

Draft Only

[0156] A wallet application running on a mobile device can be used to allow consumers to pay for purchases and present loyalty and offers via a payment terminal. One way a consumer can redeem an offer is by selecting the offer via the wallet application to be presented at checkout.

[0157] Consumers can also be provided with offers that can be instantly redeemed through the wallet application. Such offers are referred to herein as "instant offers". This feature allows merchants to reward consumers who use a mobile device running the wallet application to make purchases. Consumers benefit from the instant offer because, among other reasons, they do not need to specifically select an offer via the wallet application. Depending on the implementation, an instant offer can be used along with an offer explicitly selected by the consumer from the wallet application. Whether an offer is selected by the consumer or provided "instantly," a consumer identifier ("Consumer ID") value retrieved from the mobile device (*e.g.*, from secure element 112) is used as the key for retrieving and redeeming an instant offer.

[0158] Referring to FIG. 7, in one embodiment, a consumer selects offers from the wallet application to be presented at the checkout. At block 702, a payment is requested at a POS. If at block 704, it is determined that the payment is not a contactless payment, then at block 706 the payment process is completed via alternative means (*e.g.*, by using cash) and the checkout process is completed. If it is determined at block 704 that the payment will be a contactless payment, then the mobile device user is asked to tap his or her mobile device to the reader (*e.g.*, reader 120 described above).

[0159] In response, the mobile device is tapped to the reader. During the tap event, a number of data elements can be passed between the reader and a secure element on the mobile device as described above. In one embodiment, the payment card data, Consumer ID, loyalty number, and offer codes are passed to the reader during the tap of the reader. In this embodiment, Consumer ID is sent to the reader even if the tap is for a payment only transaction with no offers selected.

Draft Only

[0160] If at block 708 it is determined that a MoCom Consumer ID is not present, then at block 706 the payment process is completed and the checkout process is completed by processing the payment.

[0161] If it is determined at block 708 that a MoCom Consumer ID is present, then at block 710 a determination is made as to whether a MoCom offer is present (*e.g.*, an offer selected by the user via a wallet application). If at block 710 a determination is made that a MoCom offer is present, then a determination is made at block 712 as to whether a MoCom instant offer has been defined as well. If at block 712 it is determined that a MoCom instant offer has been defined, both the MoCom offer (*i.e.*, an offer selected by a user via a wallet application interface) and MoCom instant offer are processed, as shown in block 714. Once the MoCom offer and/or MoCom instant offer are processed, the payment associated with those offers is processed as shown at step 706.

[0162] If at block 710 a determination is made that a MoCom Offer is not present, then at block 716 a determination is made as to whether a MoCom instant offer has been defined. If not, the payment is completed as shown at step 706. If a determination is made at block 716 that the MoCom instant offer is present, the MoCom instant offer is processed as shown at block 718 and the payment associated with the MoCom instant offer processed as shown at block 706.

[0163] If a determination is made at block 712 that a MoCom instant offer has not been defined, then a standard MoCom offer is processed, as shown at block 720 and at block 706 the payment processed is completed.

[0164] The merchant POS system can use the presence of the ConsumerID to trigger the use of an instant offer. The offer could be, for example, a cents off or percentage off type offer that a merchant using the MoCom system defines. This can be, for example, applied for the purchase of a specific item. In an exemplary implementation, the merchant is provided an option of turning instant offer functionality off or on when a wallet offer is presented during the tap.

[0165] The instant offer can be defined by a merchant and then distributed to its retail locations. The offer can also have an associated specific start and end date.

Draft Only

The ability to distribute instant offers to different geographical areas can be taken into account as well.

Commerce Applet Package/Applet/Instance Management

[0166] The following section defines the AID values and application specific parameters used during download/installation of commerce applet 113 (FIG. 1). Table 20 defines AIDs.

TABLE 20 – AIDs

Description	AID
Package AID	A0 00 00 04 85 10 01 01
Applet AID	A0 00 00 04 85 10 01 01 00
Instance AID	A0 00 00 04 85 10 01 01 01

Applet-Specific Installation Parameters

[0167] The commerce applet's initial commerce services data characteristics may be provisioned via applet-specific installation parameters. This data follows the standard JavaCard AID and installation parameters.

These parameters must be coded as shown in Table 21:

TABLE 21 – Applet Installation Parameters

Provisioning Data	Byte Size	Default Value
Maximum Number of Loyalty Records	2	20
Maximum Number of Pre-Load Merchant Records	2	1
Maximum Number of Transaction Records	2	3
Total:	6	

Memory Requirements

[0168] Exemplary memory specifications are listed in Table 22 below. The first memory specification, "Package Download," indicates the approximate amount of non-volatile (EEPROM) memory space required to download the commerce applet package. The second memory specification, "Instantiation," indicates the amount of memory required to instantiate a new instance of the commerce applet.

Draft Only

The final memory requirement, "Transient Data Space," indicates the amount of volatile (RAM) memory that is used by each instance of the commerce applet.

TABLE 22 – Applet Memory Requirements

Memory	Byte Size
Package Download	9396
Instantiation	6260
Transient Data Space	518

Data Management

[0169] The available commerce (*e.g.*, loyalty, offers, rewards, etc.) data is stored within the commerce applet 113 onboard the secure element 112. All of the relevant commerce data is stored in three separate data tables. These data tables are managed by the commerce applet 113. Additional commerce data may be stored/managed within a corresponding commerce widget 115 onboard the handset.

[0170] In one embodiment, the data elements defined herein have a variable length. Therefore, all elements (included those with a fixed length) will be assigned a maximum length. As a result, all lengths and byte size references should be interpreted as maximum values.

Commerce Data

[0171] Commerce applet 113 manages a few data fields that are shared by all commerce service applications. These data fields are stored in persistent data variables. An exemplary data element, Consumer ID, is defined in Table 23. Additional elements may be stored as well, such as consumer/platform keys and certificates.

TABLE 23

Variable	Type	Description
ConsumerID	byte[]	Unique consumer ID assigned to a specific MoCom consumer/user.

Draft Only

Loyalty Data Table

[0172] Commerce applet 113 also includes loyalty data tables enabling the storage/management of all consumer loyalty data.

[0173] Table 24 defines the data elements (and their corresponding tag values used during TLV encoding) that are included in the loyalty data table.

TABLE 24 – Loyalty Data

Data Element	Tag Value	Byte Size	TLV Encoding Overhead
LOYALTY_PROGRAM_ID	0xDF41	8	3
LOYALTY_ACCOUNT_CODE	0xDF43	32	3
Total:		40	6
Minimum TLV Encoded Record Size:		46	

[0174] The data is stored in a record oriented data buffer, where the loyalty identifier ("Loyalty ID") is utilized as the key field for search/retrieval tasks.

[0175] In an exemplary embodiment, TLV Data Overhead includes a (maximum) of five bytes per element data overhead (2-byte tag and 3-byte length) as required by the BER-TLV encoding format.

[0176] In an alternative embodiment, an index (or hash table) may be created internally to speed up the Loyalty ID search task.

Cached Merchant Data Table

[0177] Commerce applet 113 also includes a merchant cached data table enabling the storage/management of all data related to a given merchant. This feature allows the commerce data for a given merchant to be pre-loaded by the wallet application 114 in order to improve performance.

[0178] Table 25 defines the data elements (and their corresponding tag values used during TLV encoding) that are included in the cached merchant data table.

TABLE 25 – Cached Merchant Data

Data Element	Tag Value	Byte Size	TLV Encoding Overhead
MERCHANT_ID	0xDF31	8	3
LOYALTY_PROGRAM_ID	0xDF41	8	3
LOYALTY_ACCOUNT_CODE	0xDF43	32	3

Draft Only

OFFER_ID	0xDF51	8	3
OFFER_CODE	0xDF53	130	3
.....			
Maximum		104	6
Minimum TLV Encoded Record Size:		110	

[0179] The data is stored in a record oriented data buffer, where the merchant identifier ("Merchant ID") is utilized as the key field for search/retrieval tasks. An index (or hash table) may be created internally to speed up the Merchant ID search task.

[0180] In an exemplary embodiment, TLV Data Overhead includes a (maximum) of five bytes per element data overhead (2-byte tag and 3-byte length) as required by the BER-TLV encoding format.

Transaction Log

[0181] Commerce applet 113 includes a transaction log that is used to track usage within the MoCom platform at the merchant point-of-sale. During commerce widget 115 and secure element 112 synchronization tasks, this transaction log is transmitted up to the commerce widget 115 for later over-the-air ("OTA") synchronization with the MoCom platform.

[0182] The actual content of the transaction log depends upon the Get Commerce Data command data/parameters provided by reader 120 during the transaction process at the merchant point-of-sale. An exact copy of the data payload sent to the commerce applet 113 by reader 120 via the Get Commerce Data APDU command is stored within that commerce transaction's record.

[0183] The transaction status is determined based on the logical result of the commerce data processing. If a data/processing error is detected within the commerce applet 113, the corresponding internal error code can be appended to the transaction log.

[0184] The following table defines the data elements (and their corresponding tag values used during TLV encoding) that are included in the transaction log.

TABLE 26 – Transaction Log Data

Data Element	Tag Value	Byte Size	TLV Encoding Overhead

Draft Only

Get Commerce Data command parameter(s)/data	xx	255	4
TRANSACTION_STATUS	0xDF62	3	3
Total:		266	7
Maximum TLV Encoded Record Size:		273	

[0185] The data is stored in a record oriented data buffer. A variable Get Commerce Data command data size is supported.

[0186] TLV Data Overhead includes a (maximum) of five bytes per element data overhead (2-byte tag and 3-byte length) as required by the BER-TLV encoding format.

Error Management

[0187] In an exemplary embodiment, error detection and management is handled at two levels. First, the response of the APDU command includes a two-byte Status Word result value. These responses are standardized and dictated by ISO 7816-4. However, a second level of error handling is managed internally by the Commerce Services applet. The second level of management includes the issuance of a standard 0x6909 status word in the response to the APDU command. Following this response, the client may issue a second command ("Get Internal Error Code") to obtain a two-byte internal error code. This code may be cross-referenced to Table 27. Table 27 provides details on where and why the error occurred within the applet.

[0188] Particularly, Table 27 provides a master list of all possible internal error codes returned by the Get Internal Error Code APDU command supported by the commerce applet.

TABLE 27 – Internal Error Codes

Error Code	Error Description
0x0101	SSE_INTERNAL_ERROR_APPLET_NOT_PROVISION
0x0102	SSE_INTERNAL_ERROR_COMMAND_NOT_ALLOWED_VIA_CONTACTLESS_INTERFACE
0x0103	SSE_INTERNAL_ERROR_COMMAND_NOT_ALLOWED_INVALID_CONTEXT
0x0201	SSE_INSTALL_INVALID_INSTALLATION_PARAMETER_LENGTH
0x0301	SSE_PARSE_COMMAND_DATA_INVALID_COMMERCE_TAG
0x0302	SSE_PARSE_COMMAND_DATA_INVALID_CONSUMER_ID_LENGTH

Draft Only

0x0302	SSE_PARSE_COMMAND_DATA_INVALID_MERCHANT_ID_LENGTH
0x0302	SSE_PARSE_COMMAND_DATA_INVALID_MERCHANT_LOCATION_LENGTH
0x0303	SSE_PARSE_COMMAND_DATA_INVALID_DATE_TIME_STAMP_LENGTH
0x0304	SSE_PARSE_COMMAND_DATA_INVALID_MERCHANT_COMMERCE_APP_VERSION_LENGTH
0x0305	SSE_PARSE_COMMAND_DATA_INVALID_MERCHANT_CAPABILITIES_LENGTH
0x0306	SSE_PARSE_COMMAND_DATA_INVALID_LOYALTY_ID_LENGTH
0x0307	SSE_PARSE_COMMAND_DATA_INVALID_LOYALTY_ACCOUNT_CODE_LENGTH
0x0308	SSE_PARSE_COMMAND_DATA_INVALID_OFFER_ID_LENGTH
0x0309	SSE_PARSE_COMMAND_DATA_INVALID_OFFER_TYPE_CODE_LENGTH
0x030A	SSE_PARSE_COMMAND_DATA_INVALID_TRANSACTION_ID_LENGTH
0x030B	SSE_PARSE_COMMAND_DATA_INVALID_CACHED_MERCHANT_DATA_OFFER_COUNT_LENGTH
0x030C	SSE_PARSE_COMMAND_DATA_INVALID_CACHED_MERCHANT_DATA_LENGTH
0x030D	SSE_PARSE_COMMAND_DATA_INVALID_COMMERCE_TAG
0x0A01	SSE_GET_RESPONSE_REMAINING_DATA_INVALID_RESUME_STATE
0x0B01	SSE_VERIFY_REQUIRED_PARAMETERS_INVALID_PARAMETER_TAG
0x0B02	SSE_VERIFY_REQUIRED_PARAMETERS_DATE_TIME_STAMP_NOT_PRESENT
0x0B03	SSE_VERIFY_REQUIRED_PARAMETERS_MERCHANT_ID_NOT_PRESENT
0x0B04	SSE_VERIFY_REQUIRED_PARAMETERS_MERCHANT_STORE_ID_NOT_PRESENT
0x0B05	SSE_VERIFY_REQUIRED_PARAMETERS_MERCHANT_COMMERCE_APP_VERSION_NOT_PRESENT
0x0B06	SSE_VERIFY_REQUIRED_PARAMETERS_MERCHANT_CAPABILITIES_NOT_PRESENT
0x0B07	SSE_VERIFY_REQUIRED_PARAMETERS_LOYALTY_ID_NOT_PRESENT
0x0B08	SSE_VERIFY_REQUIRED_PARAMETERS_LOYALTY_ACCOUNT_CODE_NOT_PRESENT
0x0B0A	SSE_VERIFY_REQUIRED_PARAMETERS_CONSUMER_ID_NOT_PRESENT
0x0B0B	SSE_VERIFY_REQUIRED_PARAMETERS_CACHED_MERCHANT_DATA_OFFER_COUNT_NOT_PRESENT
0x0B0C	SSE_VERIFY_REQUIRED_PARAMETERS_EMBEDDED_TLV_CACHED_MERCHANT_DATA_NOT_PRESENT
0x0C01	SSE_GET_COMMERCE_DATA_INVALID_WALLET_STATE
0x0E01	SSE_UPDATE_CACHED_MERCHANT_DATA_FAILED_CMD_BUFFER_LENGTH_EXCEEDED
0x1101	LME_INVALID_LOYALTY_TAG
0x1102	LME_INVALID_LOYALTY_ID_LENGTH
0x1103	LME_INVALID_LOYALTY_ACCOUNT_CODE_LENGTH
0x1201	LME_GET_LOYALTY_DATA_RECORD_NOT_FOUND
0x1202	LME_GET_LOYALTY_DATA_INSUFFICIENT_BUFFER_LENGTH
0x1301	LME_UPDATE_LOYALTY_ID_NOT_SPECIFIED
0x1401	LME_DELETE_LOYALTY_ID_NOT_SPECIFIED
0x1402	LME_DELETE_LOYALTY_DATA_RECORD_NOT_FOUND

Draft Only

0x1501	LME_GET_LOYALTY_RECORD_INSUFFICIENT_BUFFER_LENGTH
0x3101	TLVME_MAX_DATA_LENGTH_EXCEEDED
0x3201	TLVME_APPEND_FAILED_INVALID_LENGTH
0x3301	TLVME_GET_NEXT_TAG_FAILED_INVALID_CONTEXT_NO_CURRENT_TAG
0x3401	TLVME_GET_TLV_OBJECT_FAILED_INVALID_TAG_CLASS
0x3402	TLVME_GET_TLV_OBJECT_FAILED_INVALID_LENGTH
0x3403	TLVME_GET_TLV_OBJECT_FAILED_TLV_LENGTH_NOT_SUPPORTED
0x3501	TLVME_GET_NEXT_ELEMENT_FAILED_INVALID_TAG_CLASS
0x3502	TLVME_GET_NEXT_ELEMENT_FAILED_TLV_LENGTH_NOT_SUPPORTED
0x3503	TLVME_GET_NEXT_ELEMENT_FAILED_INVALID_LENGTH
0x3504	TLVME_GET_NEXT_ELEMENT_FAILED_BUFFER_LENGTH_EXCEEDED
0x4101	DME_DATAMANAGER_INVALID_RECORD_NUMBER
0x4102	DME_DATAMANAGER_INVALID_RECORD_LENGTH
0x4103	DME_DATAMANAGER_RECORD_NOT_INITIALIZED
0x4104	DME_DATAMANAGER_RECORD_STORE_FULL
0x4105	DME_DATAMANAGER_INVALID_DATA_LENGTH
0x4106	DME_DATAMANAGER_INSUFFICIENT_BUFFER_SIZE
0x4201	DME_DATAMANAGER_PRIMARY_INDEX_NOT_ACTIVE
0x4202	DME_DATAMANAGER_PRIMARY_INDEX_KEY_NOT_SPECIFIED
0x4203	DME_DATAMANAGER_INVALID_PRIMARY_INDEX_KEY_LENGTH
0xA201	SUE_NO_INSTALL_PARAMETERS_FOUND
0xA202	SUE_INSUFFICIENT_APPLICATION_PARAMETER_BUFFER_LENGTH
0xA203	SUE_NO_APPLICATION_SPECIFIC_INSTALL_PARAMETERS_FOUND
0xD101	SSE_SECURITY_AUTHENTICATION_FAILED
0xD102	SSE_SECURITY_INVALID_CIPHER_DATA_LENGTH
0xD103	SSE_SECURITY_INVALID_KEY_DATA_LENGTH
0xD104	SSE_SECURITY_INVALID_DIVERSIFICATION_DATA_LENGTH
0xDC00	SSE_SECURITY_CRYPTO_EXCEPTION_UNDEFINED_REASON
0xDC01	SSE_SECURITY_CRYPTO_EXCEPTION_ILLEGAL_VALUE
0xDC02	SSE_SECURITY_CRYPTO_EXCEPTION_UNINITIALIZED_KEY
0xDC03	SSE_SECURITY_CRYPTO_EXCEPTION_NO_SUCH_ALGORITHM
0xDC04	SSE_SECURITY_CRYPTO_EXCEPTION_INVALID_INIT
0xDC05	SSE_SECURITY_CRYPTO_EXCEPTION_ILLEGAL_USE

Proprietary

Commerce Services

[0189] The following section provides a detailed description of the APDU commands available via the commerce applet 113.

APDU Commands

[0190] All communications/data exchanges with the commerce applet 113 will be performed via APDU commands as defined in the ISO 7816 standards. Additional restrictions and data handling are described below.

Command Usage Restrictions

[0191] For security reasons, a subset of the available commerce service commands can be restricted to specific connection modes. In one embodiment, referred to as "contact (wallet) mode," all of the APDU commands defined in Table 18 above are available. However, in contactless mode, the following commands are allowed:

- Get Version
- Get Internal Error Code
- Get Response (Remaining Data)
- Get Commerce Data

[0192] If any other APDU command is sent in contactless mode, an exception is thrown and the Internal Error Code is set to the corresponding invalid command mode value (0x0102).

[0193] In one embodiment, the Get Commerce Data command may only be successfully executed when wallet application 114 is open. When the wallet application 114 is either started or terminated by the consumer, it is the responsibility of the wallet application 114 to notify a wallet companion applet (WCAp) so that it can perform monitoring, management and/or security functions. The WCAp applet, in turn, notifies the commerce applet of the wallet application state via a shared interface. WCAp applets are discussed in U.S. Pat. Appln. No. 13/857,400 entitled "Systems, Methods, and Computer Program Products For Securing And Managing Applications On Secure Elements," which is hereby incorporated by reference in its entirety.

Data Payload Management

[0194] Commerce applet 113 validates that all required parameters have been included in the data payload. However, in most cases all non-relevant data elements can be ignored and a command will still process normally. In one

Draft Only

embodiment, the length expected (Le) value is not verified by the commerce applet 113. It can be assumed to be the value zero, allowing the commerce applet 113 to send all available data via the response.

Get Version

[0195] The Get Version command is used to obtain the version information of the currently loaded commerce applet 113. The version will be stored in three bytes (xx.yy.zz), where xx = release version, yy = major version (Wave) number, and zz = minor version number. This information is assigned by, for example, a MoCom platform system, specified during applet development or packaging, or stored as a static value within the code, and cannot be changed.

[0196] Table 28 defines the settings for the Get Version APDU command:

TABLE 28 – Internal Get Version

CLA	INS	P1	P2	Lc	Data	Le
90	10	00	00	00	*<none>*	3

[0197] In one embodiment, no data is sent to the commerce applet. The Lc data length is 0x00.

[0198] The version information is contained within a three-byte response. The Le data length is 0x03. A length of 0x00 is also allowed. Exemplary response data elements are defined in Table 29:

TABLE 29 – Response Data

Data Element	Byte Size	Value
Commerce Specification Version Tag	1	0xDF12
Commerce Specification Version Length	1	3
Commerce Specification Version Value	3	[Version (xx.yy.zz)]
Total:	5	

[0199] Table 30 defines the possible Status Word values that may be returned by this command.

TABLE 30 – Status Codes

SW1	SW2	Description

Draft Only

90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

Provision Applet

[0200] An applet provisional command, "Provision Applet," allows the provisioning (or update) of the consumer related data, including the consumer ID and optionally related security data (key value and certificates). The new/updated data values are specified via the command data. In an exemplary embodiment, the Provision Applet command may only be used to update the Consumer ID.

[0201] Tables 31 and 32 define the settings for the Provision Applet APDU command:

TABLE 31 – Provision Applet

CLA	INS	P1	P2	Lc	Data	Le
90	12	00	00	XX	TLV-Encoded Provisioning Data	00

[0202] The incoming data, illustrated in table 31, consists of the TLV encoded provisioning data. Therefore, the Lc data length is variable.

[0203] In one embodiment, no data is returned by the commerce applet 113. The Le data length is 0x00.

TABLE 32 – Command Data

Data Element	Byte Size	Value
Provisioning Data Element Tag	1	[Element Tag]
Element Data Length	1	xx
Element Data Value	xx	[Data]
.....		
Total:	<var>	

[0204] Table 33 defines the possible Status Word values that may be returned by Provision Applet command

TABLE 33 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
67	00	Wrong Data Length

Draft Only

69	09	Internal Error

Get Consumer Info

[0205] The Get Consumer Info command is used to obtain a subset of static data related to the token owner (*i.e.*, consumer). This data includes the following:

Consumer Identifier

[0206] Table 34 defines the settings for the Get Consumer Info APDU command:

TABLE 34 – Get Consumer Info

CLA	INS	P1	P2	Lc	Data	Le
90	14	00	00	00	*<none>*	00

[0207] No data is sent to the commerce applet 113. The Lc data length is, for example, 0x00. The actual length of the requested consumer information returned by the applet is variable, specific to the available consumer data. Therefore, the Le data length is 0x00, allowing the applet to manage a variable length response.

[0208] The response data is returned as a TLV formatted data steam. The Consumer ID may also be returned.

TABLE 35 – Response Data

Data Element	Byte Size	Value
Consumer ID Tag	1	0XDF21
Consumer ID Length	1	16
Consumer ID	16	[Consumer ID]
Total:	<var>	

[0209] Table 36 defines the possible Status Word values that may be returned by this command.

TABLE 36 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

Draft Only

Get Commerce Data

[0210] The Get Commerce Data command provides commerce information (*e.g.*, loyalty, offers and rewards) for a specified merchant (or set of merchants), based on the specified merchant/loyalty identifiers and supported offer types. This command provides a single point of contact for reader 120 attached to the merchant POS system (*e.g.*, POS terminal).

[0211] A date/time stamp, merchant ID, store ID, commerce protocol version, and merchant capabilities byte can be sent as part of the incoming data. Additional loyalty identifiers may also be sent in order to specify (filter) the loyalty information requested. The applet shall search a loyalty data table (Table 5), for the specified merchant/loyalty program ID(s) and retrieve the corresponding loyalty data. Additional offer type codes may be also sent as part of the incoming data in order to specify the type of offer information requested. The commerce applet 113 searches the cached merchant data table (Table 25) for the specified merchant identifier/offer code(s) and retrieves the corresponding offer data.

Required Parameters include:

- Date/Time Stamp
- Merchant ID
- Store ID
- App Version

[0212] Once transmission has been successfully completed, the applet shall create an entry in its transaction log recording the commerce data request.

[0213] Tables 37 and 38 define the settings for the Get Commerce Data APDU command:

TABLE 37 – Get Commerce Data

CLA	INS	P1	P2	Lc	Data	Le
90	50	00	00	xx		00

Draft Only

[0214] The incoming data consists of a date/time stamp (used for transaction logging), merchant identifier, store identifier, merchant capabilities byte, and an optional set of additional data elements, including one or more additional loyalty identifiers (indicating loyalty programs supported by the merchant location), and additional offer codes (indicating the type of offers supported by the merchant location). In one embodiment, if a merchant does not specify a Merchant Capability parameter, a default mode supporting only merchant based loyalty and offers is used.

[0215] The actual length of the requested commerce data returned by the applet is variable specific to the available loyalty/offers related data. Therefore, the Le data length is 0x00, allowing the applet to manage a variable length response.

TABLE 38 - Command Data

Data Element	Byte Size	Value
Date/Time Stamp Tag	1	0xDF11
Date/Time Stamp Length	1	7
Date/Time Stamp	7	[Date/Time Stamp]
Merchant ID Tag	1	0xDF31
Merchant ID Length	1	8
Merchant ID	8	[Merchant ID]
Store ID Tag	1	0x32
Store ID Length	1	32
Store ID	32	[Store ID]
Commerce Version Tag	1	0xDF12
Commerce Version Length	1	3
Commerce Version Data	2	[Commerce App Version]
Merchant Capability Tag	1	0xDF33
Merchant Capability Length	1	2
Merchant Capability Data	1	[Merchant Capability Code]
Transaction ID Tag	1	0xDF61
Transaction ID Length	1	16
Transaction ID	16	[Transaction ID]
Additional Loyalty ID Tag	1	0xDF41
Additional Loyalty ID Length	1	8
Additional Loyalty ID	8	[Loyalty ID]
.....		
Additional Offer Type Tag	1	0xDF54
Additional Offer Type Length	1	9
Additional Offer Type Code	9	[Offer Type Code]

Draft Only

.....		
Total:	<var>	

[0216] The response data is returned as a TLV formatted data steam. The MoCom platform-specific consumer identifier and all relevant loyalty/offers data are returned in a single data payload.

Consumer ID

[0217] The Consumer ID is sent in TLV format, where the data is sent using the tag CONSUMER_ID (0XDF21). In one embodiment, unless an error is detected, the consumer ID shall always be returned.

Loyalty

[0218] In one embodiment, each instance of loyalty data shall consist of the following TLV encoded data elements:

- Loyalty Identifier
- Loyalty Account Code

[0219] Within this data stream, the first tag shall contain the Loyalty Identifier tag (*T*) byte (0xDF41). The length (*L*) byte shall specify the length of the Loyalty Identifier. The value (*V*) shall contain the actual Loyalty Identifier of *L* length for the corresponding Loyalty Data that will immediately follow.

[0220] The second tag should contain the Loyalty Account Code tag (*T*) byte (0xDF43). The length (*L*) byte shall specify the total length of the account code data linked to the previous Loyalty Identifier. The value (*V*) shall contain the actual loyalty data of *L* length.

[0221] Any additional loyalty identifiers found within the loyalty data table are appended to the TLV encoded data payload using this same format.

Offers

[0222] Each instance of offer data shall consist of the following TLV encoded data elements:

- Offer ID
- Offer Code

Draft Only

[0223] Within this data stream, the first tag contains the Offer ID tag (*T*) byte (0xDF51). The length (*L*) byte specifies the length of the Offer ID. The value (*V*) contains the Offer ID for the corresponding offer data that will immediately follow.

[0224] The second tag preferably contains the Offer Code tag (*T*) byte value (0xDF53). The length (*L*) byte specifies the length of the Offer Type Code. The value (*V*) contains the Offer Code data for the corresponding Offer ID.

[0225] Any additional offer identifiers found within the offer data table are appended to the TLV encoded data payload using this same format. Exemplary response data is defined in Table 39.

TABLE 39 – Response Data

Data Element	Byte Size	Value
Consumer Identifier Tag	1	0XDF21
Consumer Identifier Length	1	16
Consumer Identifier	16	[Consumer ID]
Loyalty Identifier Tag	1	0xDF41
Identifier Length	1	8
Loyalty Identifier	8	[Loyalty ID]
Loyalty Account Code Tag	1	0xDF43
Account Code Length	1	32
Loyalty Account Code	32	[Acct Code]
.....		
Offer ID Tag	1	0xDF51
Offer ID Length	1	8
Offer ID Value	8	[Offer ID]
Offer Code Tag	1	0xDF53
Offer Code Length	1	130
Offer Code Value	130	[Offer Code]
.....		
Total:	<var>	

[0226] Commerce applet 113 manages the transmission of multiple response packets (using the Get Response command) when the total data length exceeds 256 bytes. Table 40 defines the possible Status Word values that may be returned by the Get Response command.

TABLE 40 – Status Codes

SW1	SW2	Description

Draft Only

90	00	Successful Execution of Command
61	00	Successful Execution of Command w/ Additional data available via Get Response
67	00	Wrong Data Length
69	09	Internal Error

Post Transaction Data

[0227] The Post Transaction Data command provides a method through which the Merchant PoS system or payment terminal may return post-transaction data, including redeemed coupons, new offers, e-receipts, or other enhanced commerce data.

[0228] Tables 41 and 42 define the settings for the Post Transaction Data APDU command:

TABLE 41 – Post Transaction Data

CLA	INS	P1	P2	Lc	Data	Le
90	52	00	00	xx	<TLV-Encoded Transaction Data>	00

[0229] The incoming data consists of the TLV encoded provisioning data and a platform signature for authenticity purposes. Therefore, the Lc data length is variable.

[0230] Data need not be returned by commerce applet 113. The Le data length is 0x00.

TABLE 42 – Command Data

Data Element	Byte Size	Value
Post Transaction Data Element Tag	1	[Element Tag]
Element Data Length	1	xx
Element Data Value	xx	[Data]
.....		
Total:	<var>	

[0231] Table 43 defines the possible Status Word values that may be returned by the Post Transaction Data command.

TABLE 43 – Status Codes

SW1	SW2	Description

Draft Only

90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

Get Transaction Log

[0232] The Get Transaction Log is used to obtain all data stored in the transaction log. This command is typically used by the commerce widget for the purpose of widget and secure element data synchronization tasks.

[0233] Table 44 defines the settings for the Get Transaction Log APDU command:

TABLE 44 – Get Transaction Log

CLA	INS	P1	P2	Lc	Data	Le
90	54	00	0x	00	*<none>*	

P2 Value	Applet Behavior
0x00	Normal processing.
0x01	Clear transaction log. No data transmitted.
0x02	Get Transaction Log Status

[0234] In one embodiment, no data is sent to the commerce applet. The Lc data length is 0x00. The actual length of the transaction data returned by the applet is variable, depending on the number of transaction records and the variable length of the corresponding transaction log data. Therefore, the Le data length can be 0x00, allowing commerce applet 113 to manage variable length response.

[0235] Preferably, response data is returned as a TLV formatted data steam.

Transaction Log Response Data

[0236] Each transaction log record shall consist of an Embedded-TLV Transaction Log tag followed by all related data elements. The data elements included in the transaction record are a mirror of those provided during the corresponding Get Commerce Data command requested by the Commerce-enabled payment terminal (NFC reader) at the merchant point-of-sale. Additional transaction log records are appended to the data using the same format. Table 45 illustrates exemplary response data.

Draft Only

TABLE 45 – Response Data

Data Element	Byte Size	Value
Embedded TLV Transaction Record Tag	1	0xDF60
Embedded TLV Transaction Record Length	3	xx
TLV-encoded transaction data	xx	xx
.....		
Total:	<var>	

[0237] In one embodiment, commerce applet 113 manages the transmission of multiple response packets using the Get Response command when the total data length exceeds 256 bytes.

Transaction Log Status Response Data

[0238] When the transaction log status is requested, the commerce applet responds with status information within an embedded TLV data payload. This data includes the number of available transaction log records, loyalty and offer records sent during the last transaction. This is the same data payload provided to WCAp via the shared interface. Table 46 illustrates exemplary response data.

TABLE 46 – Response Data

Data Element	Byte Size	Value
Embedded TLV Transaction Status Tag	1	0xE4
Embedded TLV Transaction Record Length	1	0x0C
Transaction Record Count Tag	1	0xDB
Transaction Record Count Length	1	0x02
Transaction Record Count Value	2	xx
Last Transaction Loyalty Count Tag	1	0xDC
Last Transaction Loyalty Count Length	1	0x02
Last Transaction Loyalty Count Value	2	xx
Last Transaction Offer Count Tag	1	0xDD
Last Transaction Offer Count Length	1	0x02
Last Transaction Offer Count Value	2	xx
Total:	14	

[0239] Table 47 defines possible Status Word values that may be returned by the Get Transaction Log command.

TABLE 47 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command

Draft Only

61	00	Successful Execution of Command w/ Additional data available via Get Response
67	00	Wrong Data Length
6B	00	Wrong P1/P2 Parameter
69	09	Internal Error

Get Internal Error Code

[0240] The Get Internal Error Code command is used to retrieve the last internal error code generated by the Commerce Services applet. This code provides a value that can be cross-referenced with the Internal Error Codes table (Table 26), providing a more specific description of the error. This command is used for more detailed diagnostic and error resolution.

[0241] Table 48 defines the settings for the Get Internal Error Code APDU command:

TABLE 48 – Get Internal Error Code

CLA	INS	P1	P2	Lc	Data	Le
90	70	00	00	00	*<none>*	02

[0242] In one embodiment, no data is sent to the applet. The Lc data length is 0x00. The error code is contained within a two-byte response. Therefore, the Le data length is 0x02.

[0243] The following table defines the possible Status Word values that may be returned by this command.

TABLE 49 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

Loyalty Services

Get Loyalty Data

[0244] The Get Loyalty Data command defined in Tables 50 and 51 is used to obtain the stored loyalty information based on a specified loyalty identifier. The

Draft Only

two-byte loyalty identifier may be sent as part of the incoming data in order to specify the loyalty information requested. Commerce applet 113 searches a table of loyalty data for the specified merchant/loyalty ID and retrieves all of the corresponding loyalty data.

TABLE 50 – Get Loyalty Data

CLA	INS	P1	P2	Lc	Data	Le
90	30	00	00	xx	[TLV-Encoded Loyalty ID]	00

[0245] The (optional) incoming data shall consist of a TLV encoded loyalty identifier indicating the loyalty information requested. If Lc is set to 0x00 (no data incoming data is specified), all available loyalty identifiers are returned.

[0246] The actual length of the requested loyalty data returned by the applet is variable specific to the requested/available loyalty data. Therefore, the Le data length is 0x00, allowing the applet to manage a variable length response.

TABLE 51 - Command Data

Data Element	Byte Size	Value
Loyalty Identifier Tag	1	0xDF41
Loyalty Identifier Length	1	8
Loyalty Identifier	8	[Loyalty ID]
Total:	<var>	

[0247] The response data (Table 51) is returned as a TLV formatted data stream. All of the relevant loyalty data is returned in a single data payload.

[0248] In one embodiment, if a loyalty data dump is requested (Lc = 0x00), a list of all Loyalty Identifiers is returned in LV (no tag) format. Thus, only the Loyalty Identifier for each entry is included in the data payload.

[0249] Each instance of loyalty data includes the following data elements:

- Loyalty Identifier
- Loyalty Account Code

TABLE 52 – Response Data

Data Element	Byte Size	Value
Loyalty Identifier Tag	1	0xDF41

Draft Only

Identifier Length	1	8
Loyalty Identifier	8	[Loyalty ID]
Loyalty Account Code Tag	1	0xDF43
Account Code Length	1	xx
Loyalty Account Code	xx	[Acct Code]
Total (Max):	<var>	

[0250] Table 53 defines the possible Status Word values that may be returned by this command.

TABLE 53 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
61	00	Successful Execution of Command w/ Additional data available via Get Response
67	00	Wrong Data Length
69	09	Internal Error

Update Loyalty Data

[0251] The Update Loyalty Data command is used to add or update the specified merchant loyalty data. The data is sent as TLV formatted data stream. If the specified loyalty identifier exists, the corresponding loyalty data elements are updated. If the loyalty identifier does not exist, a new data record is created in the loyalty data table. Tables 54 and 55 define the settings for the Update Loyalty Data APDU command:

TABLE 54 – Update Loyalty Data

CLA	INS	P1	P2	Lc	Data	Le
90	32	00	00	xx	TLV-Encoded Loyalty Data	00

[0252] The incoming data shall consist of TLV encoded loyalty data. Therefore, the Lc data length is variable. In one embodiment, no data is returned by the applet. The Le data length is be 0x00.

TABLE 55 – Command Data

Data Element	Byte Size	Value
Loyalty Identifier Tag	1	0xDF41
Identifier Length	1	8

Draft Only

Loyalty Identifier	8	[Loyalty ID]
Loyalty Account Code Tag	1	0xDF43
Account Code Length	1	xx
Loyalty Account Code	Xx	[Acct Code]
Total:	<var>	

[0253] Table 56 defines the possible Status Word values that may be returned by this command.

TABLE 56 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

Delete Loyalty Data

[0254] The Delete Loyalty Data command is used to delete the specified merchant loyalty data. The one-byte merchant code is specified via the command data. Alternatively, the P2 byte may be used to purge all existing offers. If P2 is set to 0xFF, the entire offer data store is deleted.

[0255] Tables 57 and 58 define the settings for the Delete Loyalty Data APDU command:

TABLE 57 – Delete Loyalty Data

CLA	INS	P1	P2	Lc	Data	Le
90	34	00	xx	xx	TLV-Encoded Loyalty ID	00

[0256] The incoming data consists of a TLV-encoded loyalty identifier. Therefore, the Lc data length is variable.

[0257] In one embodiment, no data is returned by commerce applet 113. The Le data length is 0x00.

TABLE 58 – Command Data

Data Element	Byte Size	Value
Loyalty Identifier Tag	1	0xDF41
Loyalty Identifier Length	1	xx
Loyalty Identifier	Xx	[Loyalty ID]
Total:	<var>	

Draft Only

P2 Value	Applet Behavior
0x00	Normal processing.
0xFF	Purge loyalty table (delete all records)

[0258] Table 59 defines the possible Status Word values that may be returned by the Delete Loyalty Data command.

TABLE 59 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

Merchant Cached Data Services

Get Cached Merchant Data

[0259] The Get Cached Merchant Data command is used to obtain all previously loaded data pertaining to a specific merchant. The merchant identifier may be sent as part of the incoming data in order to specify the pre-loaded data requested. If provided, the commerce applet searches a table of cached merchant data for the specified merchant ID and retrieves all of the corresponding data. This command may also be used to obtain information on all cached merchants stored within the Commerce Services applet.

[0260] Table 60 defines the settings for the Get Cached Merchant Data APDU command:

TABLE 60 – Get Cached Merchant Data

CLA	INS	P1	P2	Lc	Data	Le
90	56	00	00	xx	<none>	00

[0261] In one embodiment, no data is sent to the applet. The Lc data length is 0x00. The actual length of the requested cached merchant data returned by the applet is variable, specific to the requested/available cached merchant data. Therefore, the Le data length is 0x00; allowing the applet to manage a variable length response.

Draft Only

[0262] The response data (Table 61) may be returned as a TLV formatted data stream. All of the cached data is returned in a single data payload. Each instance of cached merchant data includes the following corresponding cached merchant data elements (if available):

- Merchant Identifier
- Loyalty Identifier
- Loyalty Account Code
- Offer Identifier(s)
- Offer Code(s)

TABLE 61 – Response Data

Data Element	Byte Size	Value
Merchant ID Tag	1	0xDF31
Merchant ID Length	1	8
Merchant ID	8	[Merchant ID]
Loyalty ID Tag	1	0xDF41
Loyalty ID Length	1	8
Loyalty ID Value	8	[Loyalty ID]
Loyalty Account Code Tag	1	0xDF43
Loyalty Account Code Length	1	32
Loyalty Account Code Value	32	[Loyalty Account Code]
.....		
Offer ID Tag	1	0xDF51
Offer ID Length	1	xx
Offer ID Value	Xx	[Offer ID]
Offer Code Tag	1	0xDF53
Offer Code Length	1	xx
Offer Code Value	Xx	[Offer Code]
.....		
Total:	<var>	

[0263] In an exemplary embodiment, the cached merchant data will be loaded/managed by the wallet application and may include multiple offer IDs/codes pertaining to that specific merchant. However, the applet shall prefix the consumer identifier to the response data and append any additional loyalty/offer data requested by the Get Commerce Data command.

[0264] Table 62 defines the possible Status Word values that may be returned by this command.

Draft Only

TABLE 62 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

Update Cached Merchant Data

[0265] The Update Cached Merchant Data command is used to update the cached (quick-response) data for a specified merchant. The data is sent as TLV formatted data stream, similar to the response data returned by the Get Commerce Data command. This command is used to pre-load a given merchant's Get Commerce Data response.

[0266] Tables 63 and 64 define the settings for the Update Cached Merchant Data APDU command:

TABLE 63 – Update Cached Merchant Data

CLA	INS	P1	P2	Lc	Data	Le
90	58	00	0x	xx	TLV-Encoded Cached Merchant Data]	02

P2 Value	Applet Behavior
0x00	Normal processing.
0x01	APDU Chain (data will be appended to CMD buffer)
0Xff	Delete cached merchant data [Lc = 0]

[0267] The incoming data consists of embedded TLV encoded cached merchant data. Therefore, the Lc data length is variable.

[0268] Commerce applet returns a two byte response containing the number of available bytes remaining in the cached merchant data buffer. Therefore, the Le data length is 0x02 (or 0x00).

Draft Only

TABLE 64 – Command Data

Data Element	Byte Size	Value
Merchant ID Tag	1	0xDF31
Merchant ID Length	1	8
Merchant ID Value	8	[Merchant ID]
Cached Merchant Data Offer Count Tag	1	0x57
Cached Merchant Data Offer Count Length	1	1
Cached Merchant Data Offer Count Value	1	[CMD Offer Count]
Embedded TLV Cached Merchant Data Tag	1	0x58
Embedded TLV Cached Merchant Data Length	Xx	xx
Offer ID Tag	1	0xDF51
Offer ID Length	1	xx
Offer ID Value	Xx	[Offer ID]
Offer Code Tag	1	0xDF53
Offer Code Length	1	xx
Offer Code Value	Xx	[Offer Code]
.....		
Total:	<var>	

[0269] The response data (Table 65) returned by the command consists of a 2-byte (short) value representing the number of remaining bytes available in the cached merchant data buffer. This allows the wallet application 114 to manage how many cached offers can "fit" into the Commerce Services applet.

TABLE 65 – Response Data

Data Element	Byte Size	Value
Available Cached Merchant Data Buffer (bytes) Size	2	xx
Total:	2	

[0270] Table 66 defines the possible Status Word values that may be returned by this command.

TABLE 66 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

Draft Only

[0271] Table 67 defines the data elements and corresponding tag values and target/max byte sizes used by commerce based applications according to the example aspects described herein. Additional values have been provided for those elements with a limited/fixed value range.

TABLE 67

Commerce Services			
Shared Data Elements			
Data Element	Tag	Max Size	Description
DATE_TIME_STAMP	0x11	7	Date/Time stamp
COMMERCE_APP_VERSION	0x12	3	Supported Commerce App Version Number
Consumer Data Elements			
Data Element	Tag	Max Size	Description
CONSUMER_ID	0x21	16	MoCom Platform specific consumer identifier
CONSUMER_KEY	0x22	16	MoCom Platform generated consumer specific 3DES key
CONSUMER_CERT	0x23	8	MoCom Platform generated consumer signature/ certificate
Merchant Data Elements			
Data Element	Tag	Max Size	Description
MERCHANT_ID	0x31	8	MoCom Platform specific merchant identifier
MERCHANT_STORE_ID	0x32	32	MoCom Platform specific merchant store identifier
MERCHANT_CAPABILITY	0x33	2	Supported Commerce App Services
READER_START_MODE	0x34	2	NFC enabled payment terminal startup mode (provided by Merchant POS System during init)
Merchant Capabilities			
Data Element	Value	Max Size	Description
MERCAP_MERCHANT_LOYALTY	0x80	1	The Get Commerce Data includes a valid merchant identifier used to determine the Loyalty data received by the applet.
MERCAP_ADDITIONAL	0x40	1	The Get Commerce Data request

Draft Only

LOYALTY			includes additional Loyalty Identifiers. Additional Loyalty data is determined by the specified Loyalty ID(s).
MERCAP_MERCHANT_ OFFERS	0x20	1	Offer type fields aincluded in Get Commerce Data request
MERCAP_ADDITIONAL_ OFFERS	0x10	1	The Get Commerce Data includes a valid merchant identifier used to determine the offers data received by the applet.
MERCAP_PAYMENT	0x08	1	Merchant supports contactless payment.
MERCAP_CLOUD	0x02	1	The merchant supports cloud redemption. Only the Consumer ID will be returned by the applet for resolution in the cloud.
MERCAP_REDEMPTION	0x01	1	The Merchant & Payment Terminal support the transmission of offer redemption data (from the ECR) to the applet via the Post Transaction command.
MoCom Platform Data Elements			
PLATFORM_SIGNATURE	0x71	8	MoCom Platform generated MAC/Signature appended to command/data originating from the platform for remote verification purposes (data integrity/ authenticity).
PLATFORM_KEY	0x72	16	MoCom Platform Key
PLATFORM_CERT	0x73	8	MoCom Platform Certificate

Loyalty			
Loyalty Data Elements			
Data Element	Tag	Max Size	Description
EMBEDDED_TLV_ LOYALTY_DATA	0x40	xx	Embedded TLV loyalty data tag
LOYALTY_ID	0x41	8	MoCom Platform specific loyalty identifier
LOYALTY_STATUS	0x42	1	Loyalty card/account status (see below)
LOYALTY_ACCOUNT_ CODE	0x43	32	Loyalty account (barcode data)
LOYALTY_MAC_ SIGNATURE	0x44	8	MoCom Platform specific MAC/Signature for integrity/

Draft Only

			authenticity verification
Loyalty Status			
Data Element	Value	Max Size	Description
LOYALTY_STATUS_ DEACTIVATED	0x00	1	Loyalty account inactive. Not available.
LOYALTY_STATUS_ ACTIVE	0x01	1	Loyalty account active. Available for use.

Transaction Log			
Transaction Data Elements			
Data Element	Tag	Max Size	Description
EMBEDDED_TLV_ TRANSACTION_LOG	0x60	xx	Transaction log record data tag
TRANSACTION_ID	0x61	16	Transaction ID (assigned by ECR)
TRANSACTION_STATUS	0x62	11	Transaction status; including status byte (see below), 2-byte status word, 2-byte internal error code, 2-byte number of available transaction records, 2-byte last transaction loyalty count, 2-byte last transaction offer count
Transaction Status			
Data Element	Value	Max Size	Description
TRANSACTION_STATUS_SUCCESSFUL	0x00	1	Commerce data received. Result pending.
TRANSACTION_STATUS_FAILED	0x01	1	Error detected. Internal error code appended.

Offers			
Offer Data Elements			
Data Element	Tag	Max Size	Description
EMBEDDED_TLV_ OFFER_DATA	0x50	xx	Embedded TLV offer data tag
OFFER_ID	0x51	8	MoCom Platform specific offer identifier
OFFER_STATUS	0x52	1	Offer status (see below)
OFFER_CODE	0x53	48	Offer (UPC/EPC/GS1 Databar) barcode data
OFFER_TYPE_CODE	0x54	9	Offer Type (see below)
OFFER_MAC_ SIGNATURE	0x55	8	MoCom Platform specific data security signature

Draft Only

OFFER_UPDATE_FLAG	0x56	1	Update flag (synchronization status)
CACHED_MERCHANT_DATA_OFFER_COUNT	0x57	1	Offer Count within Cached Merchant Data
EMBEDDED_TLV_CACHED_MERCHANT_DATA	0x58	xx	Embedded TLV Cached Merchant (Offer) Data

Offer Status			
Data Element	Value	Max Size	Description
OFFER_STATUS_DEACTIVATED	0x00	1	Offer present in data store, but not available for redemption.
OFFER_STATUS_ACTIVE	0x01	1	Offer present in data store. Available for redemption.
OFFER_STATUS_EXPIRED	0x10	1	Expired Offer
OFFER_STATUS_SUBMITTED	0x20	1	Offer has been presented for redemption. Result pending.
OFFER_STATUS_REDEEMED	0x40	1	Offer has been redeemed.

Offer Type			
Data Element	Value	Max Size	Description
OFFER_TYPE_CLASS_01	0x01	1	Offer Class: Merchant Specific (merchant ID appended)
OFFER_TYPE_CLASS_02	0x02	1	Offer Class: CPG
OFFER_TYPE_CLASS_03	0x03	1	Offer Class: Misc

Draft Only

Specially Formatted Data Elements

[0272] A few of the data elements included in the commerce data payload include a format byte that identifies the data encoding used for that element. The data encoding is specified by the merchant to ensure compatibility at the point of sale. The formatted data value is supplied by the MoCom platform to the wallet application. Thus, no additional interpreting/formatting is necessary between the platform, wallet, secure element, and payment terminal. It is the role of the payment terminal (or merchant POS system) to properly interpret the data and supply it to the merchant system for processing.

[0273] The following data elements shall include the format byte:

- Loyalty Account Code
- Offer Code

[0274] Table 68 defines the possible format byte values and their corresponding encoding rule:

TABLE 68

Format Byte	Encoding Rule	Description
0x00	Hexadecimal	Each byte of data is encoded in (raw) hexadecimal format.
0x01	Binary Coded Decimal (BCD)	Each nibble represents a single digit. Thus, only decimal values are specified. A data stream containing an odd number (length) of digits includes the hex value 'F' in the first nibble of the data stream.
0x02	ASCII	Each byte represents an ACII value that is interpreted as such and handled as its corresponding CHAR value. In most cases, these data streams will be converted into a String before being passed to the merchant POS system for processing.

[0275] A BCD encoded data value that includes the hexadecimal value 'F' in the first nibble shall identify a data stream containing an odd number of digits. Thus, the BCD data stream *12345* is encoded in 3 byte buffer as follows: *0xF12345*.

Computer Readable Medium Implementation

[0276] The example embodiments described above such as, for example, the systems and procedures depicted in or discussed in connection with FIGs. 1- 7 or any part or function thereof, may be implemented by using hardware, software or a combination of the two. The implementation may be in one or more computers or other processing systems. While manipulations performed by these example embodiments may have been referred to in terms commonly associated with mental operations performed by a human operator, no human operator is needed to perform any of the operations described herein. In other words, the operations may be completely implemented with machine operations. Useful machines for performing the operation of the example embodiments presented herein include general purpose digital computers or similar devices.

Draft Only

[0277] FIG. 8 is a block diagram of a general and/or special purpose computer 800, in accordance with some of the example embodiments of the invention. The computer 800 may be, for example, a user device, a user computer, a client computer and/or a server computer, among other things.

[0278] The computer 800 may include without limitation a processor device 810, a main memory 825, and an interconnect bus 805. The processor device 810 may include without limitation a single microprocessor, or may include a plurality of microprocessors for configuring the computer 800 as a multi-processor system. The main memory 825 stores, among other things, instructions and/or data for execution by the processor device 810. The main memory 625 may include banks of dynamic random access memory (DRAM), as well as cache memory.

[0279] The computer 800 may further include a mass storage device 830, peripheral device(s) 840, portable storage medium device(s) 850, input control device(s) 880, a graphics subsystem 860, and/or an output display 870. For explanatory purposes, all components in the computer 800 are shown in FIG. 8 as being coupled via the bus 805. However, the computer 800 is not so limited. Devices of the computer 800 may be coupled via one or more data transport means. For example, the processor device 810 and/or the main memory 825 may be coupled via a local microprocessor bus. The mass storage device 830, peripheral device(s) 840, portable storage medium device(s) 850, and/or graphics subsystem 860 may be coupled via one or more input/output (I/O) buses. The mass storage device 830 may be a nonvolatile storage device for storing data and/or instructions for use by the processor device 810. The mass storage device 830 may be implemented, for example, with a magnetic disk drive or an optical disk drive. In a software embodiment, the mass storage device 830 is configured for loading contents of the mass storage device 830 into the main memory 825.

[0280] The portable storage medium device 850 operates in conjunction with a nonvolatile portable storage medium, such as, for example, a compact disc read only memory (CD-ROM), to input and output data and code to and from the computer 800. In some embodiments, the software for storing an internal identifier in metadata may be stored on a portable storage medium, and may be inputted into the computer 800 via the portable storage medium device 850. The

Draft Only

peripheral device(s) 840 may include any type of computer support device, such as, for example, an input/output (I/O) interface configured to add additional functionality to the computer 800. For example, the peripheral device(s) 840 may include a network interface card for interfacing the computer 800 with a network 820.

[0281] The input control device(s) 880 provide a portion of the user interface for a user of the computer 800. The input control device(s) 880 may include a keypad and/or a cursor control device. The keypad may be configured for inputting alphanumeric characters and/or other key information. The cursor control device may include, for example, a mouse, a trackball, a stylus, and/or cursor direction keys. In order to display textual and graphical information, the computer 800 may include the graphics subsystem 860 and the output display 870. The output display 870 may include a cathode ray tube (CRT) display and/or a liquid crystal display (LCD). The graphics subsystem 860 receives textual and graphical information, and processes the information for output to the output display 870.

[0282] Each component of the computer 800 may represent a broad category of a computer component of a general and/or special purpose computer. Components of the computer 800 are not limited to the specific implementations provided here.

[0283] Portions of the example embodiments of the invention may be conveniently implemented by using a conventional general purpose computer, a specialized digital computer and/or a microprocessor programmed according to the teachings of the present disclosure, as is apparent to those skilled in the computer art. Appropriate software coding may readily be prepared by skilled programmers based on the teachings of the present disclosure.

[0284] Some embodiments may also be implemented by the preparation of application-specific integrated circuits, field programmable gate arrays, or by interconnecting an appropriate network of conventional component circuits.

[0285] Some embodiments include a computer program product. The computer program product may be a storage medium or media having instructions stored thereon or therein which can be used to control, or cause, a computer to perform

Draft Only

any of the procedures of the example embodiments of the invention. The storage medium may include without limitation a floppy disk, a mini disk, an optical disc, a Blu-Ray Disc, a DVD, a CD-ROM, a micro-drive, a magneto-optical disk, a ROM, a RAM, an EPROM, an EEPROM, a DRAM, a VRAM, a flash memory, a flash card, a magnetic card, an optical card, nanosystems, a molecular memory integrated circuit, a RAID, remote data storage/archive/warehousing, and/or any other type of device suitable for storing instructions and/or data.

[0286] Stored on any one of the computer readable medium or media, some implementations include software for controlling both the hardware of the general and/or special computer or microprocessor, and for enabling the computer or microprocessor to interact with a human user or other mechanism utilizing the results of the example embodiments of the invention. Such software may include without limitation device drivers, operating systems, and user applications. Ultimately, such computer readable media further includes software for performing example aspects of the invention, as described above.

[0287] Included in the programming and/or software of the general and/or special purpose computer or microprocessor are software modules for implementing the procedures described above.

[0288] While various example embodiments of the invention have been described above, it should be understood that they have been presented by way of example, and not limitation. It is apparent to persons skilled in the relevant art(s) that various changes in form and detail can be made therein. Thus, the invention should not be limited by any of the above described example embodiments, but should be defined only in accordance with the following claims and their equivalents.

[0289] In addition, it should be understood that the figures are presented for example purposes only. The architecture of the example embodiments presented herein is sufficiently flexible and configurable, such that it may be utilized and navigated in ways other than that shown in the accompanying figures.

[0290] Further, the purpose of the Abstract is to enable the U.S. Patent and Trademark Office and the public generally, and especially the scientists, engineers and practitioners in the art who are not familiar with patent or legal

Draft Only

terms or phraseology, to determine quickly from a cursory inspection the nature and essence of the technical disclosure of the application. The Abstract is not intended to be limiting as to the scope of the example embodiments presented herein in any way. It is also to be understood that the procedures recited in the claims need not be performed in the order presented.

Draft Only

WHAT IS CLAIMED IS

1. A system for managing contactless transactions, comprising:

at least one memory operable to store commerce data and financial instrument data;

at least one processor coupled to the at least one memory, the one or more processors being operable to:

perform a first tap, the first tap occurring when the system is placed within a predetermined proximity to a payment terminal;

receive from the payment terminal a first select command including an application identifier (AID) corresponding to a first application;

transmit to the payment terminal a first response based on the first select command;

receive from the payment terminal a data request including information indicating supported data types; and

transmit to the payment terminal a second response based on the data request, the second response including transaction data;

wherein the transaction data includes at least a portion of the commerce data stored in the at least one memory.

2. The system of Claim 1, the at least one processor being further operable to:

receive from the payment terminal a payment AID request;

transmit to the payment terminal the AID corresponding to a second application;

receive from the payment terminal a second select command including the AID corresponding to the second application;

transmit to the payment terminal file control information (FCI) corresponding to the second application; and

transmit payment data to the payment terminal;

wherein the payment data includes at least a portion of the financial instrument data stored in the at least one memory.

Draft Only

3. The system of Claim 1 or Claim 2, the at least one processor being further operable to perform a second tap, the second tap occurring when the system is placed within a predetermined proximity to the payment terminal.

4. The system of Claim 1 or Claim 2, the at least one processor being further operable to perform a second tap, the second tap occurring when the system is placed within a predetermined proximity to the payment terminal,

wherein the first tap and the second tap occur in response to a first tap request and a second tap request, respectively, received from the payment terminal.

5. The system of Claim 1, the at least one processor being further operable to:

perform a second tap, the second tap occurring when the system is placed within a predetermined proximity to the payment terminal,

receive from the payment terminal a payment AID request;

transmit to the payment terminal the AID corresponding to a second application;

receive from the payment terminal a second select command including the AID corresponding to the second application;

transmit to the payment terminal file control information (FCI) corresponding to the second application;

transmit payment data to the payment terminal, the payment data including at least a portion of the financial instrument data stored in the at least one memory;

receive from the payment terminal a third select command including an AID corresponding to the first application;

transmit to the payment terminal a third response based on the third select command;

receive from the payment terminal post-transaction data; and

transmit to the payment terminal a fourth response based on the post-transaction data.

6. The system of Claim 1, wherein the payment terminal comprises a contactless reader and/or a point of sale terminal.

Draft Only

7. A method for managing contactless transactions, the method comprising steps of:

performing a first tap, the first tap occurring when a mobile device is placed within a predetermined proximity to a payment terminal;

receiving from the payment terminal a first select command including an application identifier (AID) corresponding to a first application;

transmitting to the payment terminal a first response based on the first select command;

receiving from the payment terminal a data request including information indicating supported data types; and

transmitting to the payment terminal a second response based on the data request, the second response including transaction data;

wherein the transaction data includes at least a portion of commerce data stored in at least one memory.

8. The method of Claim 7, further comprising steps of:

receiving from the payment terminal a payment AID request;

transmitting to the payment terminal the AID corresponding to a second application;

receiving from the payment terminal a second select command including the AID corresponding to the second application;

transmitting to the payment terminal file control information (FCI) corresponding to the second application; and

transmitting payment data to the payment terminal;

wherein the payment data includes at least a portion of the financial instrument data stored in the at least one memory.

9. The method of Claim 7 or Claim 8, further comprising a step of performing a second tap, the second tap occurring when the mobile device is placed within a predetermined proximity to the payment terminal.

Draft Only

10. The method of Claim 7 or Claim 8, further comprising a step of performing a second tap, the second tap occurring when the mobile device is placed within a predetermined proximity to the payment terminal,

wherein the first tap and the second tap occur in response to a first tap request and a second tap request, respectively, received from the payment terminal.

11. The method of Claim 7, further comprising steps of:

performing a second tap, the second tap occurring when the mobile device is placed within a predetermined proximity to the payment terminal;

receiving from the payment terminal a payment AID request;

transmitting to the payment terminal the AID corresponding to a second application;

receiving from the payment terminal a second select command including the AID corresponding to the second application;

transmitting to the payment terminal file control information (FCI) corresponding to the second application;

transmitting payment data to the payment terminal, the payment data including at least a portion of the financial instrument data stored in the at least one memory;

receiving from the payment terminal a third select command including an AID corresponding to the first application;

transmitting to the payment terminal a third response based on the third select command;

receiving from the payment terminal post-transaction data; and

transmitting to the payment terminal a fourth response based on the post-transaction data.

12. The method of Claim 7, wherein the payment terminal comprises a contactless reader and/or a point of sale terminal.

13. A non-transitory computer-readable medium having stored thereon sequences of instructions for causing one or more processors to:

Draft Only

perform a first tap, the first tap occurring when a mobile device is placed within a predetermined proximity to a payment terminal;

receive from the payment terminal a first select command including an application identifier (AID) corresponding to a first application;

transmit to the payment terminal a first response based on the first select command;

receive from the payment terminal a data request including information indicating supported data types; and

transmit to the payment terminal a second response based on the data request, the second response including transaction data;

wherein the transaction data includes at least a portion of commerce data stored in at least one memory.

14. The computer-readable medium of Claim 13, having stored thereon sequences of instructions for further causing the one or more processors to:

receive from the payment terminal a payment AID request;

transmit to the payment terminal the AID corresponding to a second application;

receive from the payment terminal a second select command including the AID corresponding to the second application;

transmit to the payment terminal file control information (FCI) corresponding to the second application; and

transmit payment data to the payment terminal;

wherein the payment data includes at least a portion of the financial instrument data stored in the at least one memory.

15. The computer-readable medium of Claim 13 or Claim 14, the one or more processors being further operable to perform a second tap, the second tap occurring when the mobile device is placed within a predetermined proximity to the payment terminal.

Draft Only

16. The computer-readable medium of Claim 13, the one or more processors being further operable to perform a second tap, the second tap occurring when the mobile device is placed within a predetermined proximity to the payment terminal,

wherein the first tap and the second tap occur in response to a first tap request and a second tap request, respectively, received from the payment terminal.

17. The computer-readable medium of Claim 13, having stored thereon sequences of instructions for further causing the one or more processors to:

perform a second tap, the second tap occurring when the mobile device is placed within a predetermined proximity to the payment terminal,

receive from the payment terminal a payment AID request;

transmit to the payment terminal the AID corresponding to a second application;

receive from the payment terminal a second select command including the AID corresponding to the second application;

transmit to the payment terminal file control information (FCI) corresponding to the second application;

transmit payment data to the payment terminal, the payment data including at least a portion of the financial instrument data stored in the at least one memory;

receive from the payment terminal a third select command including an AID corresponding to the first application;

transmit to the payment terminal a third response based on the third select command;

receive from the payment terminal post-transaction data; and

transmit to the payment terminal a fourth response based on the post-transaction data.

18. The computer-readable medium of Claim 13, wherein the payment terminal comprises a contactless reader and/or a point of sale terminal.

Draft Only

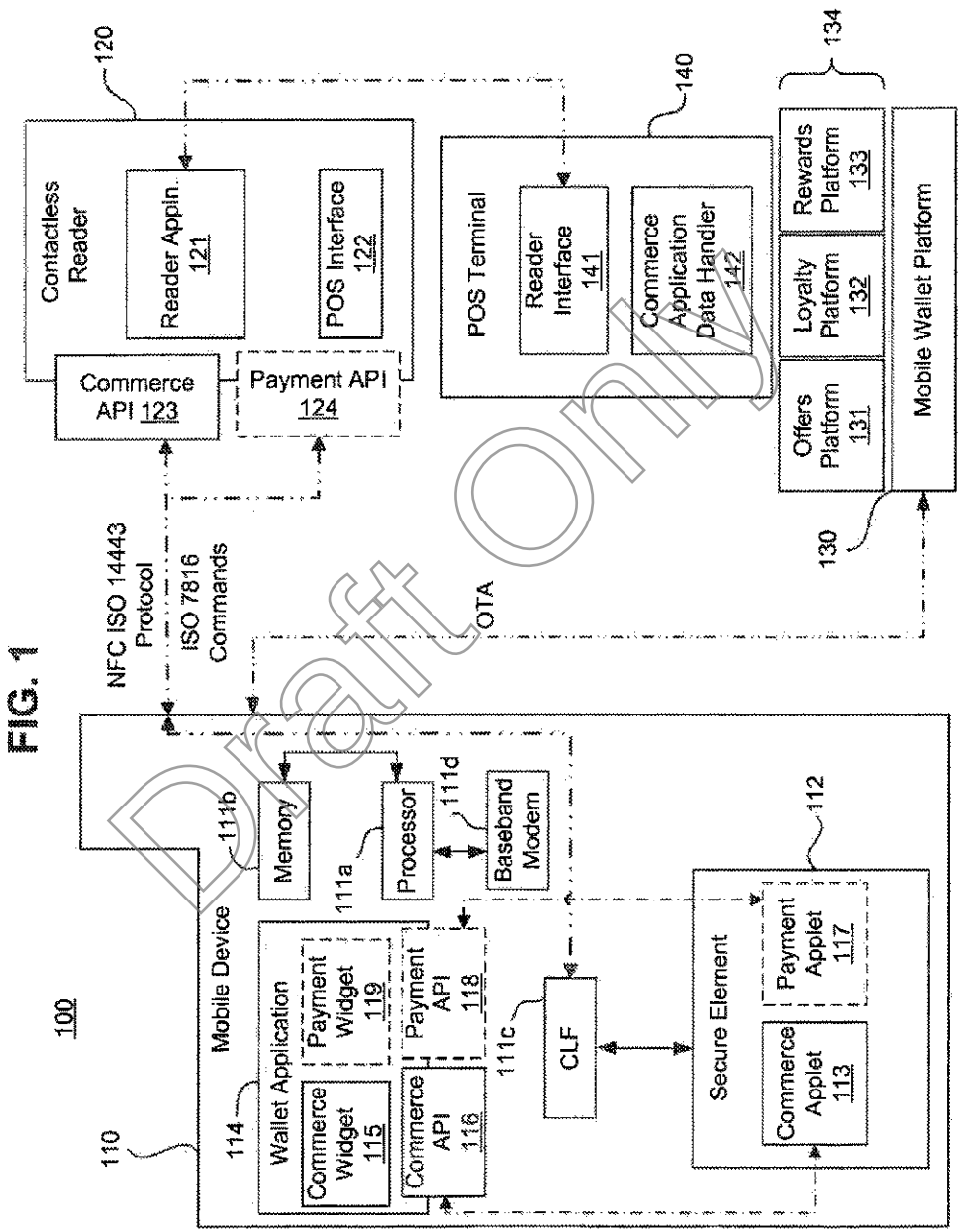


FIG. 1

Draft Only

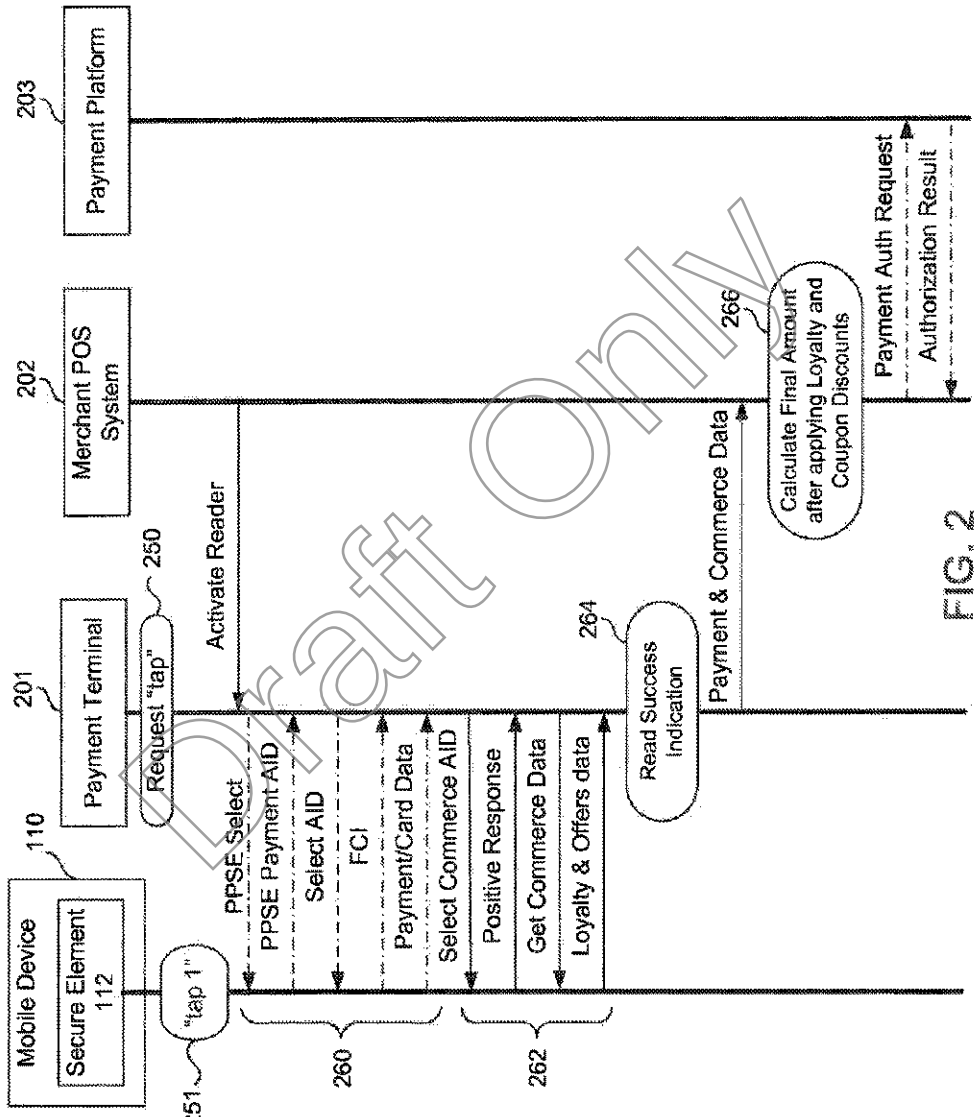


FIG. 2

Draft Only

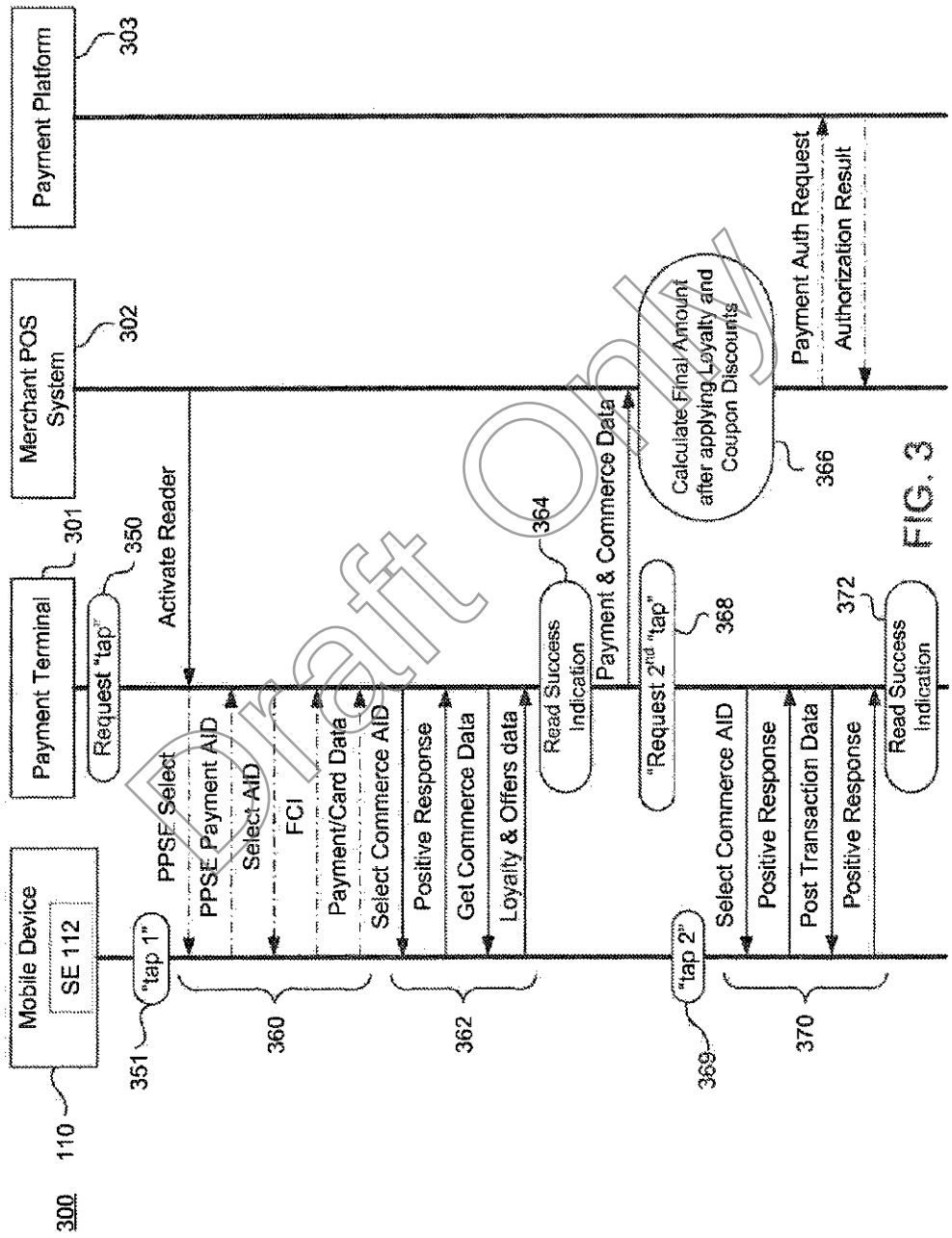


FIG. 3

Draft Only

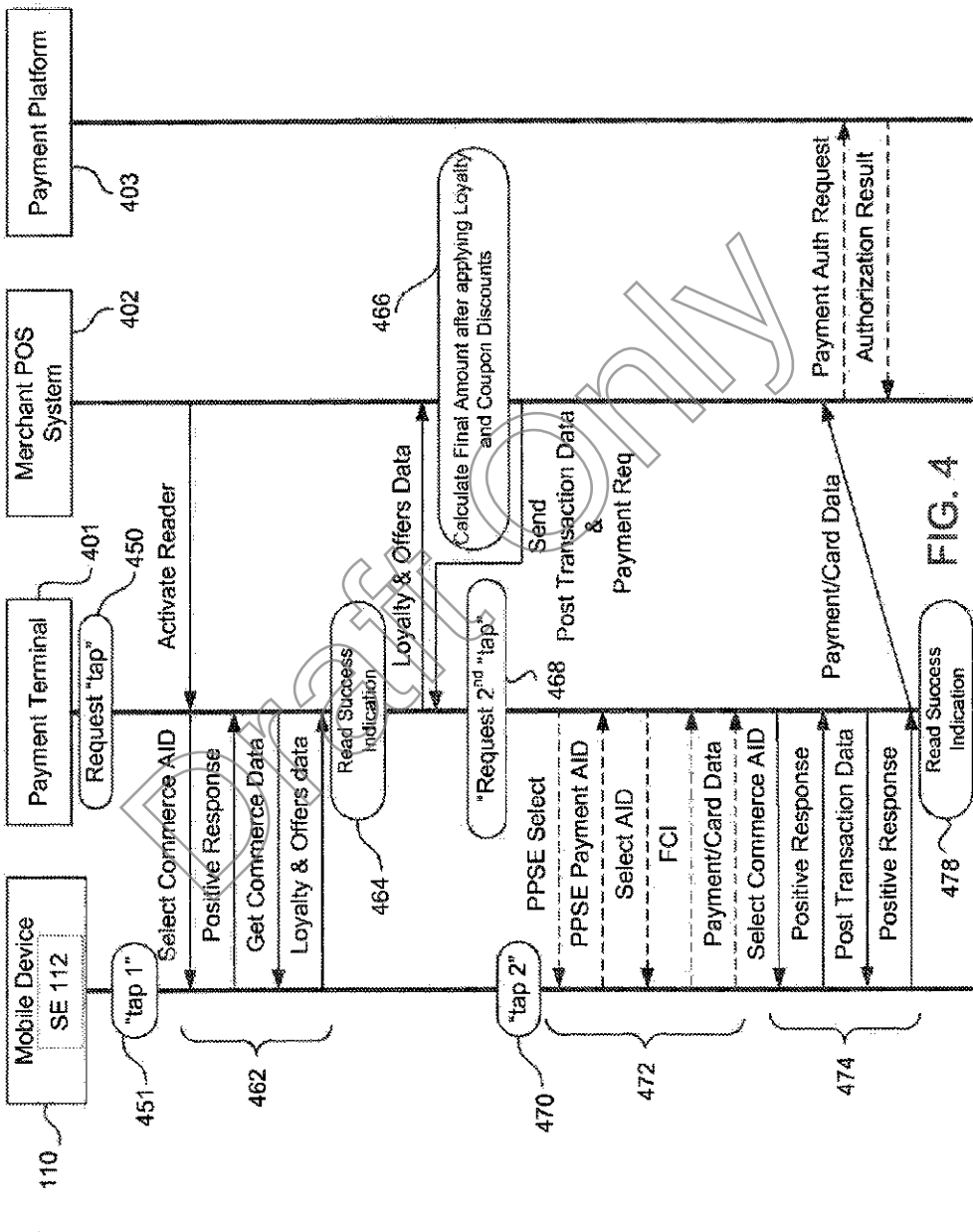
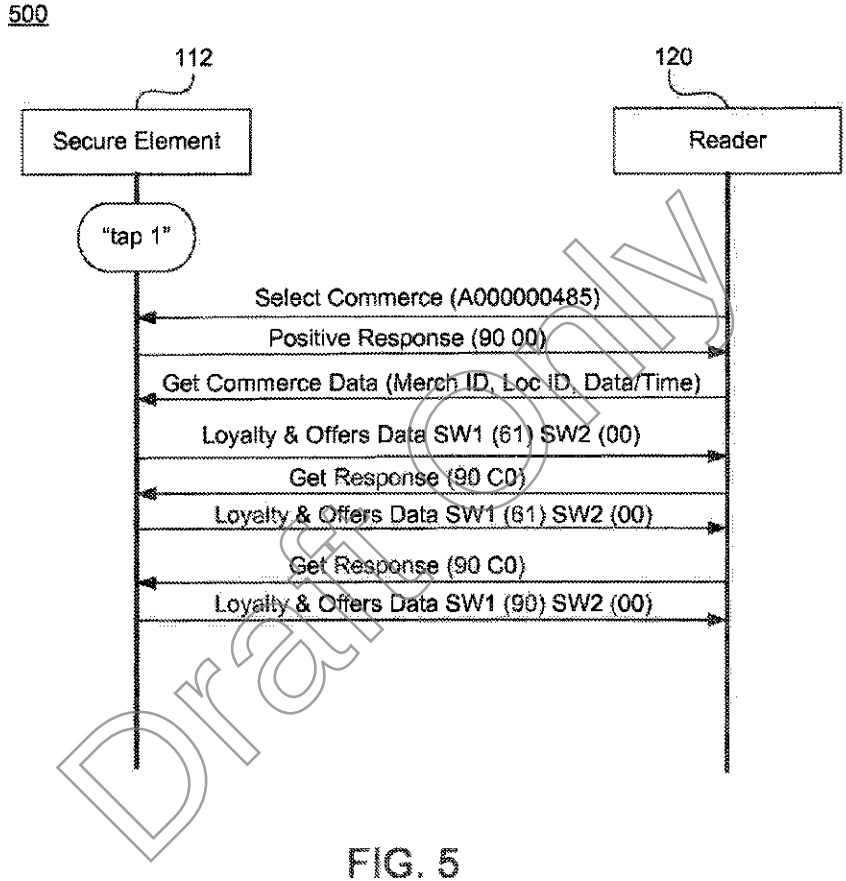


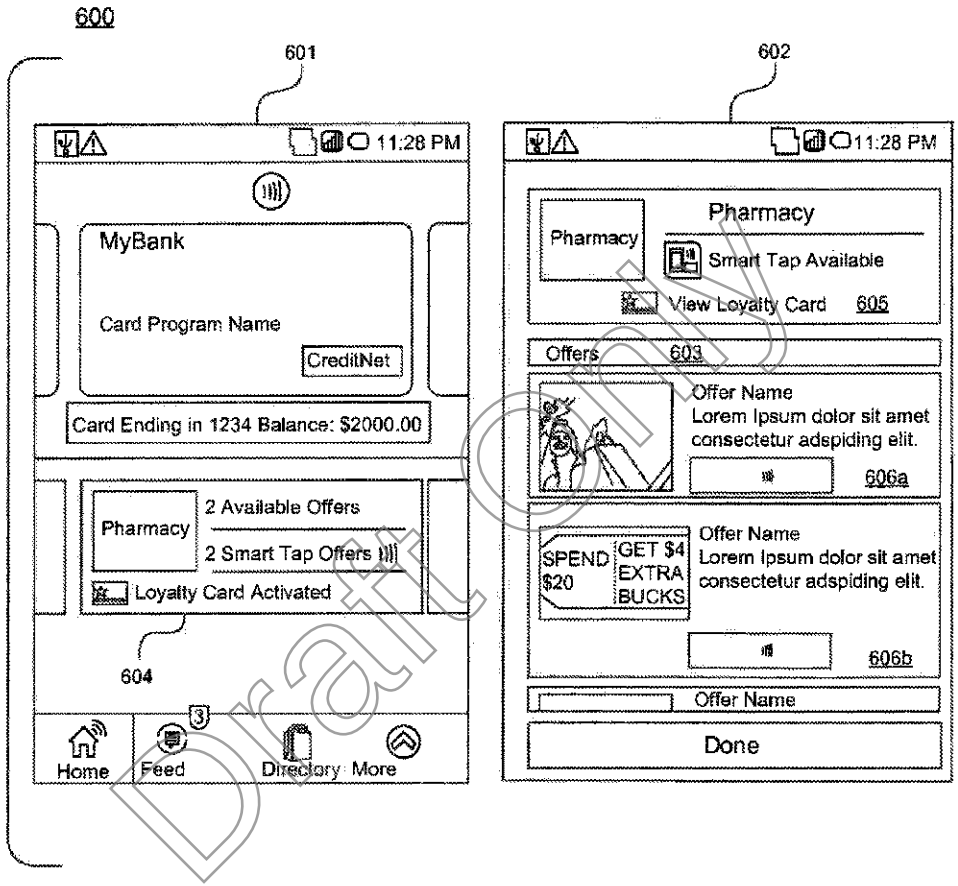
FIG. 4

Draft only



Draft Only

FIG. 5



Draft Only

FIG. 6

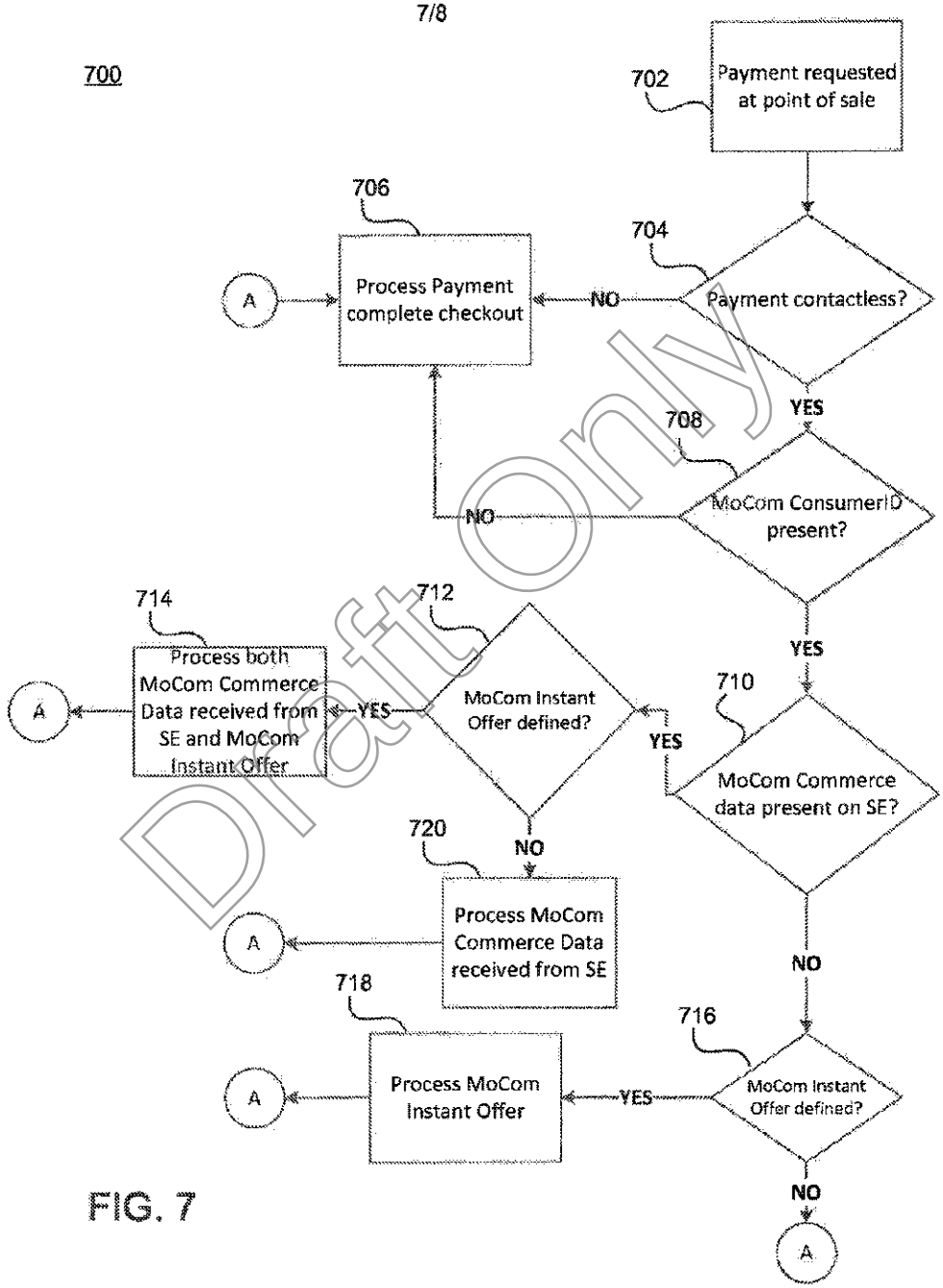


FIG. 7

Draft Only

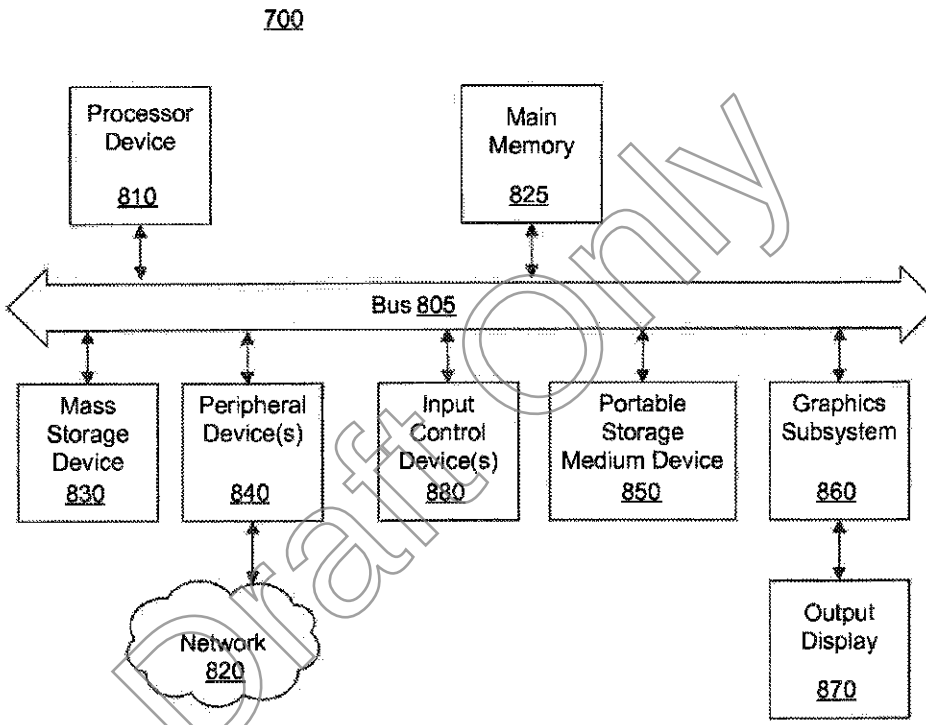


FIG. 8

Draft Only

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 ; WO2013JP53627 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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1086 of 1551

(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

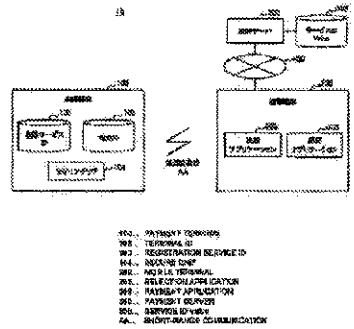
(21)国際出願番号　PCT/JP2013/053827
(22)国際出願日　平成25年2月18日(2013.2.18)
(31)優先権主張番号　特願2012-50273(P2012-50273)
(32)優先日　平成24年3月7日(2012.3.7)
(33)優先権主張国　日本国(JP)
出願番号　特願2014-503739(P2014-503739)

(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。



Draft Only

【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更に備え

Draft Only

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端末通信

Draft Only

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、
を含む決済処理方法。

Draft Only

【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

Draft Only

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、前記

CSC ServiceWorks - Ex. 1002
Page 1092 of 1551

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。

【図４】第１の実施形態に係る携帯端末の機能構成の一例を示すブロック図である。

CSC ServiceWorks - Ex. 1002
Page 1093 of 1551

【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。

Draft Only

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を含む。また、制

Draft only

【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】

Draft only

CSC ServiceWorks - Ex. 1002
Page 1096 of 1551

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１１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１１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１２と、を含む。

【００４５】

Partial

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。

【００５２】

Draft only

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モジュール、又はＷＷＡＮ（Wireless Wide Area Network）モジュー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ができる。また、暗号

Draft only

CSC ServiceWorks - Ex. 1002
Page 1099 of 1551

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。

【００６７】

Draft Only

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、表示されるサービスリストは

Draft Only

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）。

【００８５】

Draft only

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Ｓ１２５）。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１４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、決済サーバ３０

Draft Only

００へ送信する。

【００９４】

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。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１００を利用して、安全かつ汎用的な決済方法を実現できる。更に、以下のような副次的な効果も奏される。

【００９５】

まず、決済端末１００にネットワークデバイスを設けないことにより、部品点数が減るので、決済端末１００のコストダウンを図れる。また、ネットワークデバイスを設けることによるプログラムコードの増加を防止でき、ソフトウェアの開発費を抑制できる。

【００９６】

また、決済端末１００の機能を単純化できるので、新しいサービスを導入する場合の設定作業を軽減できる。また、内部設定を変更する必要も無くなるので、決済端末１００の長期利用も可能になり、メンテナンスコストも低減できる。また、決済端末１００のメモリ量を制約としないので、将来にリッチかつ複雑なサービスが導入された場合にも対応しやすくなる。

【００９７】

また、購入者が決済端末１００で決済をする場合に、決済端末１００が設置される店舗への信用が１つの不安要素となる。例えば、出店のような数日間限りの店舗にて決済する場合には、クレジットカードを渡すことは購入者の心理的に難しい。これに対して、第１の実施形態に場合には、決済サーバ３００との接続は携帯端末２００が行うため、信頼したシステム内で決済処理を実現できる。

【００９８】

＜２．第２の実施形態＞

図１１を参照しながら、本開示の第２の実施形態に係る決済処理システム２０の概要について説明する。図１１は、本開示の第２の実施形態に係る決済処理システム２０の概要を説明するための図である。

【００９９】

第２の実施形態に係る決済処理システム２０は、前述した第１の実施形態に係る決済処理システム１０と同様な決済処理を行う。決済処理システム２０は、図１１に示すように、決済端末１００と、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。以下では、第１の実施形態と同様な構成については、説明を省略する。

【０１００】

第１の実施形態ではサービスＩＤバリュー３５０（図１）が決済サーバ３００に接続されたデータベースに接続されていることとしたが、第２の実施形態では、携帯端末２００がサービスＩＤバリュー２０４を有する。すなわち、携帯端末２００が、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を有する。このため、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のサービスＩＤに対応する、携帯端末２００に格納されたサービスＩＤバリュー２０４に対して、決済処理を実行する。このため、予め携帯端末２００に登録されたバリューに対してのみ決済処理が行われ、予期せぬバリューに対して決済処理が行わることを防止できる。

【０１０１】

第２の実施形態に係る決済処理システム２０においても、決済端末１００と決済サーバ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。このため、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、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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1104 of 1551

かつ汎用的な決済方法を実現できる。

【０１０２】

＜３．第３の実施形態＞

図１２を参照しながら、本開示の第３の実施形態に係る決済処理システム３０の概要について説明する。図１１は、本開示の第３の実施形態に係る決済処理システム３０の概要を説明するための図である。

【０１０３】

第３の実施形態に係る決済処理システム３０は、前述した第１の実施形態に係る決済処理システム１０と同様な決済処理を行う。決済処理システム３０は、図１２に示すように、決済端末１００と、携帯端末２００と、決済サーバ３００と、ネットワーク４００と、ＩＣカード５００と、を有する。以下では、第１の実施形態と同様な構成については、説明を省略する。

【０１０４】

第１の実施形態ではサービスＩＤバリュー３５０（図１）が決済サーバ３００に接続されたデータベースに接続されていることとしたが、第３の実施形態では、ＩＣカード５００がサービスＩＤバリュー５１０を有する。すなわち、ＩＣカード５００が、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を有する。このため、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のサービスＩＤに対応する、ＩＣカード５００に格納されたサービスＩＤバリュー５１０に対して、決済処理を実行する。このため、ユーザが所望のバリューを記憶したＩＣカード５００と携帯端末２００と通信させるだけで、多様なバリューに対する決済処理が可能となる。

【０１０５】

ＩＣカード５００は、携帯端末２００と近距離通信（非接触通信）を行う。このため、携帯端末２００は、リーダ／ライタ機能を有する。なお、上記では、ＩＣカード５００が携帯端末２００に対して非接触通信を行うこととしたが、これに限定されない。例えば、ＩＣカード５００は携帯端末２００と接触通信を行うこととしても良い。また、ＩＣカード５００を例に挙げて説明したが、これに限定されず、サービスＩＤバリューを格納する機能を有する通信装置であれば形態を問わない。

【０１０６】

第３の実施形態に係る決済処理システム２０においても、決済端末１００と決済サーバ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。このため、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、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１００を利用して、安全かつ汎用的な決済方法を実現できる。

【０１０７】

＜４．ハードウェア構成例＞

上述した第１～第３の実施形態に係る決済処理システム１０、２０、３０による決済処理は、決済端末１００、携帯端末２００、及び決済サーバ３００が備えるハードウェア構成とソフトウェアとが協働することにより実現される。そして、決済端末１００、携帯端末２００、及び決済サーバ３００のハードウェア構成は同様であるので、以下では、図１３を参照しながら、携帯端末２００のハードウェア構成の一例について説明する。

【０１０８】

図１３は、第１～第３の実施形態に係る携帯端末２００のハードウェア構成の一例を示すブロック図である。図１３に示すように、携帯端末２００は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）２６２と、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）２６４と、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）２６６と、を有する。また、携帯端末２００は、入力装置２６８と、出力装置２７０と、ストレージ装置

Draft Only

【０１０９】
ＣＰＵ２６２は、演算処理装置および制御装置として機能し、各種プログラムに従って携帯端末２００内の動作全般を制御する。また、ＣＰＵ２６２は、マイクロプロセッサであってもよい。ＲＯＭ２６４は、ＣＰＵ２６２が使用するプログラムや演算パラメータ等を記憶する。ＲＡＭ２６６は、ＣＰＵ２６２の実行において使用するプログラムや、その実行において適宜変化するパラメータ等を一時記憶する。これらはＣＰＵバスなどから構成されるホストバスにより相互に接続されている。

【０１１０】
入力装置２６８は、マウス、キーボード、タッチパネル、ボタン、マイクロフォン、スイッチおよびレバーなどユーザが情報を入力するための入力手段と、ユーザによる入力に基づいて入力信号を生成し、ＣＰＵ２６２に出力する入力制御回路などから構成されている。携帯端末２００のユーザは、入力装置２６８を操作することにより、携帯端末２００に対して各種のデータを入力したり処理動作を指示したりすることができる。

【０１１１】
出力装置２７０は、例えば、液晶ディスプレイ（ＬＣＤ）装置、ＯＬＥＤ（Ｏｒｇａｎｉｃ Ｌｉｇｈｔ Ｅｍｉｔｔｉｎｇ Ｄｉｏｄｅ）装置およびランプなどの表示装置を含む。さらに、出力装置２７０は、スピーカおよびヘッドホンなどの音声出力装置を含む。例えば、表示装置は、生成された画像などを表示する。一方、音声出力装置は、音声データ等を音声に変換して出力する。

【０１１２】
ストレージ装置２７２は、携帯端末２００の記憶部の一例として構成されたデータ格納用の装置である。ストレージ装置２７２は、記憶媒体、記憶媒体にデータを記録する記録装置、記憶媒体からデータを読み出す読出し装置および記憶媒体に記録されたデータを削除する削除装置などを含んでもよい。このストレージ装置２７２は、ＣＰＵ２６２が実行するプログラムや各種データを格納する。

【０１１３】
ドライブ２７４は、記憶媒体用リーダライタであり、携帯端末２００に内蔵、あるいは外付けされる。ドライブ２７４は、装着されている磁気ディスク、光ディスク、光磁気ディスク、または半導体メモリ等のリムーバブル記憶媒体６００に記録されている情報を読み出して、ＲＡＭ２６６に出力する。また、ドライブ２７４は、リムーバブル記憶媒体６００に情報を書き込むこともできる。

【０１１４】
通信装置２７６は、例えば、ネットワーク４００に接続するための通信デバイス等で構成された通信インタフェースである。また、通信装置２７６は、無線ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）対応通信装置であっても、ＬＴＥ（Ｌｏｎｇ Ｔｅｒｍ Ｅｖｏｌｕｔｉｏｎ）対応通信装置であっても、有線による通信を行うワイヤー通信装置であってもよい。

【０１１５】
近距離通信装置２７８は、外部装置と近距離通信（例えば、ＮＦＣ通信）を行う装置である。近距離通信装置２７８は、例えば、通信アンテナにより外部装置のリーダ／ライタから送信された搬送波を受信し、内臓のＩＣチップにおける処理の処理結果に基づく応答信号を送信する。通信アンテナは、例えば、所定のインダクタンスをもつコイル（インダクタ）と、所定の静電容量をもつキャパシタとからなる共振回路で構成される。ＩＣチップは、受信された搬送波に基づいて搬送波信号を復調して処理し、負荷変調により応答信号を通信アンテナから送信させる。

【０１１６】
以上、添付図面を参照しながら本開示の好適な実施形態について詳細に説明したが、本開示の技術的範囲はかかる例に限定されない。本開示の技術分野における通常の知識を有する者であれば、特許請求の範囲に記載された技術的思想の範疇内において、各種の変更

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1106 of 1551

術的範囲に属するものと了解される。

【０１１７】

上記の実施形態では、通信装置としてスマートフォンを例に挙げて説明したが、これに限定されない。例えば、通信装置は、近距離通信と無線通信を有すれば、ＰＤＡ、ゲーム機、電子辞書、ノートパソコン等であっても良い。

【０１１８】

また、上記の実施形態では、近距離通信としてＮＦＣ（Near Field Communication）通信を例に挙げて説明したが、これに限定されない。例えば、近距離通信は、Bluetoothであっても良い。また、上記では、通信装置（携帯端末２００）が、決済サーバと無線通信を行うこととしたが、これに限定されない。例えば、通信装置（携帯端末２００）が、決済サーバと有線通信を行って、決済データを送受信しても良い。

【０１１９】

また、上記の実施形態のフローチャートに示されたステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的に又は個別的に実行される処理をも含む。また時系列的に処理されるステップでも、場合によっては適宜順序を変更することが可能であることは言うまでもない。

【０１２０】

本明細書において説明した情報処理装置による処理は、ソフトウェア、ハードウェア、及びソフトウェアとハードウェアとの組合せのいずれを用いて実現されてもよい。ソフトウェアを構成するプログラムは、例えば、各装置の内部又は外部に設けられる記憶媒体に予め格納される。そして、各プログラムは、例えば、実行時にＲＡＭ（Random Access Memory）に読み込まれ、ＣＰＵなどのプロセッサにより実行される。

【０１２１】

なお、以下のような構成も本開示の技術的範囲に属する。

（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

Draft Only

決済処理システム。
（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、
前記（１）に記載の決済処理システム。
（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、
前記（２）に記載の決済処理システム。
（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、
前記（２）又は（３）に記載の決済処理システム。
（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更に備え、
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、
前記（１）～（４）のいずれか１項に記載の決済処理システム。
（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、
前記（５）に記載の決済処理システム。
（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、
前記（１）～（６）のいずれか１項に記載の決済処理システム。
（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、
前記（１）～（７）のいずれか１項に記載の決済処理システム。
（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

Draft Only

前記（１）～（８）のいずれか１項に記載の決済処理システム。
（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、
前記（１）～（８）のいずれか１項に記載の決済処理システム。
（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、
前記（１）～（８）のいずれか１項に記載の決済処理システム。
（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。
（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。
（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
、

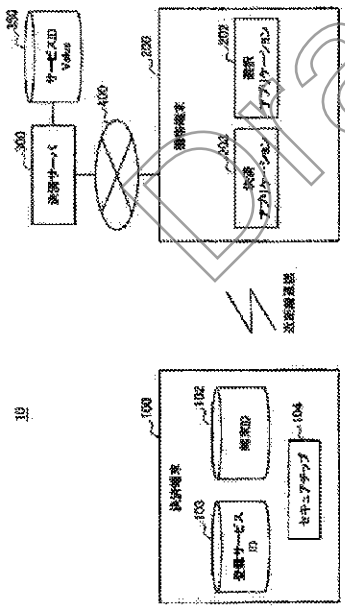
Translation Only

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。
（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、
を含む決済処理方法。
（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。
【符号の説明】
【０１２２】
１０、２０、３０　決済処理システム
１００　決済端末
１１８　近距離通信部
１２０　決済データ生成部
１２２　署名検証部
２００　携帯端末
２１８　近距離通信部
２２０　無線通信部
２２２　決済データ処理部
３００　決済サーバ

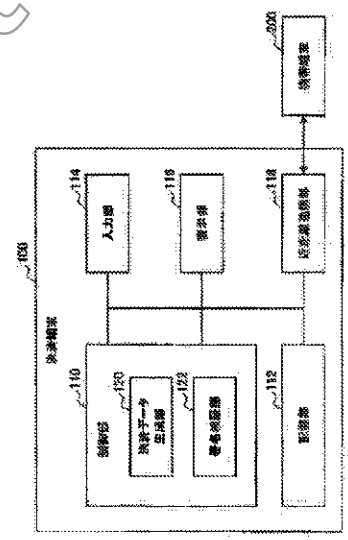
Preliminary Copy Only

３２０　署名検証部
３２２　決済処理部
３２４　決済データ処理部
４００　ネットワーク
５００　ＩＣカード

【図１】

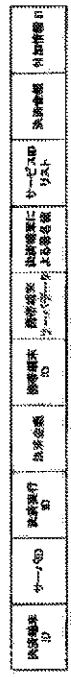


【図２】

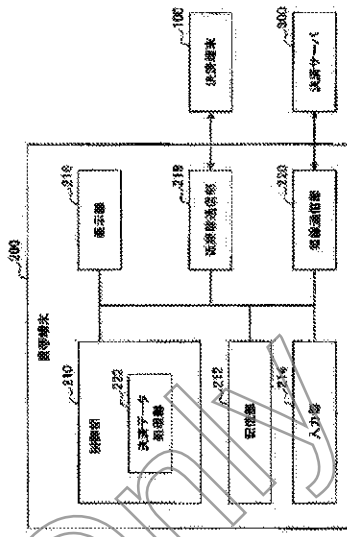


Draft Only

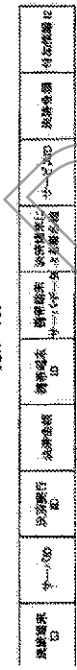
【図３】



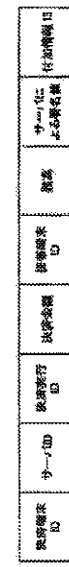
【図４】



【図５】

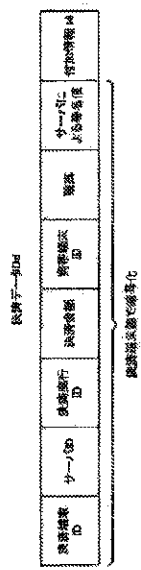


【図６】

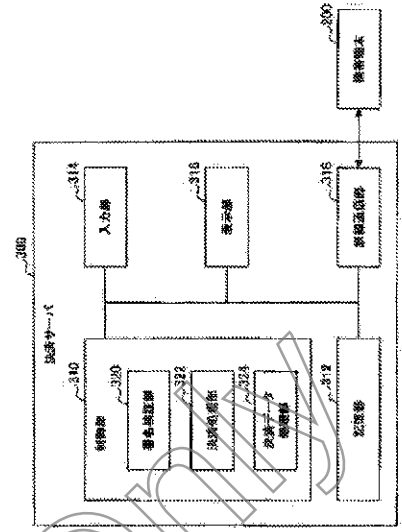


Draft Only

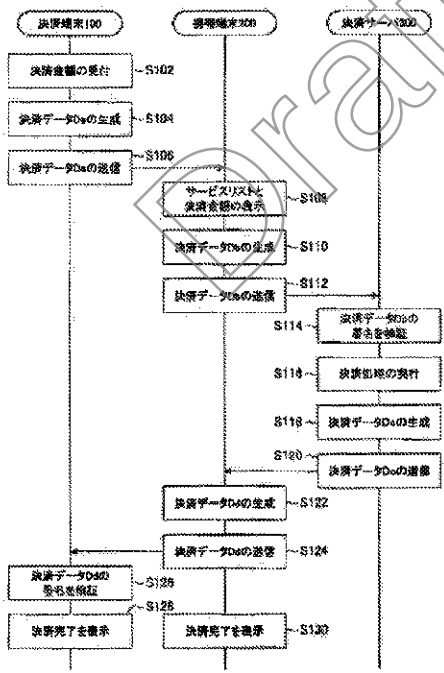
【図７】



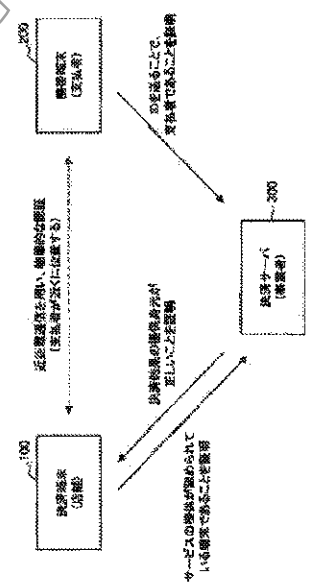
【図８】



【図９】

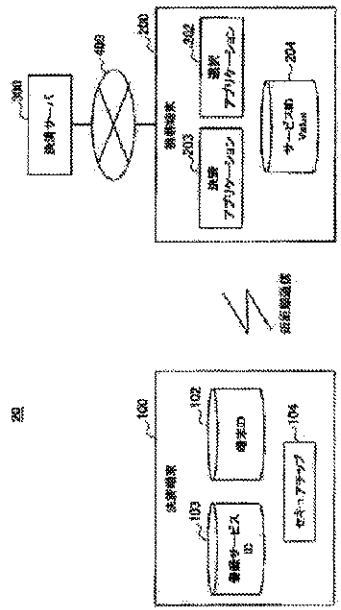


【図１０】

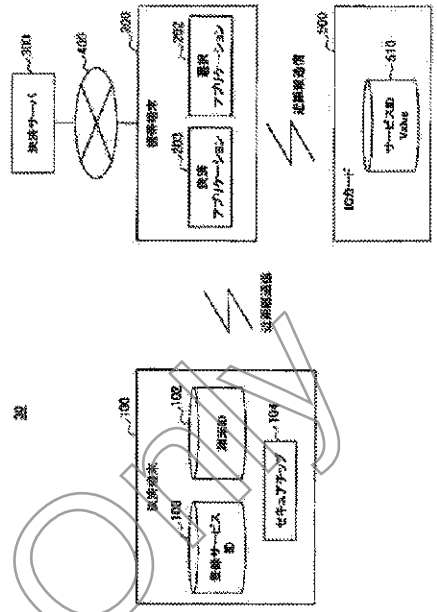


Draft Only

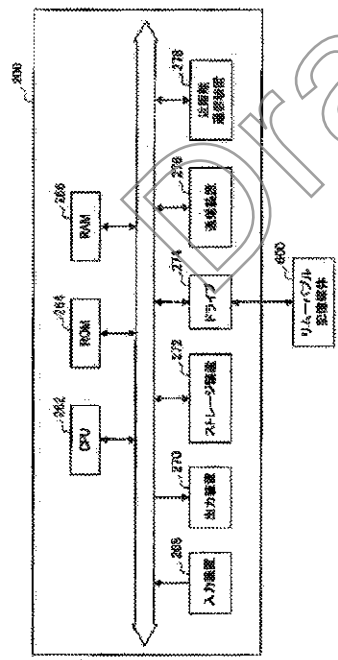
【図１１】



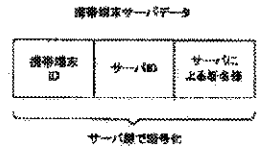
【図１２】



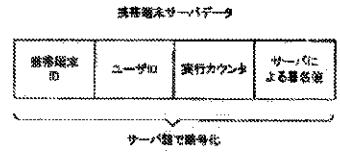
【図１３】



【図１４】



【図１５】



Draft Only

【手続補正書】
【提出日】平成27年2月5日(2015.2.5)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【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

Draft Only

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又は３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更に備え、
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１～４のいずれか１項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１～６のいずれか１項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１～７のいずれか１項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１～８のいずれか１項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１～８のいずれか１項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１～８のいずれか１項に記載の決済処理システム。
【請求項１２】

Draft Only

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。

【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

Draft Only

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。
【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。

Draft Only

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/053827

A. CLASSIFICATION OF SUBJECT MATTER
G06Q20/40(2012.01)i, *G06Q20/00*(2012.01)i, *G07G1/12*(2006.01)i, *G07G1/14*(2006.01)i

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)
G06Q20/40, G06Q20/00, G07G1/12, G07G1/14

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2013
Kokai Jitsuyo Shinan Koho	1971-2013	Toroku Jitsuyo Shinan Koho	1994-2013

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2007-241448 A (Panasonic Corp.), 20 September 2007 (20.09.2007), 0015, 0034 to 0048, 0066 to 0067, 0070 to 0072 (Family: none)	1-16
Y	JP 2004-185253 A (Mitsubishi Electric Corp.), 02 July 2004 (02.07.2004), 0016 to 0024 (Family: none)	1-16
Y	JP 2011-118769 A (Hitachi, Ltd.), 16 June 2011 (16.06.2011), 0008, 0048 to 0053, 0056 to 0059, 0070 to 0077 (Family: none)	1-16

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* 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
06 March, 2013 (06.03.13)	19 March, 2013 (19.03.13)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 2009)

Draft Only

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/053827

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2007-281948 A (NTT Docomo Inc.), 25 October 2007 (25.10.2007), 0062 to 0063 & US 2009/0287760 A1 & EP 2006768 A2 & WO 2007/116993 A1 & KR 10-2008-0098551 A & CN 101416159 A & KR 10-0971896 B1	3
A	JP 2003-051780 A (Toshiba Tec Corp.), 21 February 2003 (21.02.2003), 0016 to 0026; fig. 3 (Family: none)	1-16

Draft Only

Form PCT/ISA/210 (continuation of second sheet) (July 2009)

国際調査報告

国際出願番号 PCT/JP2013/053827

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. G06Q20/40(2012.01)i, G06Q20/00(2012.01)i, G07G1/12(2006.01)i, G07G1/14(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl. G06Q20/40, G06Q20/00, G07G1/12, G07G1/14

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2013年
日本国実用新案登録公報	1996－2013年
日本国登録実用新案公報	1994－2013年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y	JP 2007-241448 A（パナソニック株式会社）2007.09.20, 0015、0034－0048、0066－0067、0070－0072（ファミリーなし）	1－16
Y	JP 2004-186253 A（三菱電機株式会社）2004.07.02, 0016－0024（ファミリーなし）	1－16
Y	JP 2011-118789 A（株式会社日立製作所）2011.06.16, 0008、0048－0053、0056－0059、0070－0077（ファミリーなし）	1－16

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 06.03.2013	国際調査報告の発送日 19.03.2013
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 塩田 博志 3L 4839 電話番号 03－3581－1101 内線 3562

様式PCT／ISA／210（第2ページ）（2009年7月）

Draft Only

国際調査報告 国際出願番号 PCT/JP2013/053827

C（続き）． 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y	JP 2007-281948 A (株式会社エヌ・ティ・ティ・ドコモ) 2007.10.25, ００６２－００６３ & US 2009/0287760 A1 & EP 2006768 A2 & WO 2007/116993 A1 & KR 10-2008-0096551 A & CN 101416159 A & KR 10-0971896 B1	3
A	JP 2003-051780 A (東芝テック株式会社) 2003.02.21, ００１６－００２６、第３図 (ファミリーなし)	１－１６

様式PCT/ISA/210（第2ページの続き）（2009年7月）

Draft Only

フロントページの続き

(51)Int.Cl.	F I		テーマコード（参考）
	G07F 7/08	L	

(81)指定国 AP(BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, RU, TJ, TM), EP(AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC

(特許庁注：以下のものは登録商標)
1．ＦＡＣＥＢＯＯＫ
2．ＢＬＵＥＴＯＯＴＨ

Ｆターム(参考) 3E044 AA20 BA10 CA10 CB02 DC06 DE01
3E142 EA04 FA09 FA10 FA25 GA16 HA01 HA03 JA03 JA04
5L055 AA53 AA75

(注) この公表は、国際事務局（ＷＩＰＯ）により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願（日本語実用新案登録出願）の国際公開の効果は、特許法第１８４条の１０第１項(実用新案法第４８条の１３第２項）により生ずるものであり、本掲載とは関係ありません。

Draft Only

(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).

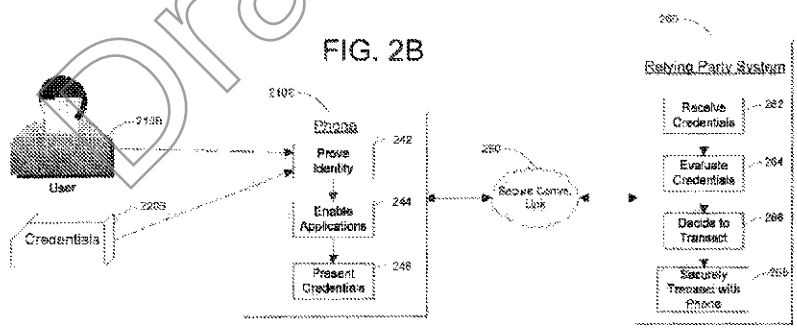
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, 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.

Draft Only

WO 2009/070430 A2

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 infrastructure (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*

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1125 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1126 of 1551

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1127 of 1551

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1128 of 1551

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1129 of 1551

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

Draft Only

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1131 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1132 of 1551

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

Draft Only

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

Draft Only

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1135 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1136 of 1551

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1137 of 1551

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

Draft Only

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1139 of 1551

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;

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1140 of 1551

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;

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1141 of 1551

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;

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1142 of 1551

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

Draft Only

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

Draft Only

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1145 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1146 of 1551

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1147 of 1551

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, in 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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1148 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1149 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1150 of 1551

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. 8 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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1151 of 1551

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1152 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1153 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1154 of 1551

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.

Draft Only

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1156 of 1551

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**

Draft Only

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1158 of 1551

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

Draft Only

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**.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1160 of 1551

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.

Draft Only

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1162 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1163 of 1551

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1164 of 1551

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1165 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1166 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1167 of 1551

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'

Draft Only

trusted authority which issued certificate **630**. In such a case, if the upstream authority discovers a fraud, it can revoke intermediate identity certificate **638**, 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

Draft Only

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

Draft only

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1171 of 1551

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

Draft Only

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1173 of 1551

access to sensitive applications and data when it is turned off, or after a fixed period of power-on idling.

Process **960** 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

Draft Only

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1175 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1176 of 1551

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

Draft Only

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

Draft Only

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1179 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1180 of 1551

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

Draft Only

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 **2820** 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

Draft Only

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

Draft Only

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

Draft Only

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

Draft Only

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.

Draft Only

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**,

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1187 of 1551

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

Draft Only

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

Draft Only

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

Draft Only

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 **1518** 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

Draft only

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1192 of 1551

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

Draft only

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1194 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1195 of 1551

("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 **1766**, 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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1196 of 1551

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

Draft Only

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

Draft Only

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

Draft Only

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1200 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1201 of 1551

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 **1630** 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 **1960**, 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

Draft Only

process **1930** 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 **1822** as illustrated in **Fig. 15A**; the secure data may be deposited, for example, in flash memory associated with smart phone **1824** 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

Draft Only

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

Draft Only

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.

Draft Only

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

Draft Only

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.

Draft Only

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

Draft Only

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

Draft Only

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1210 of 1551

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

Draft Only

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

Draft Only

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 **2610** 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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1213 of 1551

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

Draft Only

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, then 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,

Draft Only

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 in 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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1216 of 1551

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

Draft Only

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1218 of 1551

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.

Draft Only

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

Draft Only

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

Draft Only

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1222 of 1551

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

Draft Only

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

Proof Only

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

Draft Only

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1226 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1227 of 1551

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

Draft Only

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1229 of 1551

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1230 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1231 of 1551

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1232 of 1551

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

Draft Only

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1234 of 1551

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

Draft Only

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

Draft Only

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1237 of 1551

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1238 of 1551

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

DRAFT ONLY

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1240 of 1551

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

Draft Only

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

Draft Only

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1243 of 1551

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1244 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1245 of 1551

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:

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1246 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1247 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1248 of 1551

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1249 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1250 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1251 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1252 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1253 of 1551

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1254 of 1551

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

Draft only

CSC ServiceWorks - Ex. 1002
Page 1255 of 1551

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1256 of 1551

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

Draft Only

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1258 of 1551

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1259 of 1551

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.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1260 of 1551

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

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1261 of 1551

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

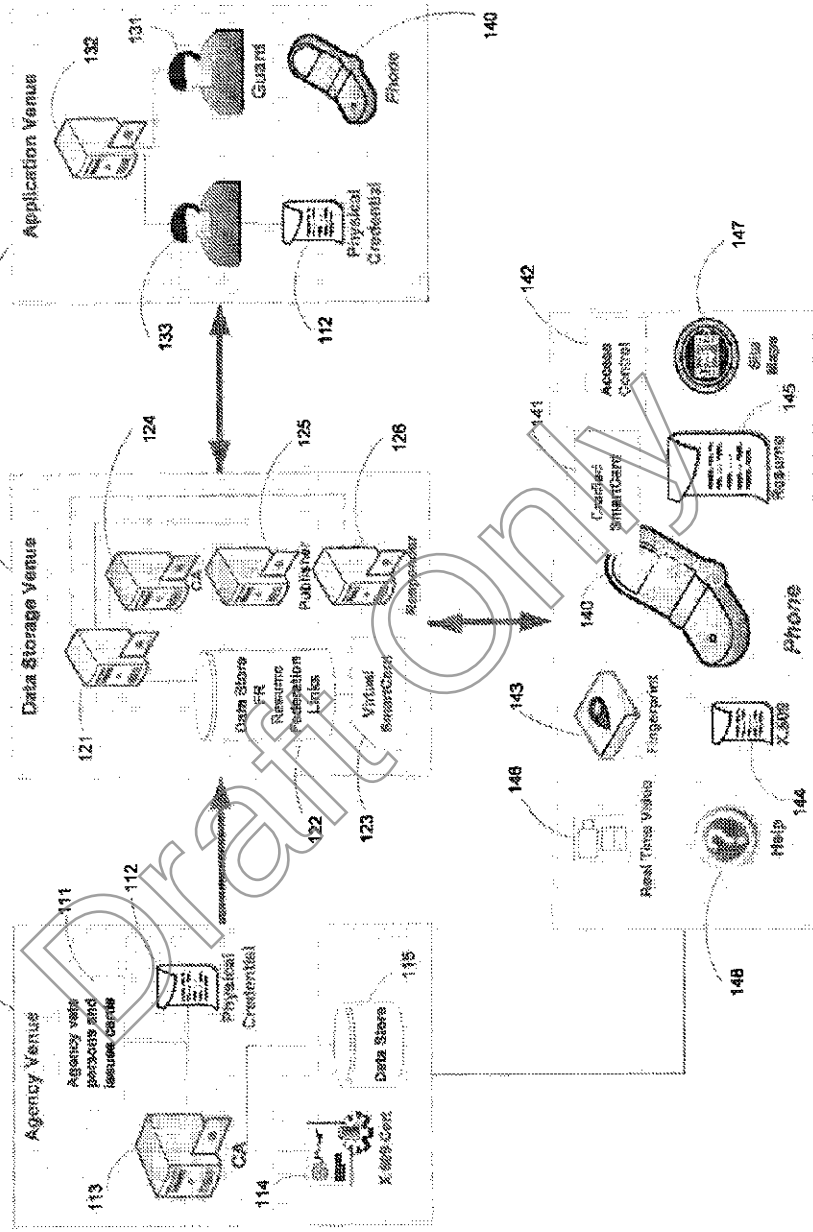
Draft only

professional.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1263 of 1551

FIG. 1



Draft Only

FIG. 2A

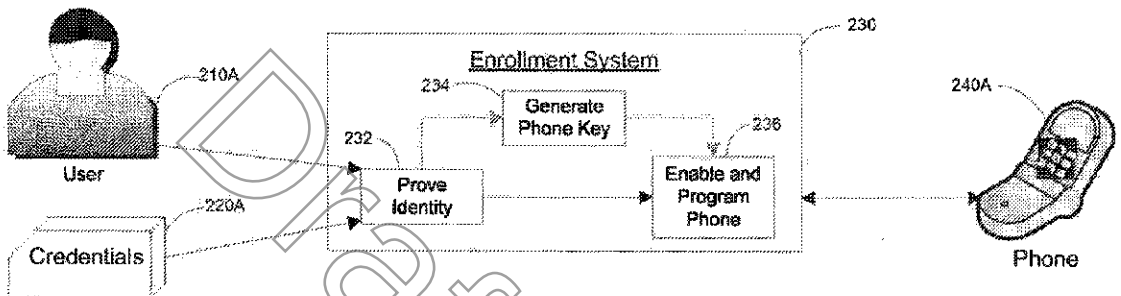
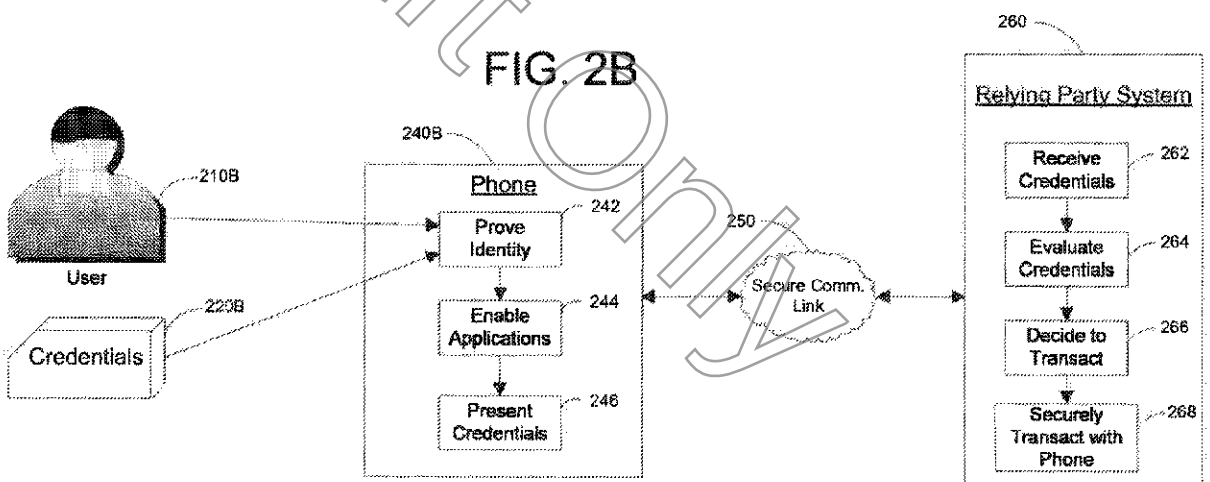
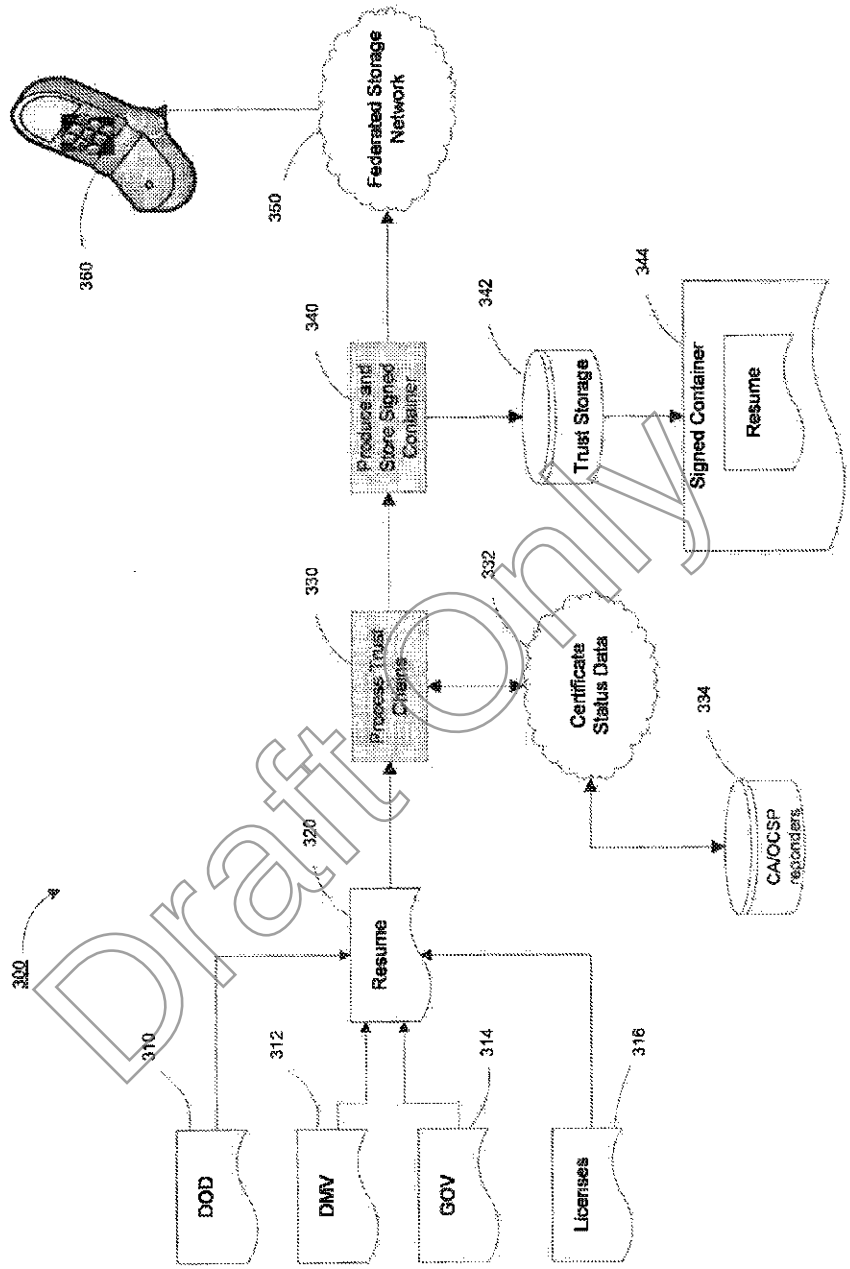


FIG. 2B



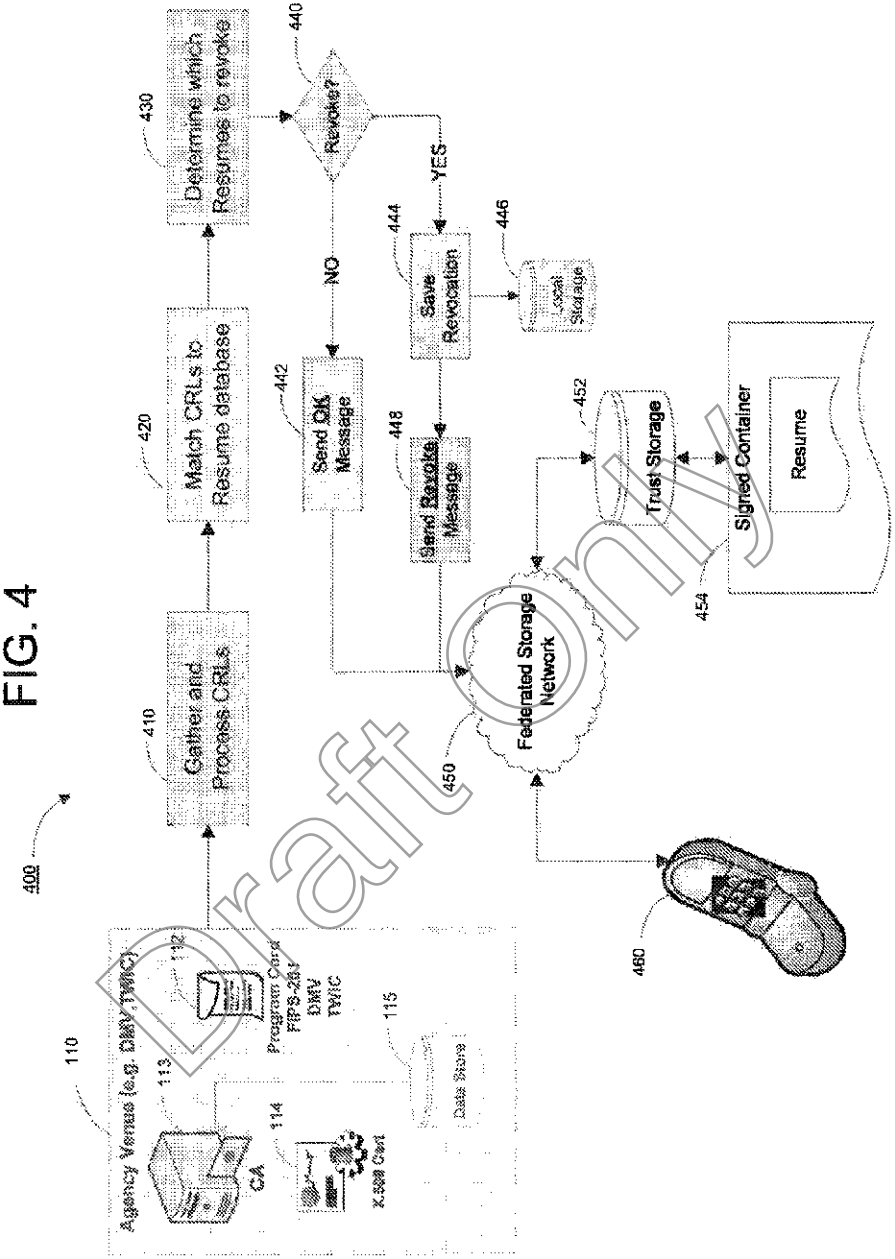
Draft Only

FIG. 3



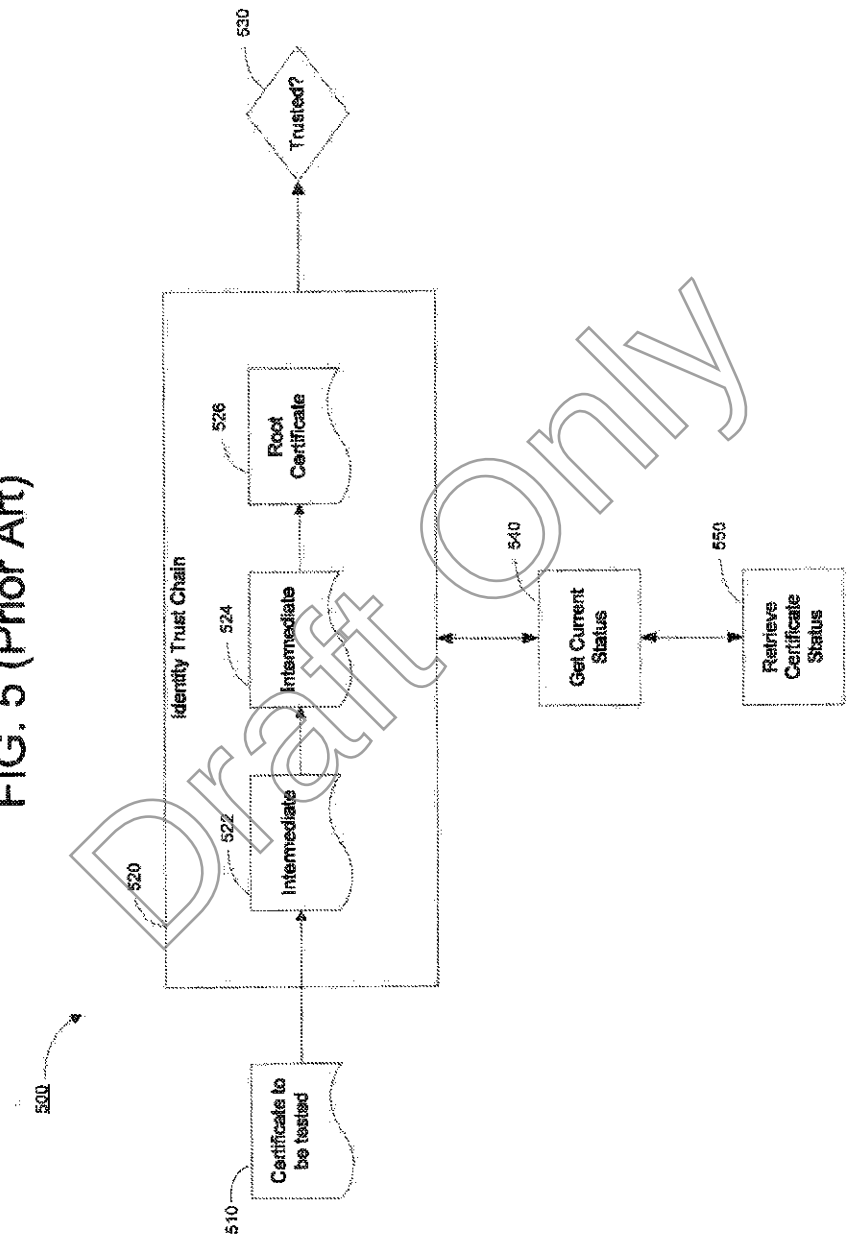
Draft Only

FIG. 4



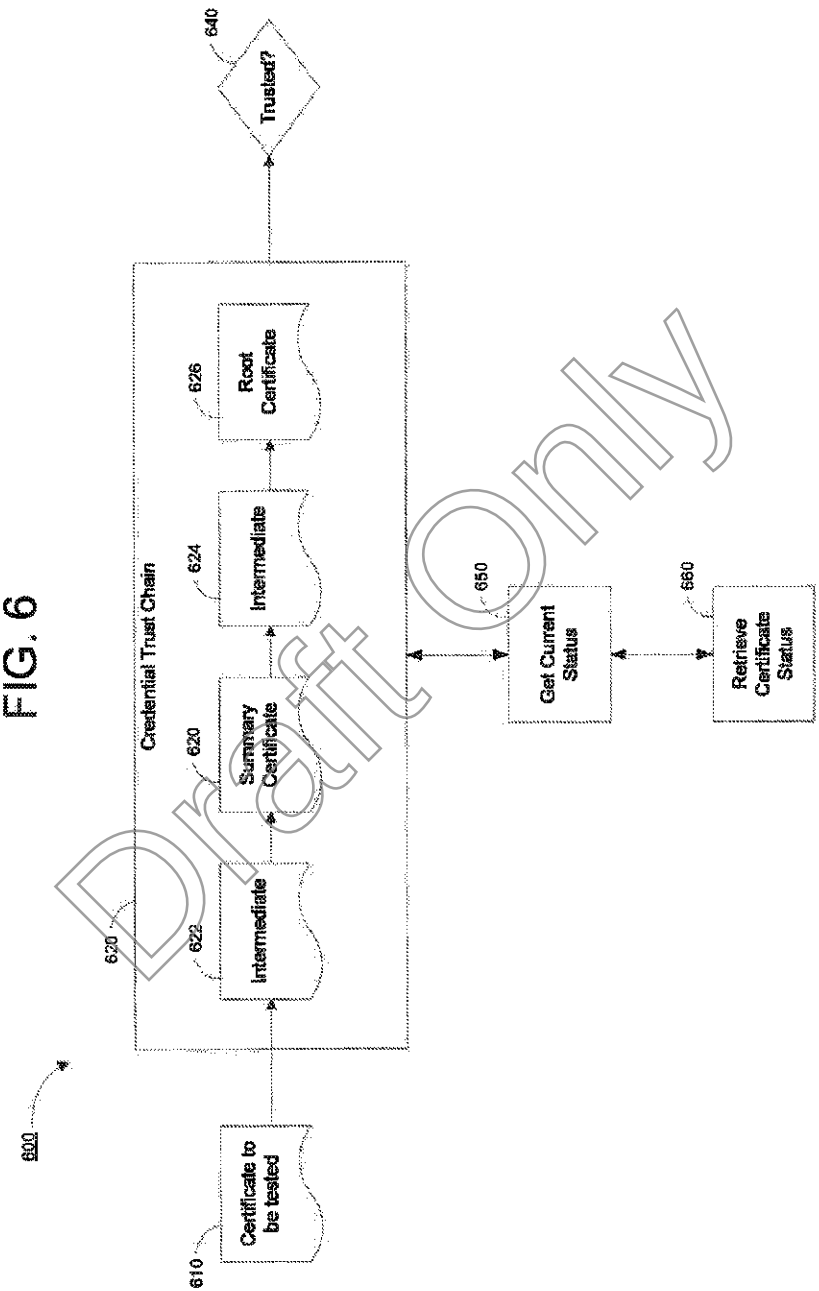
Draft Only

FIG. 5 (Prior Art)



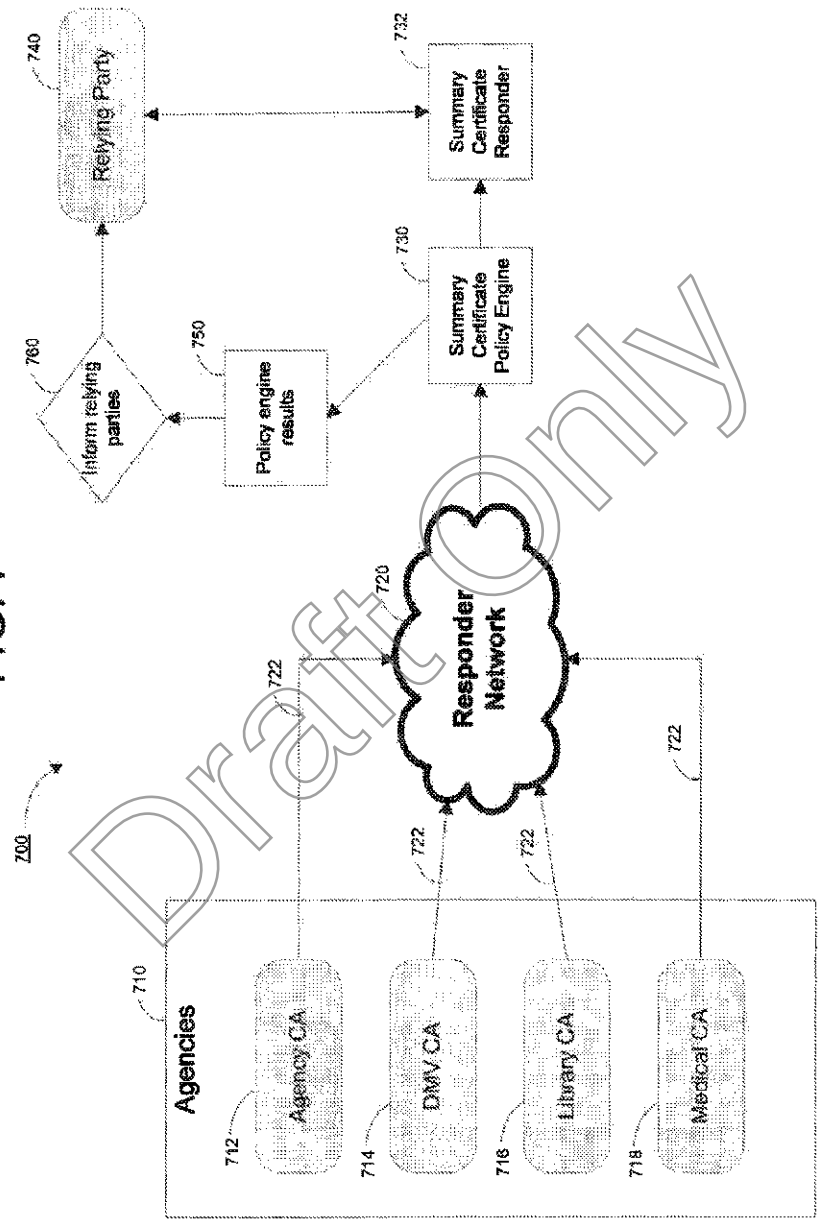
Draft Only

FIG. 6



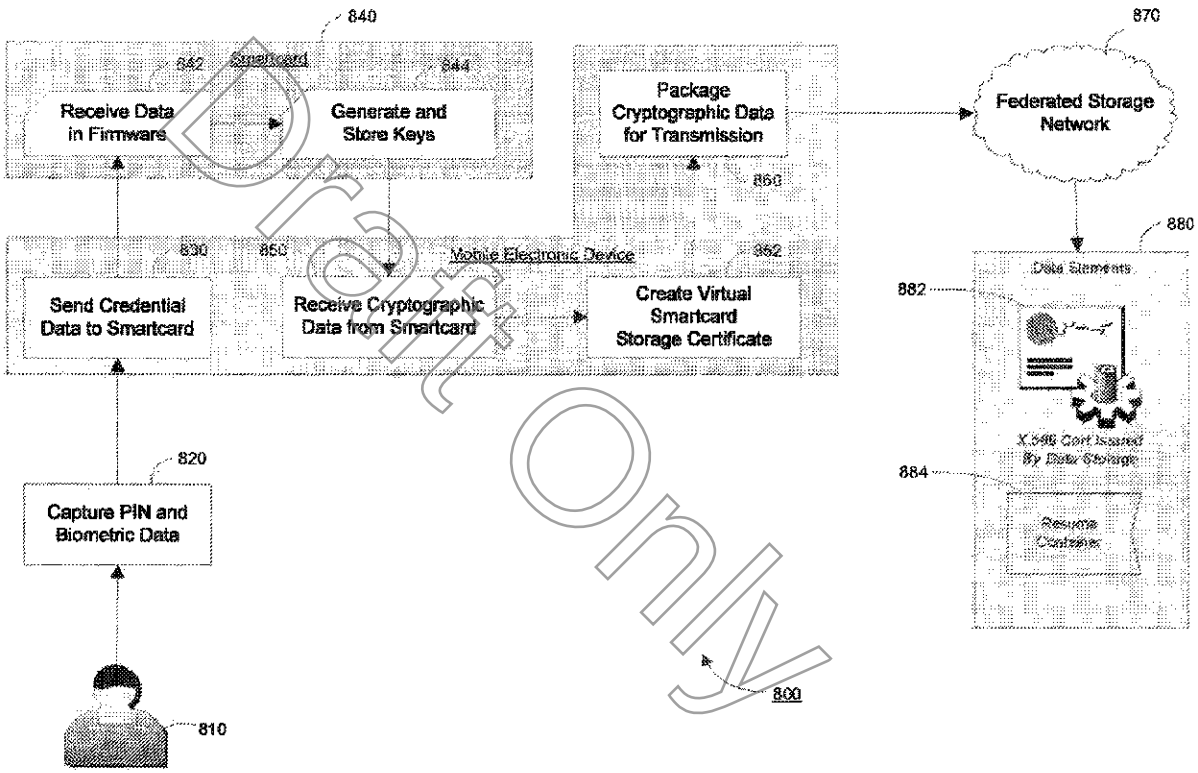
Draft Only

FIG. 7



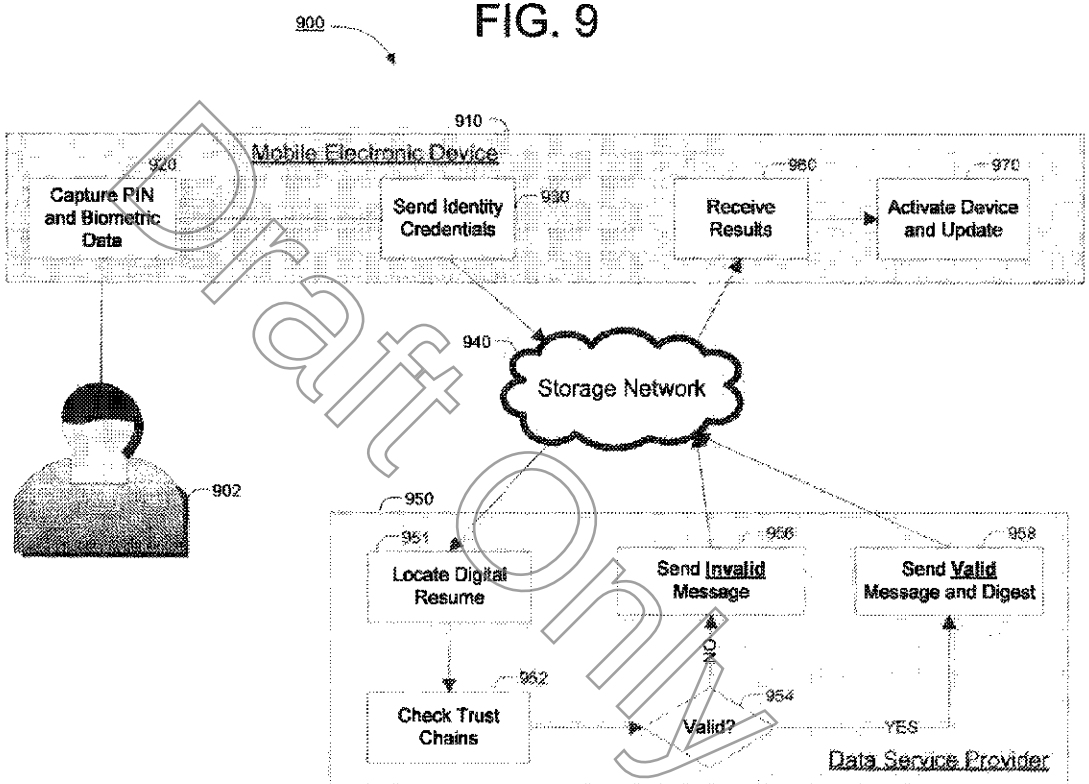
Draft Only

FIG. 8



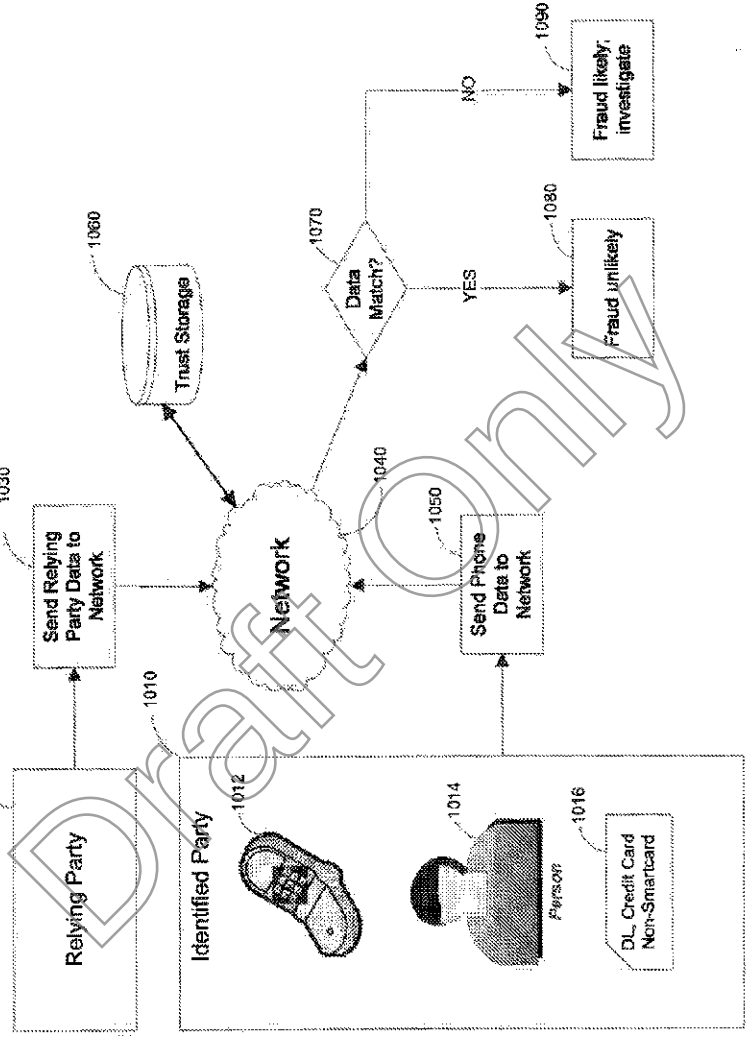
Draft Only

FIG. 9



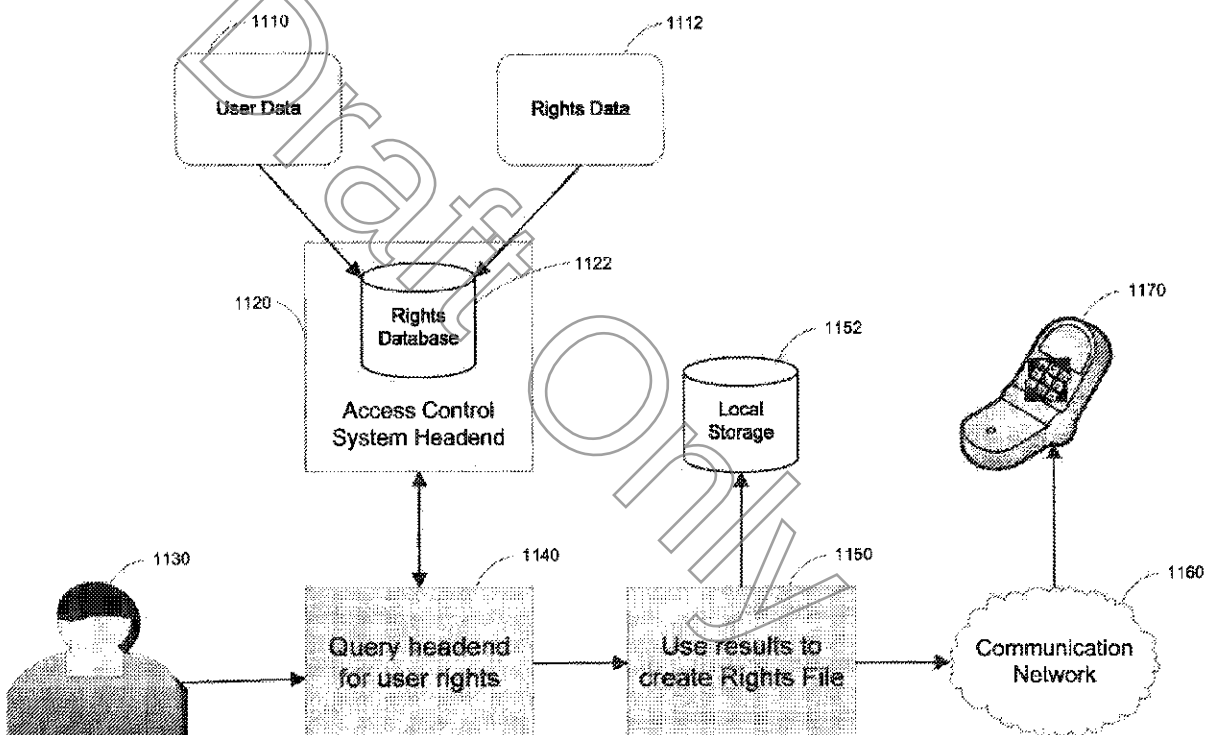
Draft Only

FIG. 10



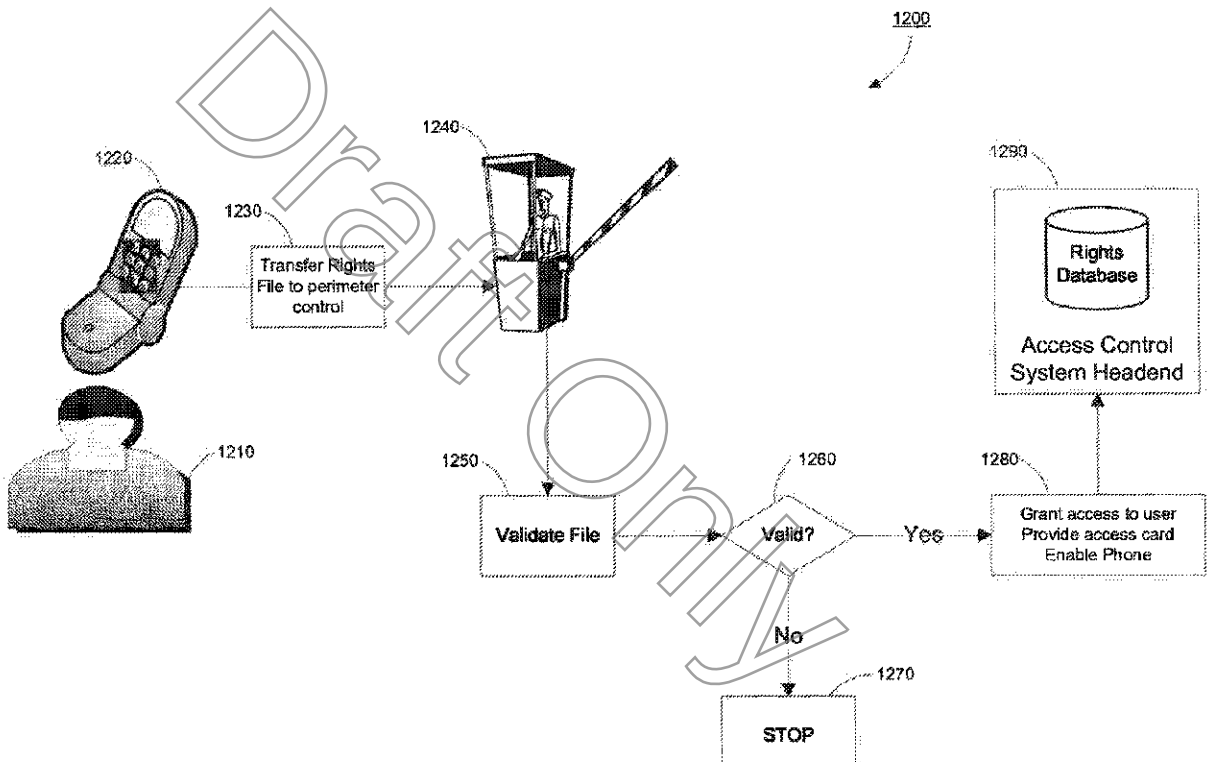
Draft Only

FIG. 11



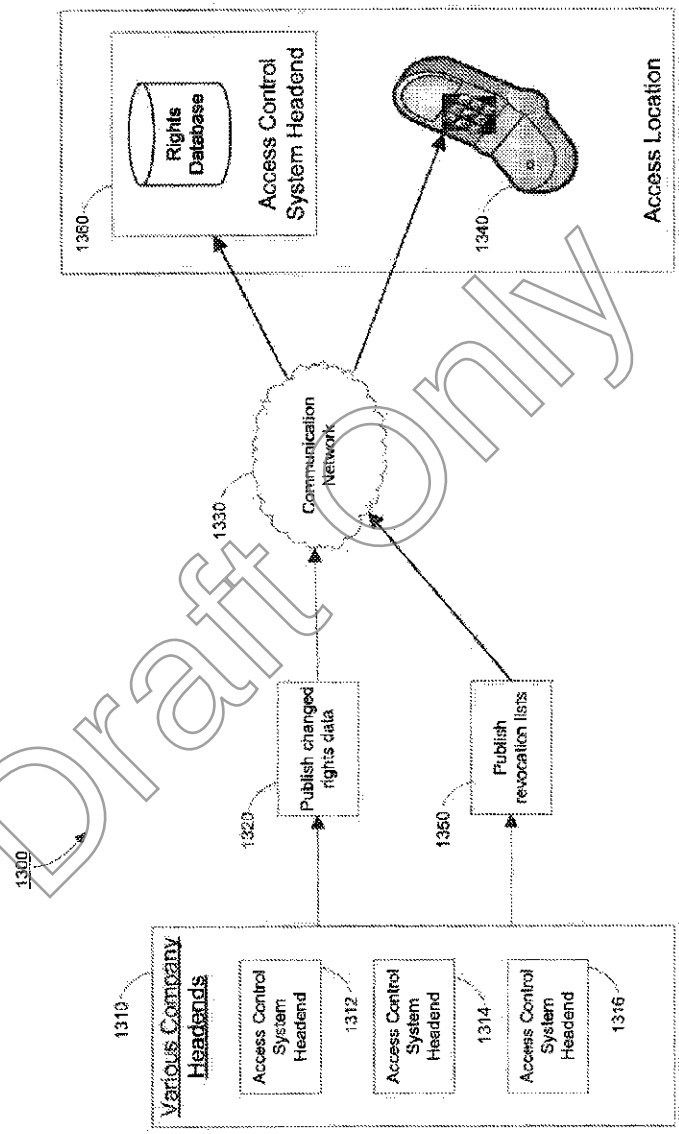
Draft Only

FIG. 12



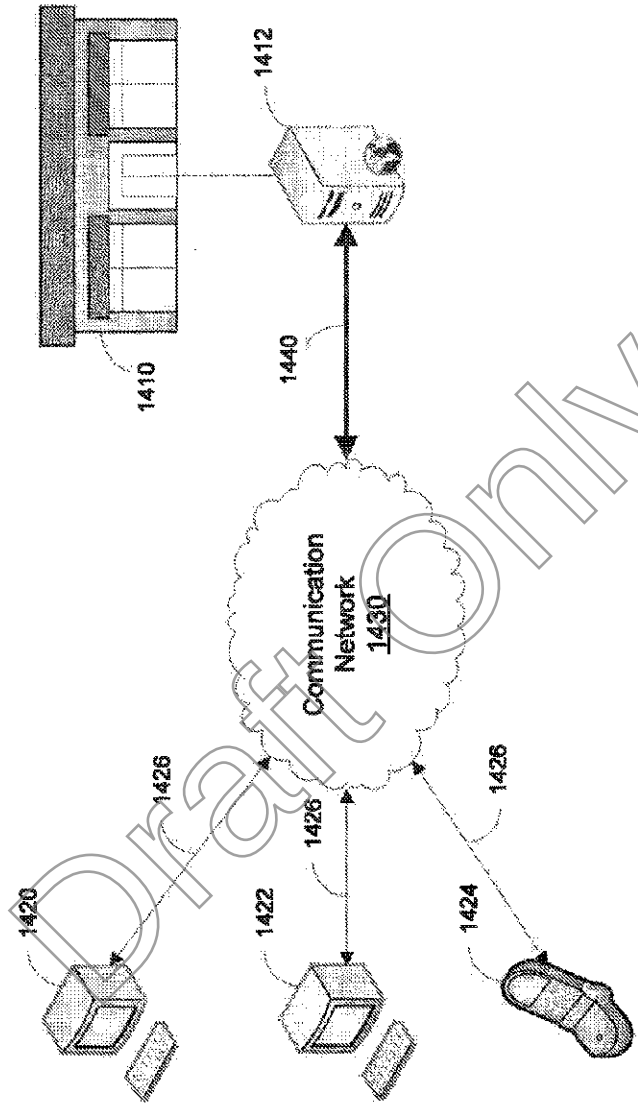
Draft Only

FIG. 13



Draft Only

FIG. 14 (Prior art)



Draft Only

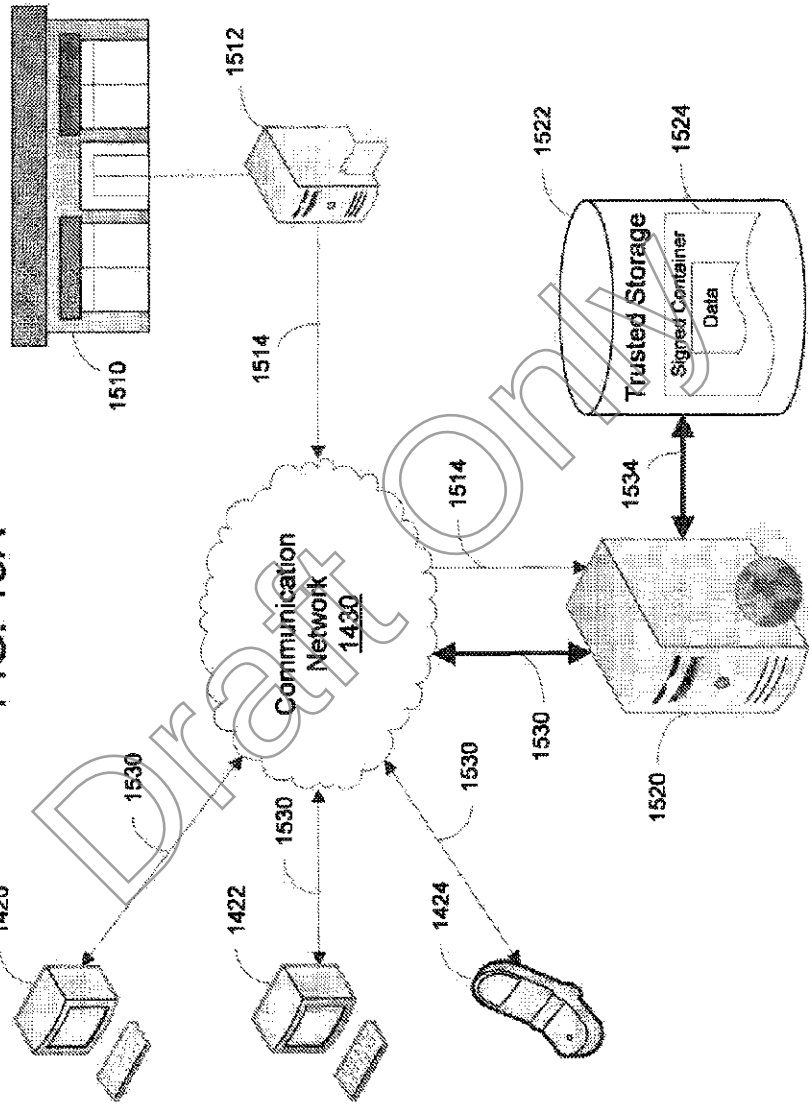
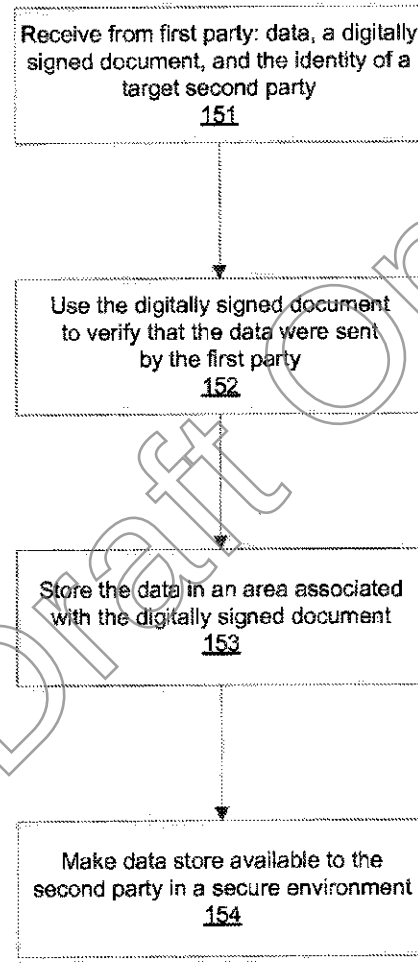


FIG. 15A

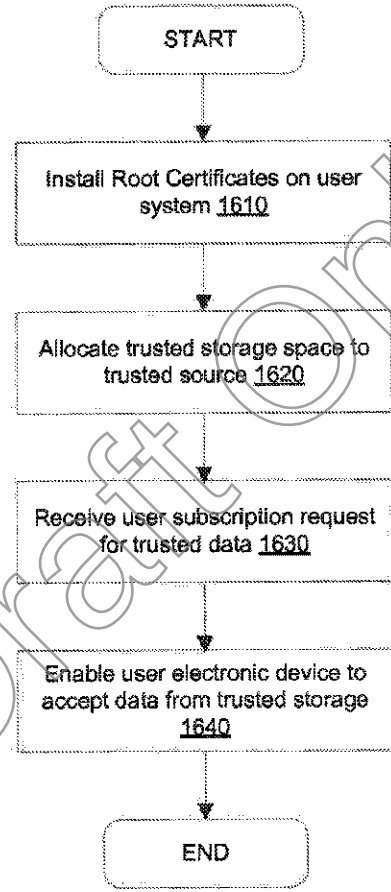
Draft Only

FIG. 15B



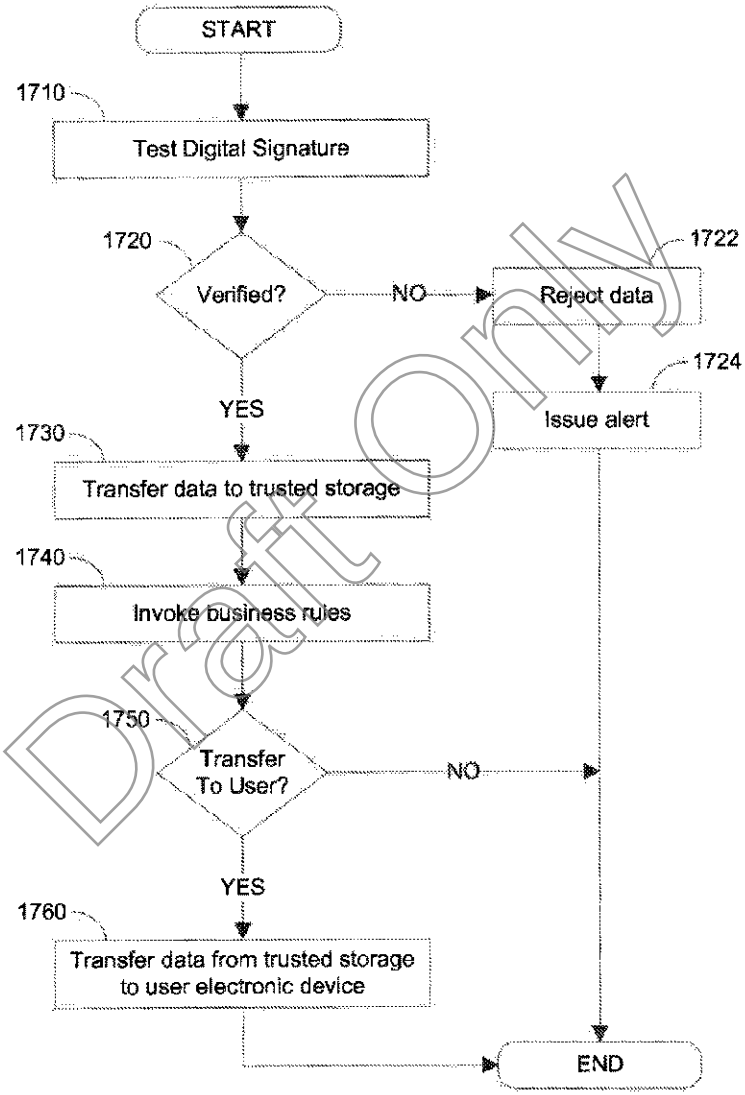
Draft Only

FIG. 16



Draft Only

FIG. 17



Draft Only

FIG. 18A (P1)

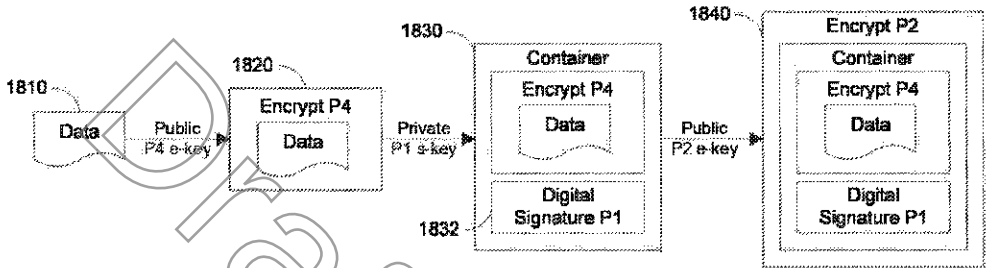
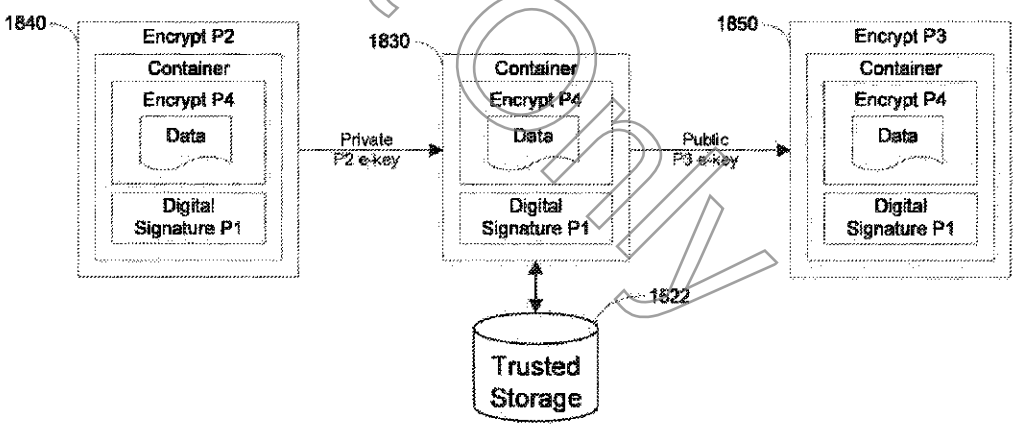


FIG. 18B (P2)



Draft Only

FIG. 18C (P3)

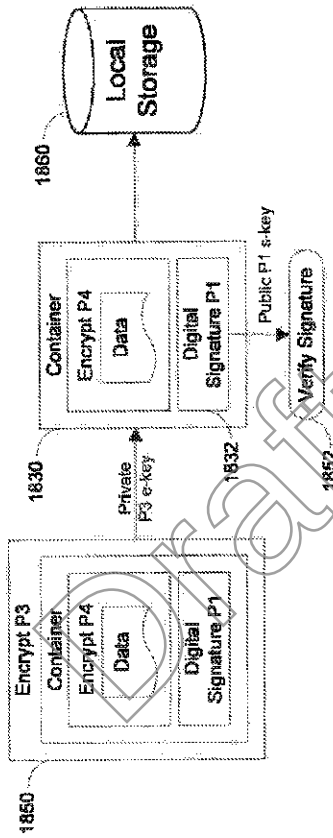
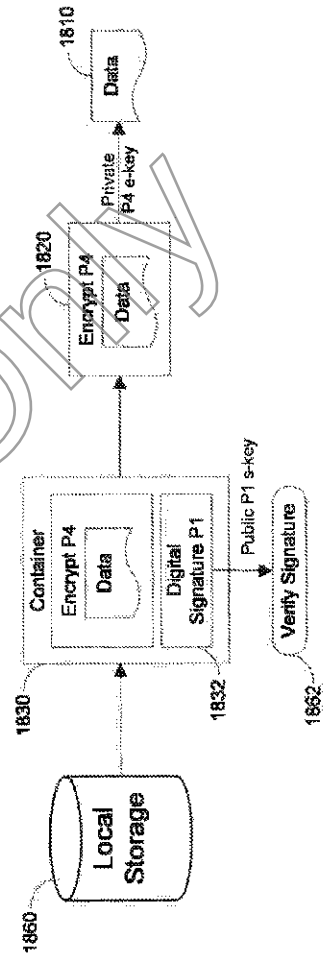
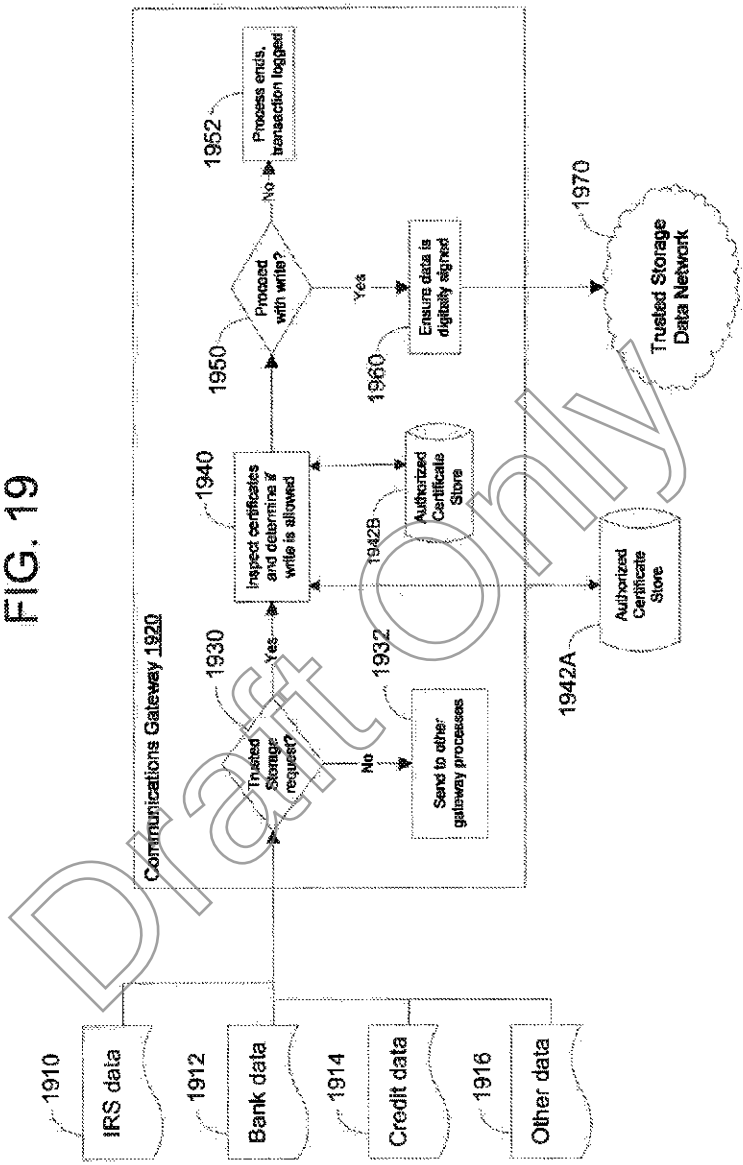


FIG. 18D (P4)



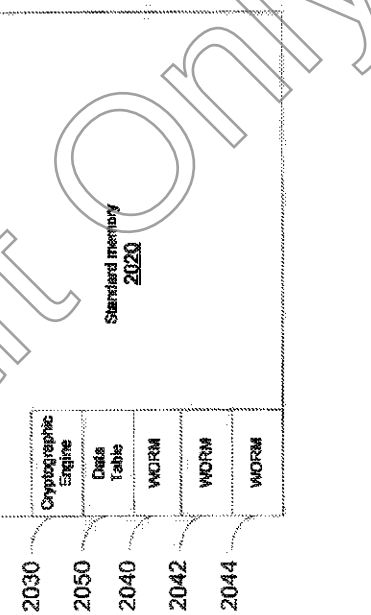
Draft Only

FIG. 19



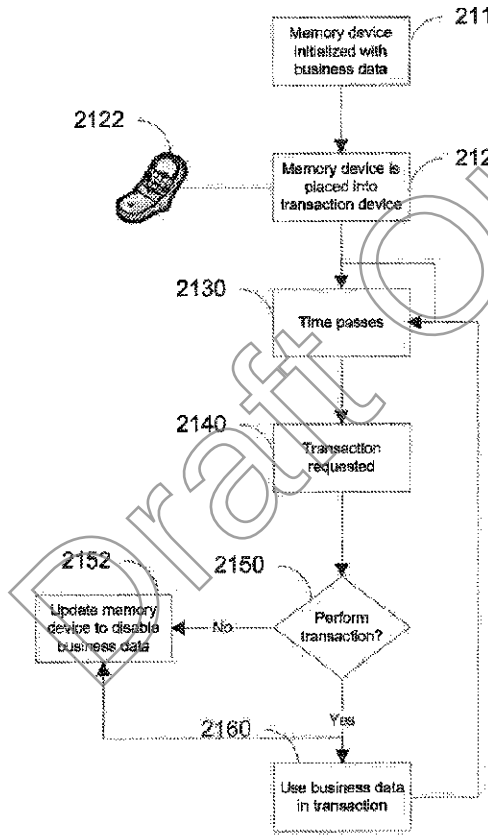
Draft Only

FIG. 20



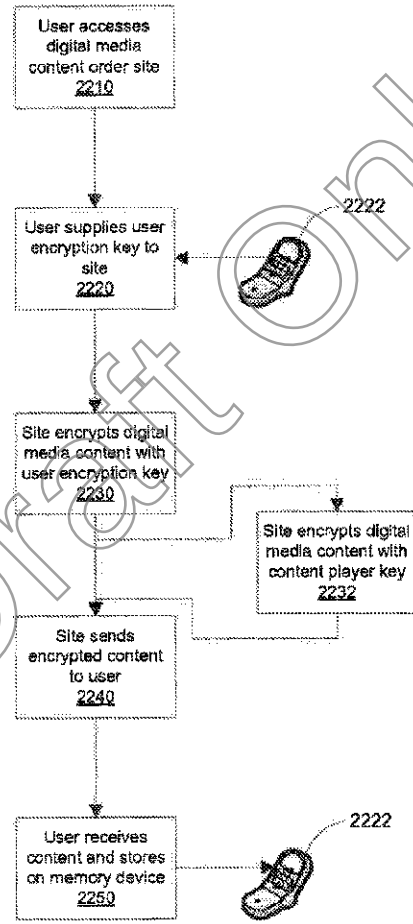
Draft Only

FIG. 21



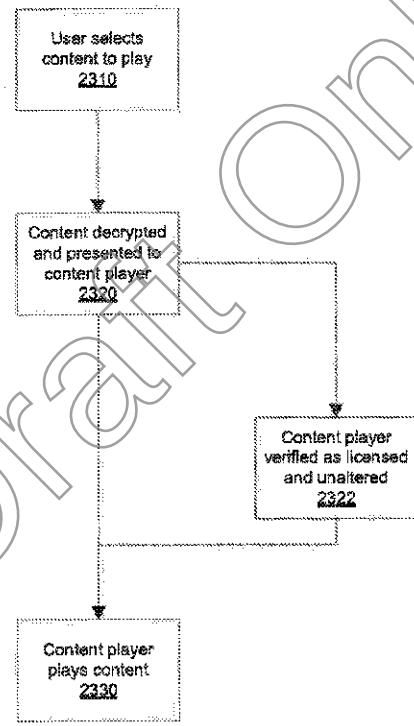
Draft Only

FIG. 22



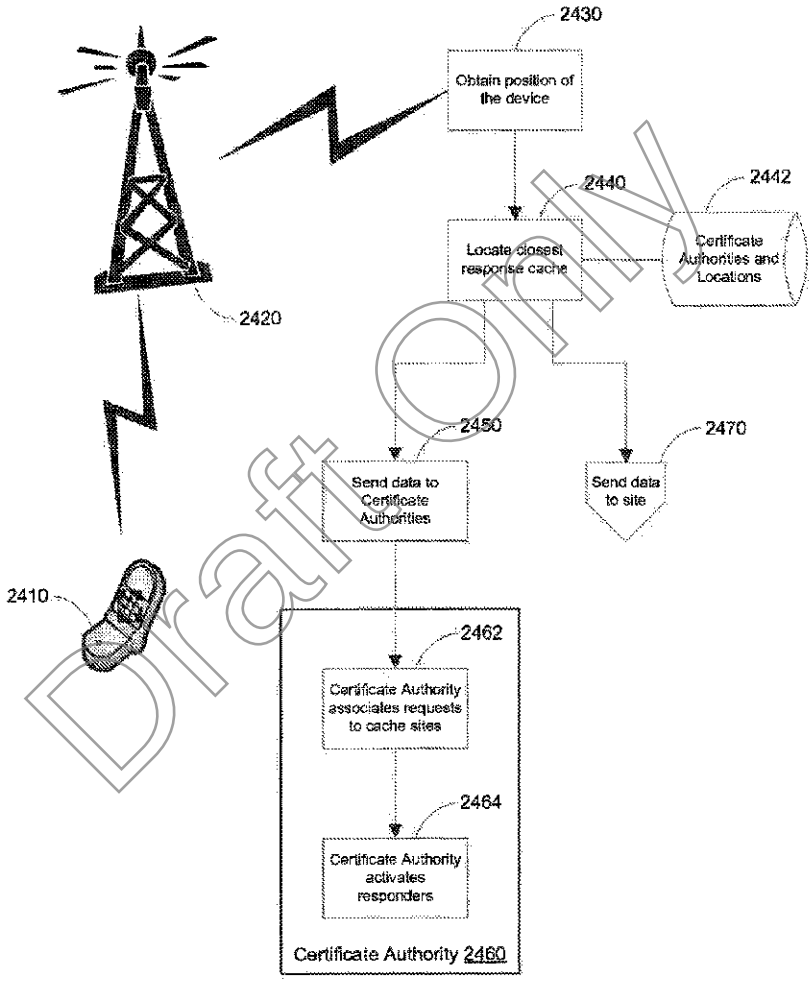
Draft Only

FIG. 23



Draft Only

FIG. 24



Draft Only

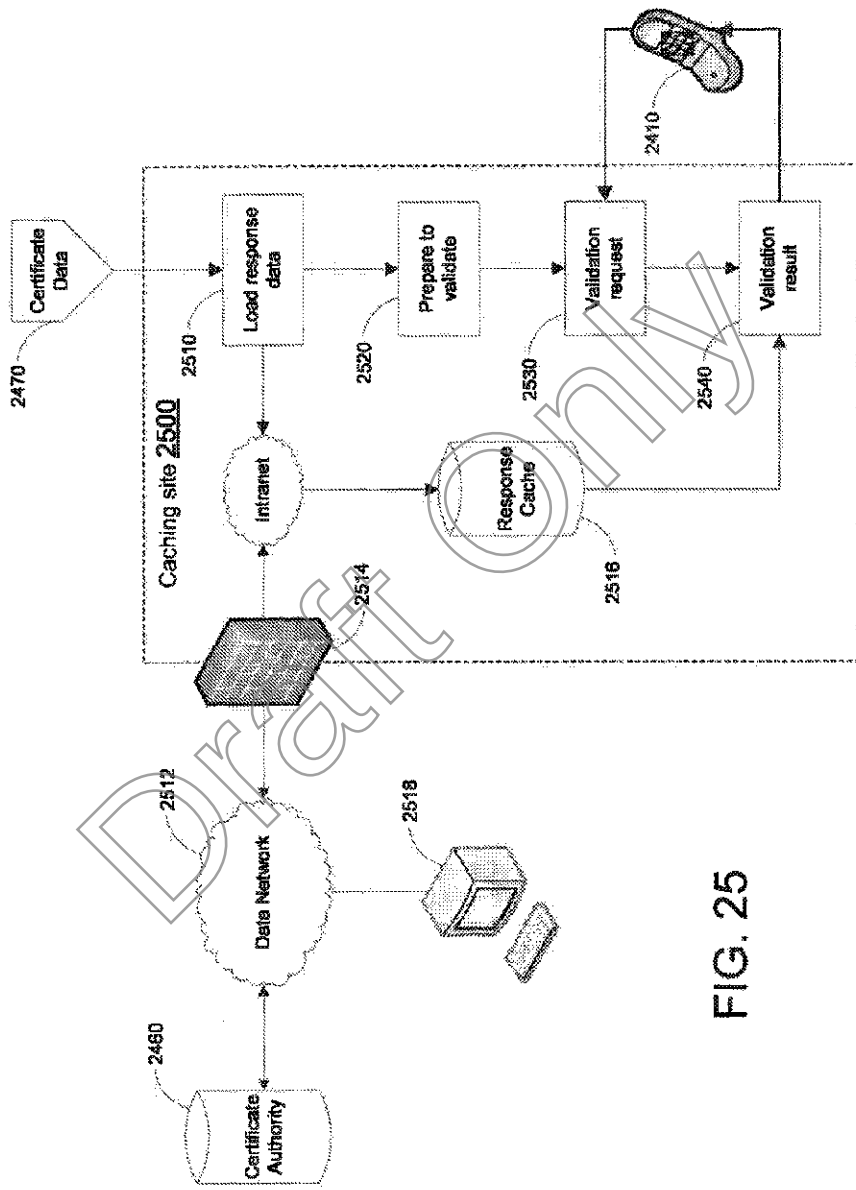
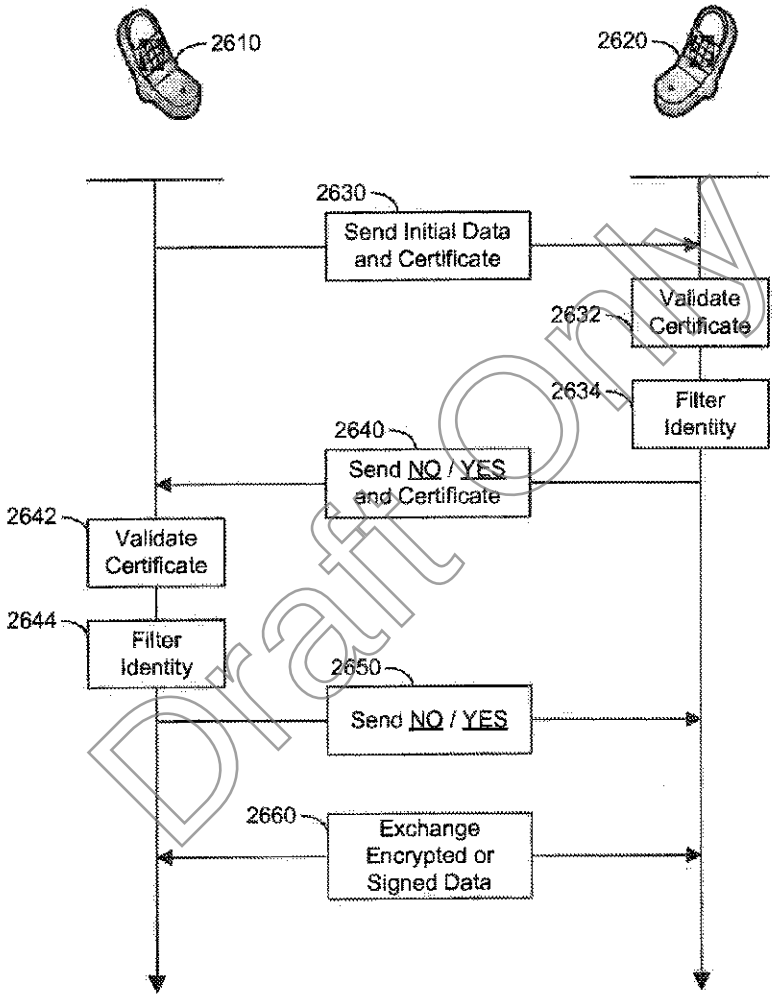


FIG. 25

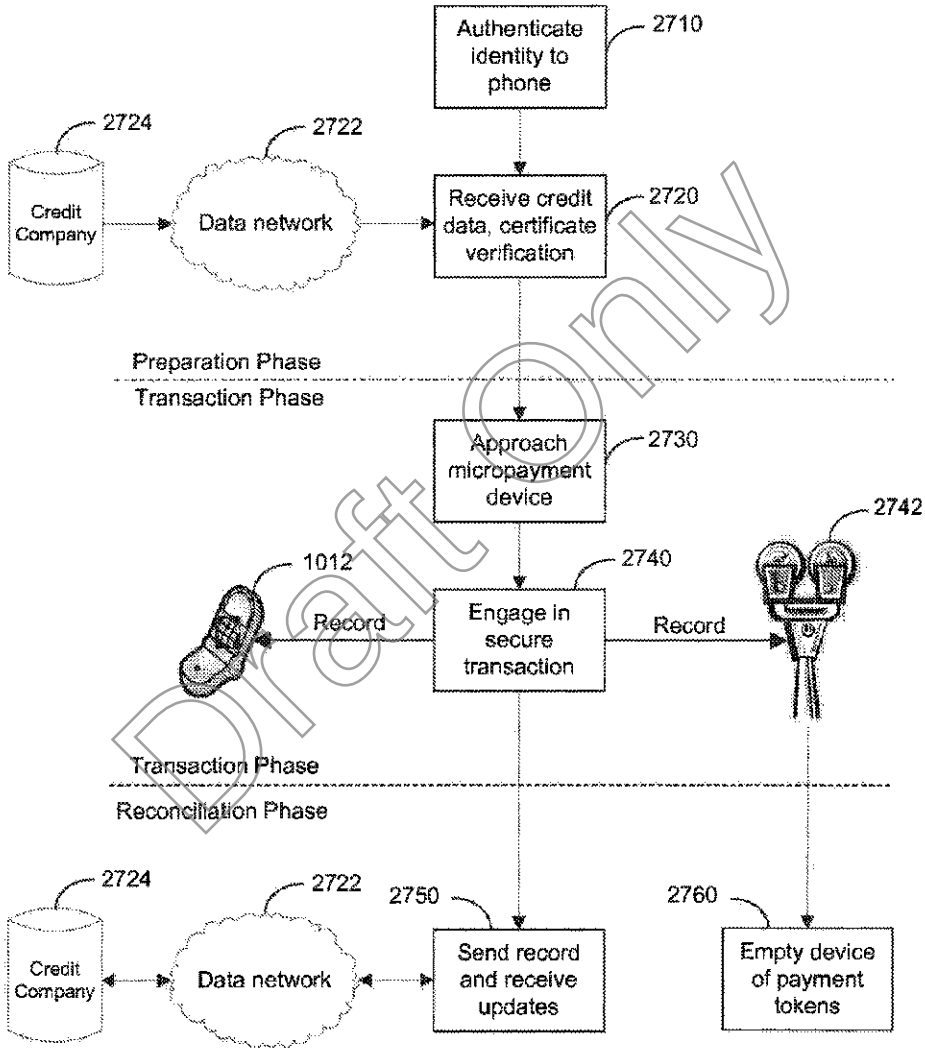
Draft Only

FIG. 26



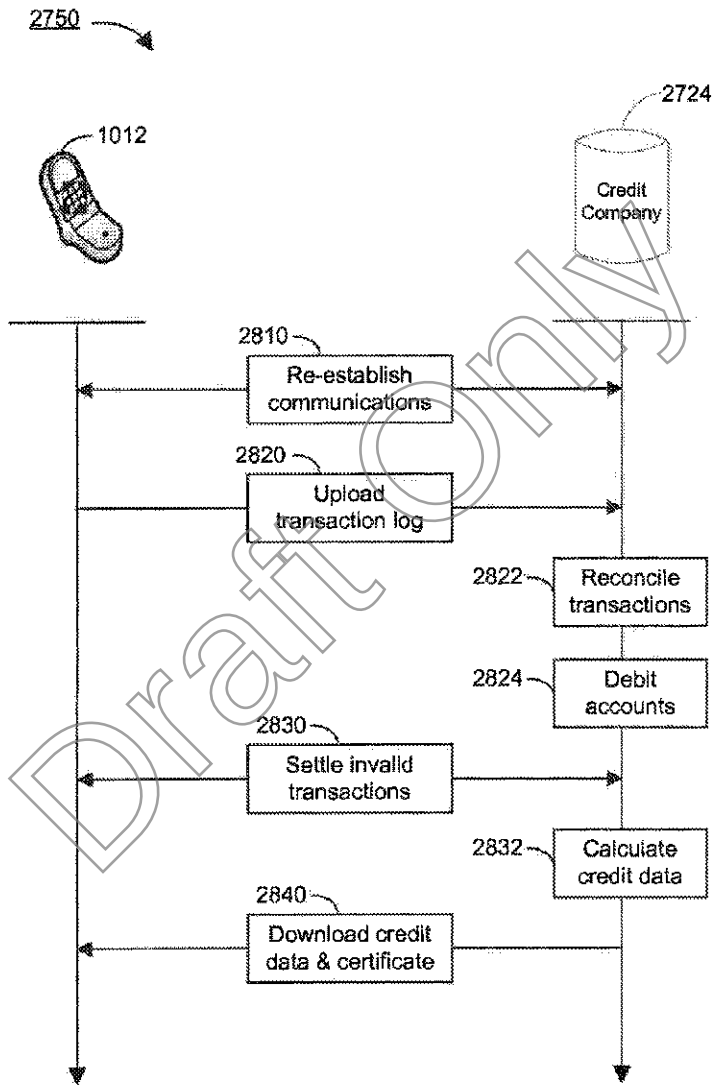
Draft Only

FIG. 27



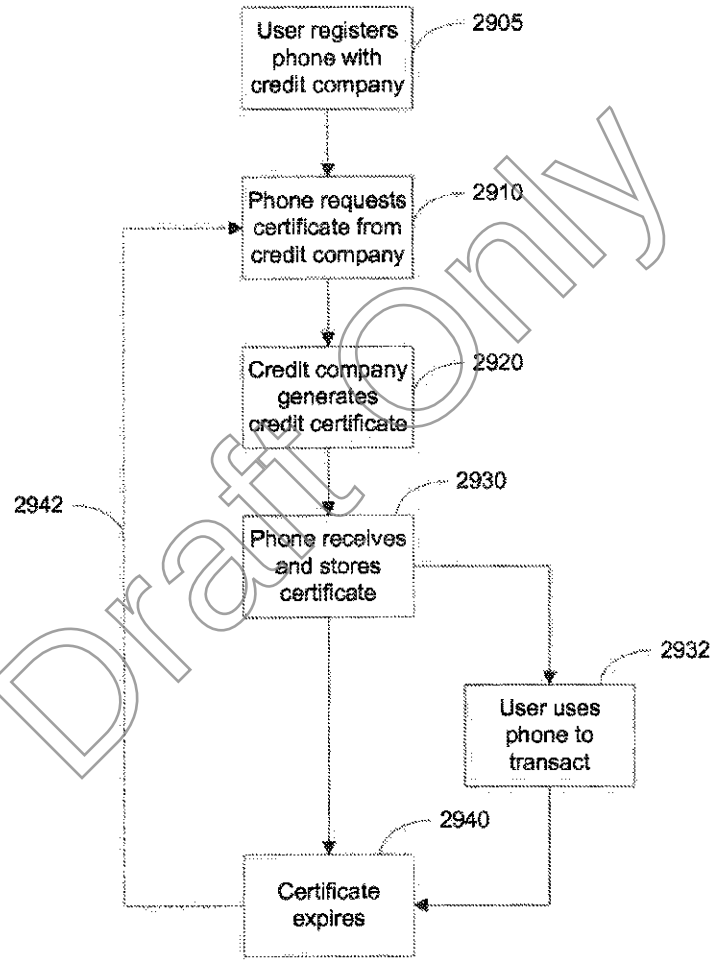
Draft Only

FIG. 28



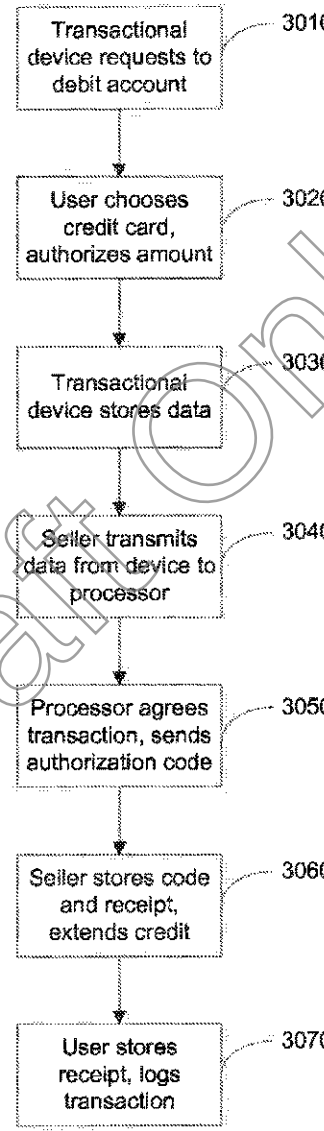
Draft Only

FIG. 29



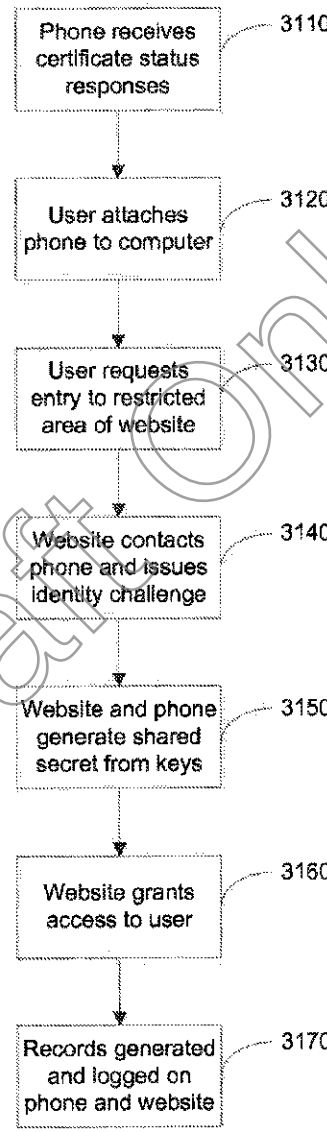
Draft Only

FIG. 30



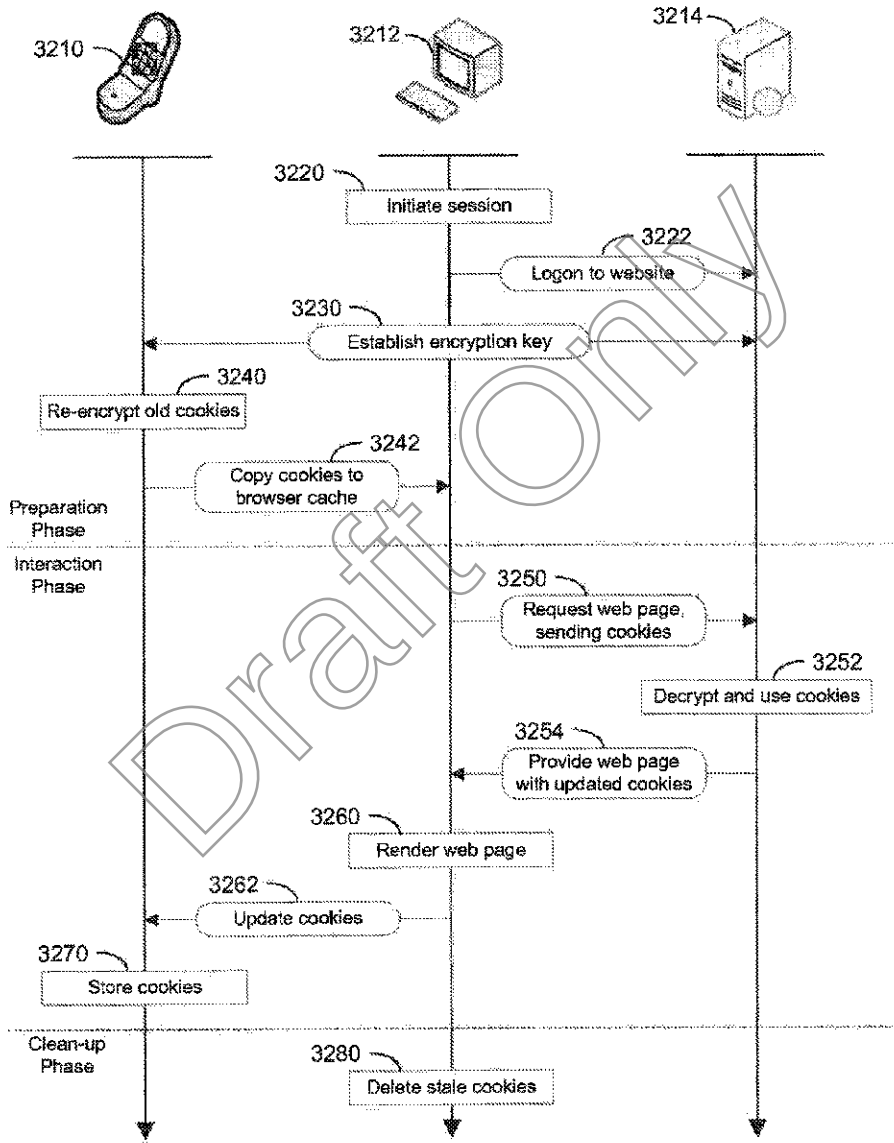
Draft Only

FIG. 31



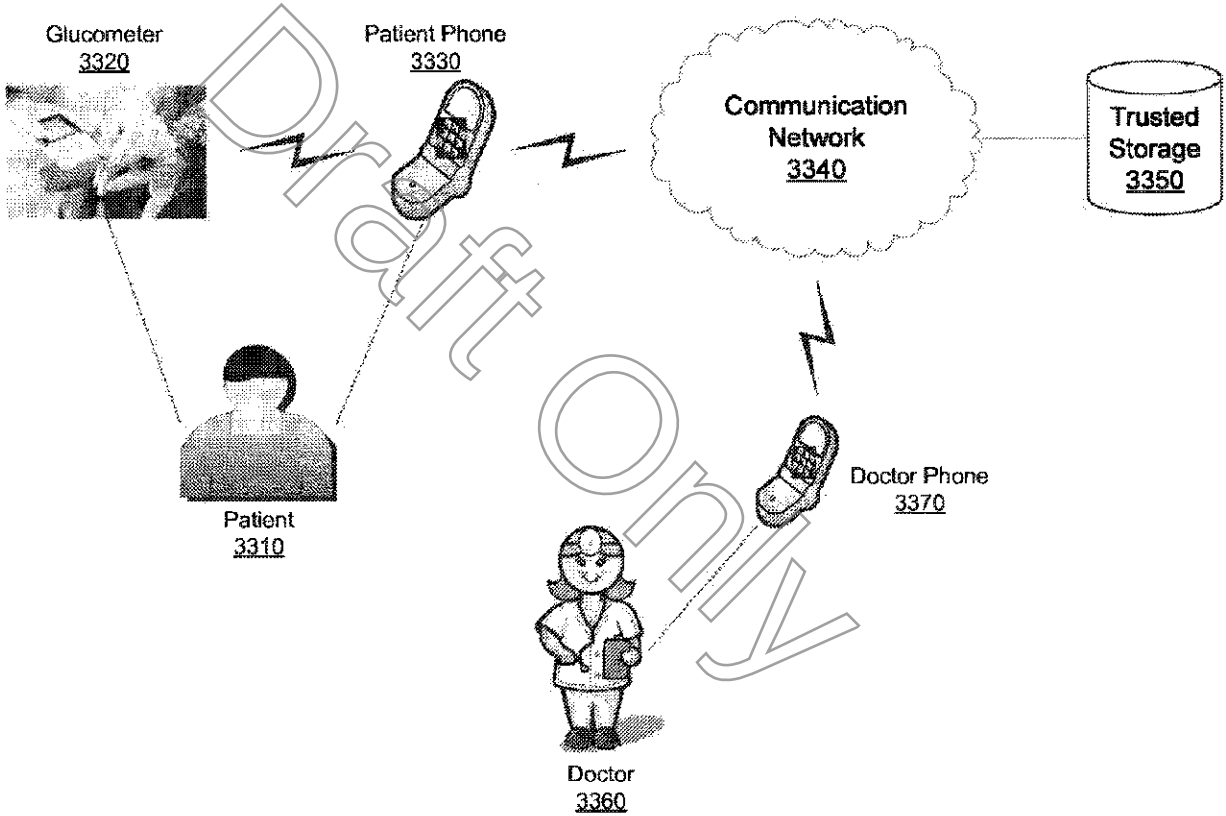
Draft Only

FIG. 32



Draft Only

FIG. 33



Draft Only

CSC ServiceWorks - Ex. 1002
Page 1298 of 1551

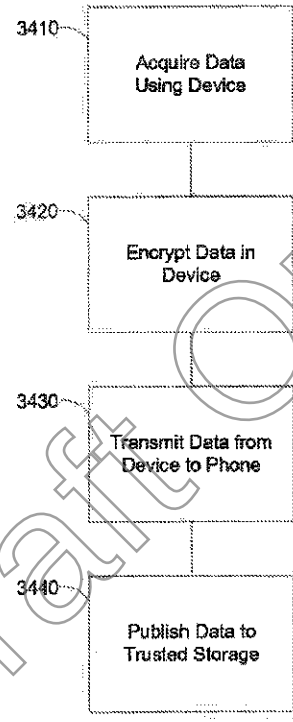


FIG. 34

Draft Only

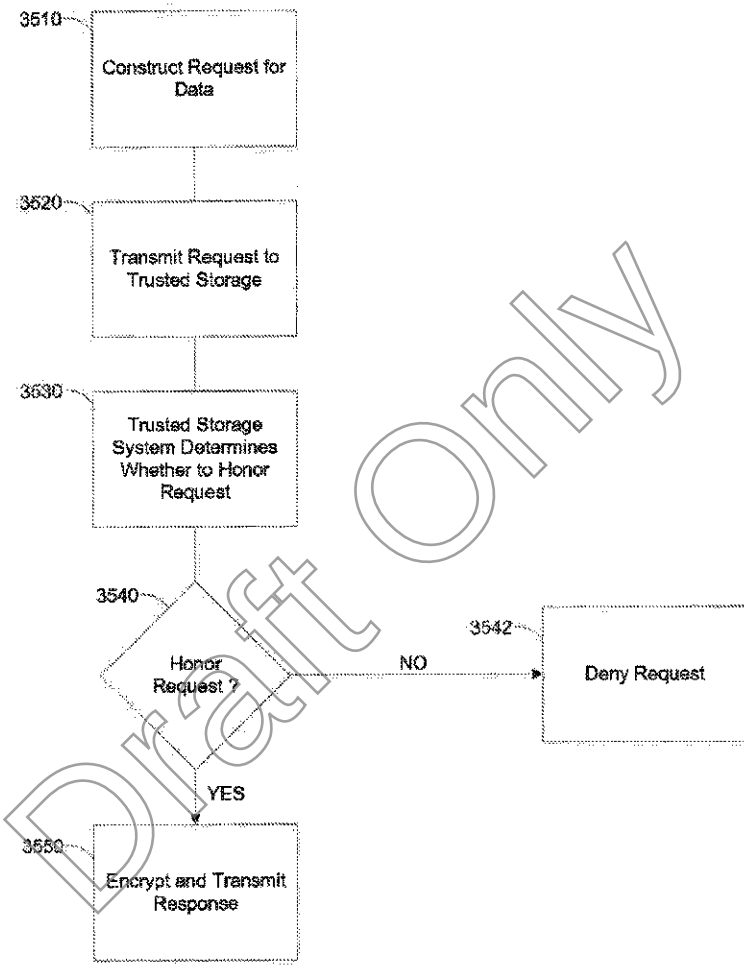


FIG. 35

Draft Only

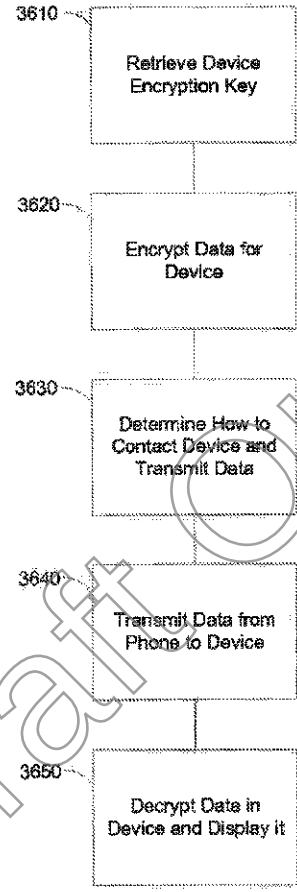


FIG. 36

Draft Only

REMARKS

This amendment responds to the **Track One** office action mailed May 23, 2022. In the **Track One** office action the Examiner:

- rejected claims 1-20 on the ground of obviousness-type double patenting as being unpatentable over claims 1-23 of U.S. Patent No. 9,659,296 B2;
- rejected claims 1-20 on the ground of obviousness-type double patenting as being unpatentable over claims 1-25 of U.S. Patent No. 10,891,614 B2; and
- provisionally rejected claims 1-20 on the ground of obviousness-type double patenting as being unpatentable over claims 2-29 of co-pending U.S. Patent Application No. 17/147,305.

After entry of this amendment, the pending claims are: claims 1-20.

MCKESSON STATEMENT

In view of *McKesson Information Solutions v. Bridge Medical* (Fed. Cir. 2007), Applicant wishes to inform the Examiner that the prosecution history of the following US Patent Applications may contain information relevant to the pending application:

14/214644, 14/320534, 14/335762, 14/611065, 14/641236, 14/321717, 14/321724, 14/321733, 14/456683, 14/968703, 14/614336, 14/458192, 14/458199, 15/893514, 15/435228, 15/878352, 15/603400, 15/406492, 16/029483, 15/956741, 16/681673, 16/748727, 16/750477, 16/934933, 17/529111, 17/147305, 16/934392, 17/216399, 17/443802, 17/654732

The Examiner is encouraged to review the art made of record, office actions, and notices of allowance, if any, in the above-mentioned applications.

REMARKS CONCERNING DOUBLE PATENTING REJECTIONS

I. REJECTION OF CLAIMS 1-20 ON THE GROUND OF OBVIOUSNESS-TYPE DOUBLE PATENTING AS BEING UNPATENTABLE OVER CLAIMS 1-23 OF U.S. PATENT NO. 9,659,296 B2

A terminal disclaimer is being filed concurrently with this response to address this nonstatutory double patenting rejection. The Applicant respectfully requests that this rejection be withdrawn.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1302 of 1551

II. REJECTION OF CLAIMS 1-20 ON THE GROUND OF OBVIOUSNESS-TYPE DOUBLE PATENTING AS BEING UNPATENTABLE OVER CLAIMS 1-25 OF U.S. PATENT NO. 10,891,614 B2

A terminal disclaimer is being filed concurrently with this response to address this nonstatutory double patenting rejection. The Applicant respectfully requests that this rejection be withdrawn.

III. PROVISIONAL REJECTION OF CLAIMS 1-20 ON THE GROUND OF OBVIOUSNESS-TYPE DOUBLE PATENTING AS BEING UNPATENTABLE OVER CLAIMS 2-29 OF CO-PENDING U.S. PATENT APPLICATION NO. 17/147,305

A terminal disclaimer is being filed concurrently with this response to address this nonstatutory double patenting rejection. The Applicant respectfully requests that this rejection be withdrawn.

Draft Only

CONCLUDING REMARKS

By responding in the foregoing remarks only to particular positions asserted by the Examiner, the Applicants do not necessarily acquiesce in other positions that have not been explicitly addressed. In addition, the Applicants' arguments for the patentability of a claim should not be understood as implying that no other reasons for the patentability of that claim exist.

In light of the above amendments and remarks, the Applicants respectfully request that the Examiner reconsider this application with a view towards allowance. The Examiner is invited to call the undersigned attorney at (650) 843-4000, if a telephone call could help resolve any remaining items.

Respectfully submitted,

Date: August 19, 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

CSC ServiceWorks - Ex. 1002
Page 1303 of 1551

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/654,732	**08/19/2022 06:27:21 PM ET**	**104402-5065-US**

Title of Invention

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	5715	FILED BY	Benjamin Pezzner
PATENT CENTER #	60891401	FILING DATE	03/14/2022
CUSTOMER #	24341	FIRST NAMED INVENTOR	Paresh K. Patel
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
petition-request.pdf	3	Terminal Disclaimer-Filed (Electronic)	49 KB
grantLetter.pdf	1	Terminal Disclaimer-Electronic-Approved	19 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
petition-request.pdf	94932D2A2EFD72C6EF1DAA7FAEAF13480DDE269E51A094BF B5777484E7AC19BD27DBA806931FD8A811224A87AEE8F2909

Draft Only

AA312D20F544A16B19EFB951C1D5A1E

grantLetter.pdf

DCBF913273A4C73C7B06D7AE40FE50E3ECF27F5A6CD1F319
1DAC56F425360E284EACA7BC85AD23FF9014763E7B4B44970
40BF7161F72E9947FE8CBD54708B413

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

Draft Only

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/654,732	**08/19/2022 06:37:09 PM ET**	**104402-5065-US**

Title of Invention

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	5715	FILED BY	Benjamin Pezzner
PATENT CENTER #	60891443	FILING DATE	03/14/2022
CUSTOMER #	24341	FIRST NAMED INVENTOR	Paresh K. Patel
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 3

DOCUMENT		PAGES	DESCRIPTION	SIZE (KB)
104402-5065-US Response.pdf		8	-	173 KB
104402-5065-US Response-A....pdf	(1-1)	1	Amendment/Request for Reconsideration-After Non-Final Rejection	120 KB
104402-5065-US Response-CLM.pdf	(2-6)	5	Claims	122 KB
104402-5065-US Response-REM.pdf	(7-8)	2	Applicant Arguments/Remarks Made in an Amendment	146 KB

Draft Only

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
104402-5065-US Response.pdf	3C0C8EA03DB65732C4BE0882CAF90D37A586D14499C153E5B61A6D2AA2040F0FBE236E6FFEB178B88873432A4B0C16493E5238B6309D6D9B1AECB2C1DBC70CD7
104402-5065-US Response-A....pdf	AE868B8E9B317EB4B3512CFA154E78D24147C190F1A88D56D6C65ACEAA4B83CBA84E75370573EC384673D0A0CEA0964E6AEE72FF88ADEEB3293A5DA922FB45F
104402-5065-US Response-CLM.pdf	C4C1CBE11D7AFD021FCCF8252E185A9C85A8FE7AE9429CFED6843C36ABB5002C7737A69A87C8DFC40F3861F53030D49F40EB76EA180E121C9FE2D4E9D572B7D6
104402-5065-US Response-REM.pdf	5B1B8D09529CEBA16965801249201 5CDC2ADFAD29B8F8A35EAF1FA93EA7D412D6E05957A89C5E00A0A659C510E863AE2BF5F8A0B9A82C0C995035CEBBEC7A0A8

Draft Only

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/654,732	08/19/2022 06:27:21 PM ET	104402-5065-US

Title of Invention

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	5715	FILED BY	Benjamin Pezzner
PATENT CENTER #	60891401	AUTHORIZED BY	-
CUSTOMER #	24341	FILING DATE	03/14/2022
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Paresh K. Patel

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 8177	E202208274980279	Benjamin Pezzner

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
2814	STATUTORY DISCLAIMER, INCLUDING TERMINAL DISCLAIMER	170.00	1	170.00
			TOTAL AMOUNT:	$170.00

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

New Applications Under 35 U.S.C. 111

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

Draft Only

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.

Draft Only

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION

APPLICATION #	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET #
17654732	03/14/2022	Paresh Patel	104402-5065-US

Title of Invention

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

✓ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

✓ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent interest
PAYRANGE INC.	100%
Total	100%

The owner(s) of percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number(s)

Application #	Filing Date
17147305	01/12/2021

as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application. The owner hereby agrees that any patent so

Draft Only

granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the reference application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.
In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said reference application, "as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application," in the event that any such patent granted on the pending reference application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

The owner(s) of percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

Patent #
9659295
10891614

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.
In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:

- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

✓ Terminal disclaimer fee under 37 CFR 1.20(d) included with Electronic Terminal Disclaimer request.

Applicant claims the following entity status:

Draft Only

Small

I hereby declare that all statements made herein of my own knowledge are true and that all statemnts made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I certify, in accordance with 37 CFR 1.4(d)(4) that I am: An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application

Signature	Name	Registration #
/Benjamin Pezzner/	Benjamin Pezzner	70711

---

* Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner). Form PTO/SB/96 may be used for making this certification. See MPEP 324.

Draft Only

UNITED STATES
PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

APPROVAL LETTER

APPLICATION #	FILING DATE	APPLICANT/PATENT UNDER REEXAMINATION
17/654,732	03/14/2022	Paresh Patel

Title of Invention

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

Electronic terminal disclaimer filed on 08/19/2022

Approved

This patent is subject to a Terminal Disclaimer

Approved / Disapproved by: Electronic Terminal Disclaimer automatically approved

Draft Only

IN THE CLAIMS:

Rewrite the pending claims and add new claims as follows:

1. (Original) A method of presenting representations of payment accepting unit events, comprising:

at a mobile device with one or more processors, memory, one or more output devices including a display, and one or more radio transceivers:

identifying one or more payment accepting units in proximity to the mobile device that are available to accept payment from a mobile payment application executing on the mobile device, the identifying based at least in part on an identifier corresponding to the one or more payment accepting units, wherein the one or more payment accepting units are payment operated machines that accept payment for dispensing of products and/or services;

displaying a user interface of the mobile payment application on the display of the mobile device, the user interface being configured to display a visual indication of the one or more payment accepting units and accept user input to (i) receive selection by a user of the mobile device of an available payment accepting unit of the one or more payment accepting units and (ii) trigger payment by the mobile payment application for a transaction initiated by the user of the mobile device with the available payment accepting unit of the one or more payment accepting units;

establishing via the one or more radio transceivers a wireless communication path including the mobile device and the available payment accepting unit of the one or more payment accepting units;

after establishing the wireless communication path, enabling user interaction with the user interface of the mobile payment application to complete the transaction;

exchanging information with the available payment accepting unit via the one or more radio transceivers, in conjunction with the transaction; and

after exchanging the information, displaying, on the display, an updated user interface of the mobile payment application to the user of the mobile device.

2. (Original) The method of claim 1, wherein the updated user interface of the mobile payment application includes at least one of:

a message displayed on the display of the mobile device;

a banner notification displayed on a display of the mobile device; and/or

a visual alert from one or more LEDs of the mobile device.

Draft Only

3. (Original) The method of claim 1, wherein the information indicates completion of the transaction between the user of the mobile device and the available payment accepting unit.

4. (Original) The method of claim 3, wherein the mobile device includes a long-range transceiver and the information at least includes an amount of the completed transaction, and the method further comprises:

sending at least the amount of the completed transaction to a server via the long-range transceiver.

5. (Original) The method of claim 1, wherein the information indicates abortion of the transaction initiated by the user of the mobile device.

6. (Original) The method of claim 1, wherein the information indicates failure of the transaction initiated by the user of the mobile device or a malfunction associated with the available payment accepting unit.

7. (Original) The method of claim 1, wherein the mobile device includes an accelerometer and the method further comprises:

based on data from the accelerometer, determining whether the user is walking away from the available payment accepting unit; and

in accordance with a determination that the user is walking away from the available payment accepting unit, canceling the wireless communication path.

8. (Original) The method of claim 1, wherein the information reflects availability of the available payment accepting unit to conduct a transaction.

9. (Original) The method of claim 1, further comprising:

in addition to exchanging the information, receiving, via the one or more radio transceivers, a coupon that is targeted to the user of the mobile device based on the transaction.

10. (Original) The method of claim 1, wherein the user interface of the mobile payment application, after establishing the wireless communication path, indicates that the wireless communication path has been established with the available payment accepting unit.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1315 of 1551

11. (Original) The method of claim 1, wherein the user interface of the mobile payment application, after establishing the wireless communication path, includes:

a visual representation of the available payment accepting unit;

an indication of a prepared balance; and

an affordance that when slid, indicates the initiation of the transaction;

wherein the affordance is slid in response to receiving a user input of swipe on the affordance displayed on the display of the mobile device.

12. (Original) The method of claim 1, wherein the payment operated machines include a payment activated washer, a payment activated dryer, a vending machine, a parking meter, a toll booth, an arcade game, a kiosk, a photo booth, or a ticket dispensing machine.

13. (Original) A mobile device, comprising:

one or more radio transceivers;

one or more output devices including a display;

one or more processors; and

memory storing one or more programs to be executed by the one or more processors, the one or more programs comprising instructions for:

identifying one or more payment accepting units in proximity to the mobile device that are available to accept payment from a mobile payment application executing on the mobile device, the identifying based at least in part on an identifier corresponding to the one or more payment accepting units, wherein the one or more payment accepting units are payment operated machines that accept payment for dispensing of products and/or services;

displaying a user interface of the mobile payment application on the display of the mobile device, the user interface being configured to display a visual indication of the one or more payment accepting units and accept user input to (i) receive selection by a user of the mobile device of an available payment accepting unit of the one or more payment accepting units and (ii) trigger payment by the mobile payment application for a transaction initiated by the user of the mobile device with the available payment accepting unit of the one or more payment accepting units;

establishing via the one or more radio transceivers a wireless communication path including the mobile device and the available payment accepting unit of the one or more payment accepting units;

Draft Only

after establishing the wireless communication path, enabling user interaction with the user interface of the mobile payment application to complete the transaction;

exchanging information with the available payment accepting unit via the one or more radio transceivers, in conjunction with the transaction; and

after exchanging the information, displaying, on the display, an updated user interface of the mobile payment application to the user of the mobile device.

14. (Original) The mobile device of claim 13, wherein identifying the one or more payment accepting units includes identifying a payment activated washer, a payment activated dryer, a vending machine, a parking meter, a toll booth, an arcade game, a kiosk, a photo booth, or a ticket dispensing machine.

15. (Original) A non-transitory computer readable storage medium storing one or more programs, the one or more programs comprising instructions, which, when executed by a mobile device with one or more processors, one or more output devices including a display, and one or more radio transceivers, cause the mobile device to perform operations comprising:

identifying one or more payment accepting units in proximity to the mobile device that are available to accept payment from a mobile payment application executing on the mobile device, the identifying based at least in part on an identifier corresponding to the one or more payment accepting units, wherein the one or more payment accepting units are payment operated machines that accept payment for dispensing of products and/or services;

displaying a user interface of the mobile payment application on the display of the mobile device, the user interface being configured to display a visual indication of the one or more payment accepting units and accept user input to (i) receive selection by a user of the mobile device of an available payment accepting unit of the one or more payment accepting units and (ii) trigger payment by the mobile payment application for a transaction initiated by the user of the mobile device with the available payment accepting unit of the one or more payment accepting units;

establishing via the one or more radio transceivers a wireless communication path including the mobile device and the available payment accepting unit of the one or more payment accepting units;

after establishing the wireless communication path, enabling user interaction with the user interface of the mobile payment application to complete the transaction;

Draft Only

exchanging information with the available payment accepting unit via the one or more radio transceivers, in conjunction with the transaction; and

after exchanging the information, displaying, on the display, an updated user interface of the mobile payment application to the user of the mobile device.

16. (Original) The non-transitory computer readable storage medium of claim 15, wherein the updated user interface of the mobile payment application includes at least one of:

a message displayed on the display of the mobile device;

a banner notification displayed on a display of the mobile device; and/or

a visual alert from one or more LEDs of the mobile device.

17. (Original) The non-transitory computer readable storage medium of claim 15, wherein:

the information indicates completion of the transaction between the user of the mobile device and the available payment accepting unit;

the information at least includes an amount of the completed transaction; and

the instructions further cause the mobile device to send at least the amount of the completed transaction to a server.

18. (Original) The non-transitory computer readable storage medium of claim 15, wherein the information indicates abortion of the transaction initiated by the user of the mobile device.

19. (Original) The non-transitory computer readable storage medium of claim 15, wherein the information indicates failure of the transaction initiated by the user of the mobile device or a malfunction associated with the available payment accepting unit.

20. (Original) The non-transitory computer readable storage medium of claim 15, wherein identifying the one or more payment accepting units includes identifying a payment activated washer, a payment activated dryer, a vending machine, a parking meter, a toll booth, an arcade game, a kiosk, a photo booth, or a ticket dispensing machine.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1318 of 1551

Electronically filed ***, 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:	Poinvil, Frantzy
For:	*Method and System for Presenting Representations of Payment Accepting Unit Events*	Atty. Docket No.:	104402-5065-US

RESPONSE TO **TRACK ONE** OFFICE ACTION & INTERVIEW SUMMARY

Mail Stop: Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The enclosed Amendment is in response to the **Track One** Office Action dated May 23, 2022 for the above-identified patent application.

The Commissioner is hereby authorized to charge any required fee(s) to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 104402-5065-US).

Draft Only

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
17/654,732	03/14/2022	Paresh K. Patel	104402-5065-US

CONFIRMATION NO. 5715

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

PUBLICATION NOTICE

OC00000013470825

Title:METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

Publication No.US-2022-0198450-A1
Publication Date:06/23/2022

Draft Only

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently https://portal.uspto.gov/pair/PublicPair. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	411	(payee$ OR seller$1) adj10 (terminal$1 OR computer$1 OR device$1) adj10 (payment$ OR card$1 OR mobile) adj10 (bluetooth OR wireless$)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/16 06:56 AM
L2	1971	(payee$ OR seller$1) adj15 (terminal$1 OR computer$1 OR mobile OR phone OR device$1) adj15 (id$1 OR identif$) adj15 pay$	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/16 06:58 AM
L3	1189	(Select$ OR chos$or choos$ OR accept$) adj15(payee$ OR seller$1) adj15 (terminal$1 OR computer$1 OR mobile OR phone OR device$1) adj15 (pay$ OR card$1)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/16 07:09 AM
L4	54413	((vending adj5 machine$1) OR kiosk$1) adj15 (mobile$ OR phone$1 OR transceiv$)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/16 07:19 AM
L5	411	L2 AND l3	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/16 07:20 AM
L6	9	L5 AND L4	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/16 07:23 AM
L7	54	L5 AND L1	(US-PGPUB; USPAT; USOCR; FIT (AP, AT,	OR	ON	ON	2022/05/16 07:23 AM

Draft Only

			AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L8	0	(mobile OR wireless OR gps) adj15 accelerometer$1 adj15 (walk$ OR distance$) adj15 (transaction$)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/16 07:47 AM
L9	17	(mobile OR wireless OR gps) SAME accelerometer$1 adj15 (walk$ OR distance$) SAME (transaction$)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/16 07:48 AM

PE2E SEARCH - Search History (Interference)

There are no Interference searches to show.

Draft Only

Dialog

STIC
Electronic and Technical Information Center

Search Strategy from Dialog

May 16 2022 10:05

Draft Only

Search Strategy

Databases: ABI/INFORM® Professional Advanced, Abstracts in New Technology & Engineering, AdisInsight: Drugs, AdisInsight: Trials, Adis Pharmacoeconomics & Outcomes News, AGRICOLA, AGRIS, Allied & Complementary Medicine™, Analytical Abstracts, APA PsycInfo®, Aqualine, Aquatic Science & Fisheries Abstracts (ASFA), Australian Education Index, BIOSIS® Toxicology, BIOSIS Previews®, British Library Inside Conferences, British Nursing Index, Business & Industry, CAB ABSTRACTS, Chemical Business Newsbase, Chemical Engineering & Biotechnology Abstracts, Chemical Safety Newsbase, Civil Engineering Abstracts, ClinicalTrials.gov, Current Contents® Search, Derwent Drug File, Derwent Drug Registry, DH-DATA: Health Administration, Medical Toxicology & Environmental Health, DIOGENES® FDA Regulatory Updates, Drug Information Fulltext, Earthquake Engineering Abstracts, EconLit, Ei Compendex®, Ei EnCompassLIT, Embase®, EMCare®, ERIC, ESPICOM Pharmaceutical & Medical Device News, FDAnews, FLUIDEX (Fluid Engineering Abstracts), Foodline®: MARKET, Foodline®: PRODUCT, Foodline®: SCIENCE, FSTA®, Gale Group Computer Database™, Gale Group Health Periodicals Database, Gale Group New Product Announcements / Plus®, Gale Group Newsletter Database™, Gale Group PharmaBiomed Business Journals, Gale Group PROMT®, Gale Group Trade & Industry Database™, GEOBASE, GeoRef, Global Health, HSELINE: Health and Safety, ICONDA - International Construction Database, IMS Company Profiles, IMS New Product Focus, IMS Pharma Trademarks, IMS R&D Focus, IMS R&D Focus Drug News, Inspec®, International Pharmaceutical Abstracts, Jane's Defense & Aerospace News, King's Fund, KOSMET: Cosmetic Science, Lancet Titles, Material Safety Datasheets - OHS™, Mechanical & Transportation Engineering Abstracts, MEDLINE®, Meteorological & Geoastrophysical Abstracts, Morressier Life Science Conference Abstracts and Posters, New England Journal of Medicine, Northern Light Life Sciences Conference Abstracts, NTIS: National Technical Information Service, Oceanic Abstracts, PAIS International, Paperbase, PAPERCHEM, ProQuest Advanced Tech & Aerospace Professional, ProQuest Biological & Health Science Professional, ProQuest Dissertations and Theses Professional, ProQuest Environmental Science Professional, ProQuest Materials Research Professional, ProQuest Newsstand Professional, ProQuest Technology Research Professional, Prous Science Daily Essentials, Prous Science Drug Data Report, Prous Science Drugs Of The Future™, Publicly Available Content, Registry of Toxic Effects of Chemical Substances (RTECS®), SciSearch®: a Cited Reference Science Database, Social SciSearch®, ToxFile®, Transport Research International Documentation, TULSA™ (Petroleum Abstracts), UBM Computer Full Text, Weldasearch®, Zoological Record

Draft Only

Set#	Searched for	Results
S1	(((payee* or seller[*1]) pre/10 (terminal[*1] or computer[*1] or device[*1])) pre/10 (payment* or card[*1] or mobile)) pre/10 (bluetooth or wireless*)	17*
S2	(((payee* or seller[*1]) pre/15 (terminal[*1] or computer[*1] or mobile or phone or device[*1])) pre/15 (id[*1] or identif*)) pre/15 pay*	116*
S3	(((Select* or chos* or choos* or accept*) pre/15 (payee* or seller[*1])) pre/15 (terminal[*1] or computer[*1] or mobile or phone or device[*1])) pre/15 (pay* or card[*1])	61*
S4	((vending pre/5 machine[*1]) or kiosk[*1]) pre/15 (mobile* or phone[*1] or transceiv*)	41761*
S5	((mobile or wireless or gps) near/40 accelerometer[*1] pre/15 (walk* or distance*)) near/40 (transaction*)	8*
S6	s2 and s4	0*
S7	s4 and ((payment[*1] or paying) pre/8 (trigg* or	1109*

	transaction[*1]))	
S8	(((Select* or chos* or choos* or accept*) or pre/15 or (payee* or seller[*1])) or pre/15 or (terminal[*1] or computer[*1] or mobile or phone or device[*1]))	258307359*
S9	s7 and s8	1109°
S10	s9 and mobile and accelerat*	280°

* Duplicates are removed from the search, but included in the result count.

° Duplicates are removed from the search and from the result count.

Draft Only

Contact ProQuest
Copyright © 2022 ProQuest LLC. All rights reserved. - Terms and Conditions

Draft Only

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/654,732	Patel, Paresh K.
	Examiner	Art Unit
	FRANTZY POINVIL	3698

CPC - Searched*		
Symbol	Date	Examiner
G06Q20/40; G06Q20/18; G06Q20/322; G06Q20/3226; G06Q20/327; G06Q20/3278; G07F7/0893; G07F9/023	05/16/2022	FP

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
705	3-44	05/16/2022	FP

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
See the attached DAV and Proquest searches.	05/16/2022	FP

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

Draft Only

/FRANTZY POINVIL/ Primary Examiner, Art Unit 3698	

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/654,732	Patel, Paresh K.
	Examiner	Art Unit
	FRANTZY POINVIL	3698

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	05/16/2022								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1328 of 1551

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/654,732	03/14/2022	Paresh K. Patel	104402-5065-US	5715

24341 7590 05/23/2022

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

EXAMINER
POINVIL, FRANTZY

ART UNIT	PAPER NUMBER
3698	

NOTIFICATION DATE	DELIVERY MODE
05/23/2022	ELECTRONIC

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

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

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

padocketingdepartment@morganlewis.com
vskliba@morganlewis.com

Draft Only

Office Action Summary	Application No. 17/654,732	Applicant(s) Patel, Paresh K.	
	Examiner FRANTZY POINVIL	Art Unit 3698	AIA (FITF) Status Yes

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

Period for Reply

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

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

Status

1)☑ Responsive to communication(s) filed on 3/14/2022.

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

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

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

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

Disposition of Claims*

5) ☑ Claim(s) 1-20 is/are pending in the application.

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

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-20 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

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

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

Application Papers

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

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

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

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

Priority under 35 U.S.C. § 119

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

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

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

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

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

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

Attachment(s)

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

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

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

4) ☐ Other: _____.

Draft Only

DETAILED ACTION

Notice of Pre-AIA or AIA Status

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

Double Patenting

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See In re Goodman, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); In re Longi, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); In re Van Ornum, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); In re Vogel, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and. In re Thorington, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-20 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-23 of U.S. Patent No. 9,659,296. Although the

Draft Only

conflicting claims are not identical, they are not patentably distinct from each other because claims 1-20 of the instant application are directed to a similar subject matter contained in claims 1-23 of the '296 patent. The only difference between the instant application and the '296 patent is merely a labeling difference. It is noted that all the features of claims 1-20 are contained in claims 1-23 of the '296 patent.

Claims 1-20 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-25 of U.S. Patent No. 10,891,614. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1-20 of the instant application are directed to a similar subject matter contained in claims 1-25 of the '614 patent. The only difference between the instant application and the '614 patent is merely a labeling difference. It is noted that all the features of claims 1-20 are contained in claims 1-25 of the '614 patent.

Claims 1-20 are provisionally rejected under the Judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 2-29 of copending Application No. 17,147,305. Although the conflicting claims are not patentably distinct from each other because claims 1-20 of the instant application are directed to a similar subject matter contained in claims 2-29 of the '305 application. Both inventions are obvious variations of each other achieving the same end result. It would have been obvious to one of ordinary skill in the art to note that the features of claims 1-20 of the instant application are contained in claims 2-29 of the '305 application.

Draft Only

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

3. The prior art taken alone or in combination failed to teach or disclose the limitations of claims 1, 13 and 15.

Wheeler (US Pub. No. 20180374076) discloses a system and method for performing automated operations to identify one or more computing devices associated with potential payees that are within a defined proximity of a user mobile device. A processor-based computing system retrieves stored photographic and biographic information regarding the identified potential payees, and displays the retrieved photographic and biographic information for possible selection by a user of the mobile device. One or more payments from the user of the mobile device may be specified and initiated via the processor-based computing system to potential payees selected by the user, including for partial or full payment of a customer order of the user with a merchant associated with an identified point-of-sale computing system.

Ganesan (US Pub. No. 20180197167) discloses a person-to-person (P2P) payment system for providing a payment from a payer to a payee without the payer identifying a payee payment receiving preference. The payment system includes a setup system for setting up payment between the payer and the payee and a messaging system for handling messages between the payer and the payment system and the payee and the payment system, including communications with the payee by way of a payee phone number or email address provided by the payer. A risk assessment system determines a risk score for the P2P transaction and, based on that score, the bank of the payer provides a guarantee to the bank of the payee.

Draft Only

Conclusion

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to FRANTZY POINVIL whose telephone number is (571)272-6797. The examiner can normally be reached M-Th 7:00AM to 5:30PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Michael Anderson** can be reached on 571-270-0508. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/fp/

/FRANTZY POINVIL/
Primary Examiner, Art Unit 3698

May 16, 2022

Draft Only

Notice of References Cited	Application/Control No. 17/654,732	Applicant(s)/Patent Under Reexamination Patel, Paresh K.	
	Examiner FRANTZY POINVIL	Art Unit 3698	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20190236586-A1	08-2019	Mei; Jingqing	G06Q20/34	1/1
*	B	US-20180374076-A1	12-2018	Wheeler; Therman	G06Q20/3224	1/1
*	C	US-20180197167-A1	07-2018	Ganesan; Ravi	G06Q20/4016	1/1
*	D	US-20080040265-A1	02-2008	Rackley III; Brady Lee	G06Q20/3255	705/40
*	E	US-11227275-B2	01-2022	Van Heerden; Lauren	G06Q20/383	1/1
*	F	US-10380573-B2	08-2019	Lin; Gloria	G06Q20/3278	1/1
*	G	US-20040122685-A1	06-2004	Bunce, Daryl	G06Q20/04	705/325
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

Draft Only

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/654,732	03/14/2022	Paresh K. Patel	104402-5065-US	5715

24341 7590 04/18/2022
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER
CENTRAL, DOCKET

ART UNIT	PAPER NUMBER
OPAP	

NOTIFICATION DATE	DELIVERY MODE
04/18/2022	ELECTRONIC

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

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

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

padocketingdepartment@morganlewis.com
vskliba@morganlewis.com

Draft Only

Decision Granting Request for Prioritized Examination (Track I)	**Application No.** 17/654,732	**Applicant(s)** Patel, Paresh K.	
	Examiner CHERYL P GIBSON BAYLOR	**Art Unit** OPET	**AIA (FITF) Status** Yes

1. THE REQUEST FILED 14 March 2022 IS **GRANTED** .

The above-identified application has met the requirements for prioritized examination

A. ☑ for an original nonprovisional application (Track I).
B. ☐ for an application undergoing continued examination (RCE).

2. **The above-identified application will undergo prioritized examination**. The application will be accorded special status throughout its entire course of prosecution until one of the following occurs:

A. filing a **petition for extension of time** to extend the time period for filing a reply;

B. filing an **amendment to amend the application to contain more than four independent claims, more than thirty total claims**, or a multiple dependent claim;

C. filing a **request for continued examination** ;

D. filing a notice of appeal;

E. filing a request for suspension of action;

F. mailing of a notice of allowance;

G. mailing of a final Office action;

H. completion of examination as defined in 37 CFR 41.102; or

I. abandonment of the application.

Draft Only

Telephone inquiries with regard to this decision should be directed to CHERYL GIBSON BAYLOR at (571)272-3213. In his/her absence, calls may be directed to Petition Help Desk at (571) 272-3282.

/CHERYL GIBSON BAYLOR/ Paralegal Specialist, OPET	

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 17/654,732

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	80		N/A	
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	350		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	400		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*	x 50 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 240 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	830		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE(S)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE(S)	OTHER THAN SMALL ENTITY ADDITIONAL FEE(S)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

Draft Only

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
17/654,732	03/14/2022		830	104402-5065-US	20	3

CONFIRMATION NO. 5715

FILING RECEIPT

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

Date Mailed: 03/18/2022

Draft Only

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

Paresh K. Patel, Portland, OR;

Applicant(s)

PAYRANGE INC., Portland, OR;

Power of Attorney: The patent practitioners associated with Customer Number 24341

Domestic Priority data as claimed by applicant

This application is a CON of 17/147,305 01/12/2021
which is a CON of 15/603,400 05/23/2017 PAT 10891614
which is a CON of 14/458,199 08/12/2014 PAT 9659296
which is a CIP of 14/456,683 08/11/2014 PAT 9256873
which is a CON of 14/335,762 07/18/2014 PAT 9547859
which is a CON of 14/214,644 03/14/2014 PAT 8856045
which claims benefit of 61/917,936 12/18/2013
and is a CIP of 29/477,025 12/18/2013 PAT D755183

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 03/17/2022
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/654,732**
Projected Publication Date: 06/23/2022
Non-Publication Request: No
Early Publication Request: No
**** SMALL ENTITY ****
Title

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

Preliminary Class

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative,

Draft Only

this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

Draft Only

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

Draft Only

PTO/SB/424 (12-11)

CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION UNDER 37 CFR 1.102(e) (Page 1 of 1)

First Named Inventor:	Paresh K. Patel	Nonprovisional Application Number (if known):	
Title of Invention:	METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION FOR THE ABOVE-IDENTIFIED APPLICATION.

1. The processing fee set forth in 37 CFR 1.17(i), the prioritized examination fee set forth in 37 CFR 1.17(c), and if not already paid, the publication fee set forth in 37 CFR 1.18(d) have been filed with the request. The basic filing fee, search fee, examination fee, and any required excess claims and application size fees are filed with the request or have been already been paid.

2. The application contains or is amended to contain no more than four independent claims and no more than thirty total claims, and no multiple dependent claims.

3. The applicable box is checked below:

I. ☑ Original Application (Track One) - Prioritized Examination under § 1.102(e)(1)

i. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.

---OR---

(b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper.

ii. An executed oath or declaration under 37 CFR 1.63 is filed with the application.

II. ☐ Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)

i. A request for continued examination has been filed with, or prior to, this form.
ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Draft Only

Signature /Benjamin Pezzner/	Date March 14, 2022
Name (Print/Typed) Benjamin Pezzner	Practitioner Registration Number 70711

Note: *Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required in accordance with 37 CFR 1.33 and 11.18. Please see 37 CFR 1.4(d) for the form of the signature. If necessary, submit multiple forms for more than one signature, see below*.*

☐ *Total of _____ forms are submitted.

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

PRIORITY

[0001] The present application is:

- a continuation of U.S. Patent Application No. 17/147,305, filed January 12, 2021,
- which is a continuation of U.S. Patent Application No. 15/603,400, filed May 23, 2017 and issued as U.S. Patent No. 10,891,614 on January 12, 2021,
- which is a continuation of U.S. Patent Application No. 14/458,199, filed August 12, 2014 and issued as U.S. Patent No. 9,659,296 on May 23, 2017,
- which is a continuation-in-part of U.S. Patent Application Number 14/456,683, filed August 11, 2014 and issued as U.S. Patent No. 9,256,873 on February 9, 2016,
- which is a continuation of U.S. Patent Application Number 14/335,762, filed July 18, 2014 and issued as U.S. Patent No. 9,547,859 on January 17, 2017,
- which is a continuation of U.S. Patent Application Number 14/214,644, filed March 14, 2014 and issued as U.S. Patent No. 8,856,045 on October 7, 2014,
- which claims priority to U.S. Provisional Patent Application Number 61/917,936, filed December 18, 2013,
- U.S. Patent Application Number 14/214,644, filed March 14, 2014, is also a continuation-in-part of U.S. Design Patent Application Number 29/477,025, filed December 18, 2013 and issued as U.S. Design Patent No. D755,183 on May 3, 2016.

The present application is based on and claims priority to these applications, the disclosures of which are hereby incorporated by reference in their entirety.

Draft Only

TECHNICAL FIELD

[0002] The present application relates to the field of payment processing systems, and in particular, to a mobile-device-to-machine payment processing system over a non-persistent network connection.

CSC ServiceWorks - Ex. 1002
Page 1344 of 1551

BACKGROUND

[0003] Vending machines (or "automatic retailing" machines), in the broadest sense, have been around for thousands of years. The first simple mechanical coin operated vending machines were introduced in the 1880s. Modern vending machines stock many different types of products including, but not limited to drinks (e.g., water, juice, coffee, and soda) and edible food products/items (e.g., snacks, candy, fruit, and frozen meals), as well as a wide variety of non-food items. In this fast paced world, vending machines are ubiquitous.

[0004] Vending machines are one type of "payment accepting unit" (payment accepting units are also referred to herein generically as "machines"). A payment accepting unit (or machine) is equipment that requires payment for the dispensing of products and/or services. In addition to vending machines, payment accepting units can also be other machines that require payment for the dispensing of a product and/or services including, but not limited to parking meters, toll booths, laundromat washers and dryers, arcade games, kiosks, photo booths, toll booths, transit ticket dispensing machines, and other known or yet to be discovered payment accepting units.

[0005] In using a payment accepting unit, a user will (1) approach the payment accepting unit, (2) determine from the face of the payment accepting unit the product (or service) he/she desires, (3) insert payment (e.g., coins, bills, or payment cards), and (4) input his/her selection into the payment accepting unit using a user interface (e.g., a series of buttons, a key pad, touch screen, or other input mechanism using, for example, the column and row at which a product is located). Based on the user's inputted selection, technology within the payment accepting unit provides the desired product (or service) to the user.

[0006] As the number of people with Internet-connected mobile devices proliferates, so does the variety of uses for such devices. Mobile payment is a logical extension. There is a large development effort around bringing mobile payment to the retail sector in an effort to not only provide options to the user, but also increased convenience.

SUMMARY

[0007] Disclosed herein is a payment processing system or, more specifically, a mobile-device-to-machine payment processing system over a non-persistent network connection with

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1345 of 1551

hands-free mode and manual mode (sometimes also herein called "swipe" or "swipe-to-pay" mode).

[0008] In some implementations, a method of presenting representations of payment accepting unit events is performed at a device (e.g., the mobile device 150, Figures 5 and 21) with one or more processors, memory, one or more output devices, and two or more communication capabilities. After sending a request to a payment module (e.g., the adapter module 100, Figures 5 and 20), via a first communication capability (e.g., a short-range communication technology/protocol such as BLE), to initiate a transaction with a payment accepting unit (e.g., the payment accepting unit 120, Figures 5 and 19) (sometimes also herein called "machine 120") associated with the payment module, the method includes obtaining a notification from the payment module via the first communication capability, where the notification indicates an event at the payment accepting unit associated with the payment module. In response to obtaining the notification, the method includes providing a representation of the notification to a user of the mobile device via the one or more output devices of the mobile device (e.g., a message displayed on a display of the mobile device, a vibration produced by a vibration mechanism of the mobile device, an aural alert produced by a speaker of the mobile device, and/or the like).

[0009] In some implementations, a method of retrofitting an offline-payment operated machine to accept electronic payments is performed at a payment module (e.g., the adapter module 100, Figures 5 and 20) with one or more processors, memory, a short-range communication capability (e.g., a short-range communication technology/protocol such as BLE), and a first interface module configured to couple the payment module with a control unit of an offline-payment operated machine (e.g., the payment accepting unit 120, Figures 5 and 19) (sometimes also herein called "machine 120"). The method includes receiving a transaction request via the short-range communication capability from a respective mobile device to perform a transaction with the offline-payment operated machine. The method includes validating the transaction request, where validation of the transaction request indicates that the respective mobile device is authorized to initiate payment for the transaction by a remote server (e.g., the server 130, Figures 5 and 22) via the long-range communication capability (e.g., the long-range communication technology/protocol such as GSM, CDMA, or Wi-Fi). In accordance with a determination that the transaction request is valid, the method includes causing the offline-

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1346 of 1551

payment operated machine to perform the requested transaction by issuing a signal to perform the transaction to the control unit of the offline-payment operated machine via the first interface module.

[0010] In some implementations, a device (e.g., the machine 120, (Figures 5 and 19), the adapter module 100 (Figures 5 and 20), the mobile device 150 (Figures 5 and 21), the server 130 (Figures 5 and 22), or a combination thereof) includes one or more processors and memory storing one or more programs for execution by the one or more processors, the one or more programs include instructions for performing, or controlling performance of, the operations of any of the methods described herein. In some implementations, a non-transitory computer readable storage medium storing one or more programs, the one or more programs comprising instructions, which, when executed by a device (e.g., the machine 120, (Figures 5 and 19), the adapter module 100 (Figures 5 and 20), the mobile device 150 (Figures 5 and 21), the server 130 (Figures 5 and 22), or a combination thereof) with one or more processors, cause the computer system to perform, or control performance of, the operations of any of the methods described herein. In some implementations, a device (e.g., the machine 120, (Figures 5 and 19), the adapter module 100 (Figures 5 and 20), the mobile device 150 (Figures 5 and 21), the server 130 (Figures 5 and 22), or a combination thereof) includes means for performing, or controlling performance of, the operations of any of the methods described herein.

[0011] The subject matter described herein is particularly pointed out and distinctly claimed in the concluding portion of this specification. Objectives, features, combinations, and advantages described and implied herein will be more readily understood upon consideration of the following detailed description of the invention, taken in conjunction with the accompanying drawings.

Draft Only

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] Figure 1 is a schematic diagram that shows three zones: a "communication zone" (e.g., Bluetooth range), an "authorization zone," and a "payment zone" in accordance with some implementations.

[0013] Figure 2 is a schematic diagram that shows the three zones of Figure 1 with multiple users therein in accordance with some implementations.

CSC ServiceWorks - Ex. 1002
Page 1347 of 1551

[0014] Figure 3 is a table that illustrates the hands-free credit or alert user principle in accordance with some implementations.

[0015] Figure 4 is a flow chart showing the logging received signal strength indicator (RSSI) information in accordance with some implementations.

[0016] Figure 5 is a block schematic that shows elements of the payment processing system including, but not limited to, the adapter module, the machine, the mobile device, and servers, as well as communications therebetween in accordance with some implementations.

[0017] Figure 6 is a block schematic that shows three areas of encryption used (each is bi-directional) between the adapter module, the machine, the mobile device, and/or servers in accordance with some implementations.

[0018] Figure 7 is a block diagram that shows communications, messaging, vending sequence, and purchase flow between the adapter module, the mobile device, and a system management server in accordance with some implementations.

[0019] Figure 8A is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) when the user enters the "communication zone" (e.g., Bluetooth range) in accordance with some implementations.

[0020] Figure 8B is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) when the user enters the "authorization zone" in accordance with some implementations.

[0021] Figure 8C is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) when the user enters the "payment zone" and, in particular, detailing a hands-free mode embodiment and a swipe mode embodiment in accordance with some implementations.

[0022] Figure 8D is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1348 of 1551

sequence, and purchase flow) in a vending transaction including a loop for multiple transactions in accordance with some implementations.

[0023] Figure 8E is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) in the login mode in accordance with some implementations.

[0024] Figure 8F is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) during boot-up of the adapter module in accordance with some implementations.

[0025] Figure 8G is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) during an account check/update process in accordance with some implementations.

[0026] Figures 9A-9E are flow charts that show example steps and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) in accordance with some implementations.

[0027] Figures 10A-10D show a mobile device with a graphical representation of a mobile application shown thereon, the mobile application being used as part of the mobile-device-to-machine payment processing system in accordance with some implementations.

[0028] Figure 11 is a perspective view of the in-line dongle adapter module in accordance with some implementations.

[0029] Figure 12 is a front plan view of the in-line dongle adapter module of Figure 11 in accordance with some implementations.

[0030] Figure 13 is a back plan view of the in-line dongle adapter module of Figure 11 in accordance with some implementations.

[0031] Figure 14 is a side view of the in-line dongle adapter module of Figure 11 in accordance with some implementations.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1349 of 1551

[0032] Figure 15 is a first end view of a connector receptacle of the in-line dongle adapter module of Figure 11 in accordance with some implementations.

[0033] Figure 16 is a second end view of a connector receptacle of the in-line dongle adapter module of Figure 11 in accordance with some implementations.

[0034] Figure 17 is a perspective view taken from the first end of the in-line dongle adapter module of Figure 11, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for illustrative purposes in accordance with some implementations.

[0035] Figure 18 is a perspective view taken from the second end of the in-line dongle adapter module of Figure 11, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for illustrative purposes in accordance with some implementations.

[0036] Figure 19 is a perspective view of the in-line dongle adapter module of Figure 11 within a vending machine in accordance with some implementations.

[0037] Figure 20 is a block diagram of an adapter module in accordance with some implementations.

[0038] Figure 21 is a block diagram of a mobile device in accordance with some implementations.

[0039] Figure 22 is a block diagram of a server in accordance with some implementations.

[0040] Figure 23 is a schematic flow diagram of a process for authenticating a user to perform a transaction in the payment processing system in accordance with some implementations.

[0041] Figure 24A is a block diagram of a packet of information broadcast by the payment module (sometimes also herein called the "adapter module") in accordance with some implementations.

[0042] Figure 24B is a block diagram of an authorization request in accordance with some implementations.

Draft Only

[0043] Figure 24C is a block diagram of an authorization grant token in accordance with some implementations.

[0044] Figure 24D is a block diagram of transaction information generated by the payment module in accordance with some implementations.

[0045] Figure 25A illustrates a schematic flow diagram of a process for providing a representation of a machine event at a mobile device in accordance with some implementations

[0046] Figure 25B is a schematic flow diagram of a process for processing acknowledgment information in the payment processing system in accordance with some implementations.

[0047] Figures 26A-26D illustrate example user interfaces for providing a representation of a machine event at a mobile device in accordance with some implementations.

[0048] Figures 27A-27B illustrate a flowchart diagram of a method of presenting representations of payment accepting unit events in accordance with some implementations.

[0049] Figure 28A illustrates a block diagram of an offline-payment operated machine in accordance with some implementations.

[0050] Figure 28B illustrates signals sampled by the payment module in accordance with some implementations.

[0051] Figures 29A-29B illustrate a flowchart diagram of a method 1600 of retrofitting an offline-payment operated machine to accept electronic payments in accordance with some implementations.

[0052] Figure 30 illustrates a flowchart diagram of a method of enabling a payment operated machine to accept electronic payments in accordance with some implementations.

[0053] Like reference numerals refer to corresponding parts throughout the several views of the drawings.

DETAILED DESCRIPTION

[0054] Disclosed herein is a payment processing system or, more specifically, a mobile-device-to-machine payment processing system for processing transactions over a non-persistent

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1351 of 1551

network connection. The mobile-device-to-machine payment processing system disclosed herein focuses on the unattended retail space (e.g., a payment accepting unit 120, sometimes also herein called a "machine 120"). More specifically, the mobile-device-to-machine payment processing system disclosed herein allows a user (having a mobile device 150 with a mobile application 140 thereon) to make a cashless purchase from a payment accepting unit 120 (having an adapter module 100 associated therewith).

[0055] The mobile-device-to-machine payment processing system described herein can be implemented with one or more of the following features: easy installation feature, a non-persistent network connection feature; a manual (swipe to pay) mode feature; a hands-free mode feature; and a multiple vending transactions (multi-vend) feature.

[0056] Easy Installation: Installation is very easy, requires no tools, requires no configuration, and takes as little as 30 seconds. This is accomplished by using an adapter module 100 (sometimes also herein called "payment module 100") such as an in-line dongle (a hardware device with software thereon) design for in-line insertion within a multi-drop bus (MDB) of a payment accepting unit 120 (e.g., a vending machine) (sometimes also herein called 'the machine 120"). Installation is as simple as "powering down" (turning off) the machine 120, identifying the "wire" that connects with a payment receiving mechanism (e.g., the coin mechanism), disconnecting the wire (so that there are two loose ends, such as a male connection end or adapter of an MDB and a female connection end or adapter of an MDB), plugging (inserting) the adapter module 100 in serial ("in-line") with the wire (e.g., connecting the MDB female adapter to a male adapter of the adapter module 100 and connecting the MDB male adapter to a female adapter of the adapter module 100), tucking the wire and the installed adapter module 100 back into position, and "powering up" (turning on) the machine 120. Most vending machines made since 1995 have this industry standard MDB technology that would allow this easy 30-second installation. On machines without MDB technology, the adapter module 100 can be configured or designed to work with other serial protocols or activate a switch. In essence the adapter module 100 simulates establishing payment on payment accepting unit 120 in much the same manner as other alternative forms of payment (e.g., cash).

[0057] Non-persistent Network Connection: Although payment accepting units (or "machines") that accept only cash (e.g., paper currency and coins) may not require a connection

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1352 of 1551

(persistent or non-persistent) to a network, traditional payment accepting units that accept cashless payments (e.g., credit cards, debit cards, and alternative mobile device payment methods using, for example, smart phones) require a persistent connection to a network (wired or wireless) to facilitate the cashless payments. In other words, without a persistent (ongoing or accessible on demand) network connection, traditional payment accepting units cannot accept cashless payments. Most traditional payment accepting units that accept cashless payments include the technology to accomplish this persistent network connection that allows them to connect to a remote server. If the network connection to a traditional machine is temporarily interrupted, cashless payments will be temporarily unavailable. If the machine is located in a location where no network connection is available, cashless payments is not possible. In addition to using a mobile device 150 as an intermediary between the payment accepting units 120 and the server 130, the mobile-device-to-machine payment processing system described herein minimizes (i.e., the manual mode) or eliminates (i.e., the hands-free mode) user interaction with the mobile device 150. Further, in some implementations, the mobile-device-to-machine payment processing system described herein facilitates the acceptance of cashless payments without requiring any network connection near the payment accepting unit 120. In some implementations, when the mobile-device-to-machine payment processing system described herein is located in a remote location where network connection is unavailable, the mobile-device-to-machine payment processing system, therefore, can still accept cashless payments.

[0058] Manual (Swipe-to-Pay) Mode: Using a "swipe-to-pay" feature (or just "swipe") refers to a user's action implemented on his/her mobile device 150 where he/she quickly brushes his/her finger (or other pre-determined interaction) on the mobile device's touch screen 152 (Figures 10A-10D) or other input devices associated with the mobile device 150. From the user's perspective, when the user is within range, a pre-installed mobile application 140 automatically connects to the payment accepting unit 120 (e.g., a vending machine). The mobile application 140 might display (on the touch screen 152) a prepaid balance that the user "swipes" to transfer payment to the payment accepting unit 120. The user could observe the transferred funds on the touch screen 152 of the mobile device 150 and/or on the display 122, 124 (Figure 19) of the payment accepting unit 120. The transaction is completed just as if cash was inserted in the machine 120 with the user inputting his selection on the payment accepting unit 120 and the payment accepting unit 120 dispensing the product or service. After the selection is made, the

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1353 of 1551

change is returned to the mobile device 150 and this may be shown on the touch screen 152 of the mobile device 150.

[0059] Hands-Free Mode: A "hands-free pay" feature (or just "hands-free") would most likely be used with "favorite" payment accepting units 120 (e.g., a frequently used vending machine at a user's work or school). From the user's perspective, he/she would approach the favorite payment accepting unit 120 and notice that the display 122, 124 (Figure 19) of the payment accepting unit 120 shows funds available, he/she would select the product or service using the payment accepting unit's input mechanisms (e.g., buttons 126 or a touch screen display 124 shown in Figure 19), and he/she would retrieve dispensed services or products. It would be that simple. More specifically, when the user is within range, a pre-installed mobile application 140 automatically connects to the payment accepting unit 120 (e.g., a vending machine). The user may leave the mobile device 150 in a pocket, purse, briefcase, backpack, or other carrier. As the user approaches the payment accepting unit 120 and is in approximately "arm's-length" distance (e.g., 3 to 5 feet) of the payment accepting unit 120, the user could observe the transferred funds on the display 122, 124 (Figure 19) of the payment accepting unit 120. The transaction is completed just as if cash was inserted into the payment accepting unit 120 with the user inputting his/her selection on the payment accepting unit 120 and the payment accepting unit 120 dispensing the product or service. After the selection is made, the change is returned to the mobile device 150. Figure 3 details when the hands-free mode would be available.

[0060] Multiple Vending Transactions (Multi-Vend): Both the manual and hands-free modes could be used multiple times in sequence (implemented, for example, as a loop) so that a user may make multiple purchases. After making his/her first selection and receiving his product (or service), the user would observe that additional funds were available on the display 122, 124 (Figure 19) on the payment accepting unit 120. He/she could make another selection (or multiple selections) and receive additional product(s) (or service(s)). More specifically, the display 122, 124 (Figure 19) may reset as if the transaction is complete, but then, because the user is still standing in range, the mobile application 140 would send another credit to the payment accepting unit 120, allowing for a second purchase. When the user walks away, the system clears (e.g., returns unused funds to the application 140 on the mobile device 150).

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1354 of 1551

[0061] The features described above, alone or in combination with other features described herein will revolutionize the hundred billion dollar automated retail industry. The hardware is very low cost and there are no reoccurring fees because no cellular connection is required on the machine 120. Using the mobile-device-to-machine payment processing system described herein, operators of machines 120 can increase frequency of visits by purchasers and items sold with each visit.

[0062] The mobile-device-to-machine payment processing system described herein may be implemented as an apparatus, system, and/or method for enabling payments to a machine 120 via a mobile device 150. The mobile-device-to-machine payment processing system may be better understood with reference to the drawings, but the shown mobile-device-to-machine payment processing system is not intended to be of a limiting nature.

DEFINITIONS

[0063] Before describing the mobile-device-to-machine payment processing system and the figures, some of the terminology should be clarified. Please note that the terms and phrases may have additional definitions and/or examples throughout the specification. Where otherwise not specifically defined, words, phrases, and acronyms are given their ordinary meaning in the art. The following paragraphs provide some of the definitions for terms and phrases used herein.

[0064] Adapter Module 100: As shown in Figures 1 and 2, the adapter module 100 (sometimes also herein called the "payment module 100") is a physical device that is installed in a machine 120 (a payment accepting unit 120). The shown adapter module 100 is an in-line dongle (a hardware device with software thereon) device that may be inserted in-line within a multi-drop bus (MDB) of a machine 120. The adapter module 100 bridges the communication between the machine 120 and a mobile device 150. Although described as a unique component, it should be noted that the adapter module 100 could be implemented as a plurality of devices or integrated into other devices (e.g., components of a machine 120). In its unique component form, the adapter module 100 can be easily inserted into a machine 120 so that the machine 120 is able to perform new features with the assistance of the adapter module 100. Figure 20 shows components associated with the adapter module 100. As shown in Figure 20, the communications unit 770 of the adapter module 100 includes short-range communication capability 776 (e.g., Bluetooth mechanisms).The shown example may be divided into multiple

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1355 of 1551

distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g., a computer or a payment accepting unit) as long as the components are associated with each other.

[0065] Mobile Device 150 and Application 140 (also referred to as a "mobile application," "mobile app," or "app"): In general, a mobile device 150 may be a user's personal mobile device 150. The mobile device 150 (with a mobile application 140 thereon) acts as a communication bridge between the adapter module 100 (associated with a payment accepting unit 120) and the server 130. The mobile device 150 and the application 140, however, are not "trusted" in that the communications (transmissions) it passes are encrypted. Encrypted (secured) communications are undecipherable (unencryptable, unreadable, and/or unusable) by the mobile device 150. This keeps the communications passed between the adapter module 100 and the server 130 secured and safe from hacking. Mobile devices include, but are not limited to smart phones, tablet or laptop computers, or personal digital assistants (PDAs), smart cards, or other technology (e.g., a hardware-software combination) known or yet to be discovered that has structure and/or capabilities similar to the mobile devices described herein. The mobile device 150 preferably has an application (e.g., the application 140) running on it. The term "app" is used broadly to include any software program(s) capable of implementing the features described herein. Figures 10A-10D show user interfaces for the application 140 displayed by the mobile device 150. It should be noted that the phrase "mobile device" can be assumed to include the relevant app unless specifically stated otherwise. Similarly, it should be noted that an "app" can be assumed to be running on an associated mobile device unless specifically stated otherwise. Figure 21 shows components associated with the mobile device 150. The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g., the cell phone itself) as long as the components are associated with each other.

[0066] Payment accepting unit 120 (or Machine 120): A payment accepting unit 120 (or the machine 120) is equipment that requires payment for the dispensing of an product and/or service. Payment accepting units 120 may be vending machines, parking meters, toll booths, laundromat washers and dryers, arcade games, kiosks, photo booths, toll booths, transit ticket dispensing machines, and other known or yet to be discovered payment accepting units 120. Some payment accepting units 120 can accept cashless payments (payments other than cash

Draft Only

(paper currency and coins)) by accepting payment from, for example, credit cards, debit cards, and mobile devices.

[0067] Network Connections: For purposes of this discussion, a persistent network connection is a wired or wireless communications connection that is ongoing (e.g., a dedicated connection, a dedicated online connection, and/or a hardwired connection) or accessible on demand (e.g., the ability for the machine to make a temporary connection to a server or the ability for the user to contact a server from his mobile device). Typically the persistent network connection has been conducted over "long-range communication technology" or "long-range communication protocol" (e.g., hardwired, telephone network technology, cellular technology (e.g., GSM, CDMA, or the like), Wi-Fi technology, wide area network (WAN), local area network (LAN), or any wired or wireless communication technology over the Internet that is known or yet to be discovered). Traditionally, machines that accept payment other than cash require a persistent (ongoing or accessible on demand) connection to a network to facilitate payment. This is true for machines that accept, for example, credit cards and debit cards. The payment accepting units 120 described herein do not require a traditional persistent network connection. The user's mobile device 150 acts as a communication bridge between the adapter module 100 and the server 130. Communications between user mobile devices 150 and the servers (e.g., a system management server 130 and/or a funding source server 160) take place using long-range communication technology. Communications between user mobile devices 150 and the adapter module 100 of the payment accepting unit 120 take place using "short-range communication technology" or "short-range communication protocol" (e.g., Bluetooth (such as Bluetooth 4.0, Bluetooth Smart, Bluetooth Low Energy (BLE)), near-field communication (NFC), Ultra Wideband (UWB), radio frequency identification (RFID), infrared wireless, induction wireless, or any wired or wireless technology that could be used to communicate a small distance (approximately a hundred feet or closer) that is known or yet to be discovered). Therefore, neither the adapter module 100 nor the payment accepting unit 120 requires a traditional persistent long-range wireless network connection. The communications technology shown in the figures may be replaced with alternative like communications technology and, therefore, specific shown communications technologies are not meant to be limiting. For example, Wi-Fi technology could be replaced with another long-range communication technology.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1357 of 1551

[0068] Server: A server is the host processing server that may be operated by the company running the payment processing system. For each user, the server 130 preferably maintains at least one "virtual wallet" having at least one "balance" (which can be $0) of designated funds for which the server 130 keeps an accounting. The balance may represent, for example, "cash" or it may be a "promotional value" that represents funds that may be spent under certain circumstances. If these funds begin to be depleted, the user may be notified (e.g., via the application 140 on the mobile device 150) that additional funds need to be designated and/or transferred. Alternatively, funds from other sources (e.g., the funding source server 160) may be automatically transferred to restore a predetermined balance. The balance may also be increased based on a promotion (e.g., points earned or coupons). As shown in Figure 22, the server includes appropriate processors 950, memory 960 (which would keep an accounting of the user's balance in a manner similar to a gift card), and communication systems 970. As shown in Figure 22, the communications unit 970 of the server 130 includes long-range communication capability 972 (e.g., cellular technology and/or Wi-Fi mechanisms). The server 130 also includes a security unit 955 for encrypting and decrypting messages. The server 130 receives an authorization request (sometimes also herein called an "AuthRequest") from the adapter module 100 (via a mobile device 150) and, if funds are available, returns an authorization grant (sometimes also herein called an "AuthGrant" or an "authorization grant token") for funds. Figure 22 shows components associated with the server 130. The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g., a computer or a main frame) as long as the components are associated with each other.

[0069] Advertise Presence: Each adapter module 100 advertises its presence by broadcasting signals (advertising broadcast signals) to mobile devices in the zones 102, 104, 106. Each adapter module 100 can listen to other adapter modules' advertisements.

[0070] Received Signal Strength Indicator (RSSI): The adapter module 100 may have a self-calibrating signal strength to determine zone thresholds (e.g., a payment zone threshold and an authentication zone threshold). At the time the user selects an item (product or service) from the payment accepting unit 120, the Received Signal Strength Indicator (RSSI) is logged. At this moment, it is presumed the user is within "arm's-length" (which may be a predetermined length approximating the distance of a user standing in front of a machine for the purpose of making a

Draft Only

purchase) from the payment accepting unit 120. A mathematical computation (i.e., In-Range Heuristics) is conducted to derive the optimal RSSI threshold at which point payment should be triggered by an application 140 on a mobile device 150. The threshold may be payment accepting unit specific and can vary over a period of time. This optimal zone threshold is preferably reported to the mobile device 150 during an initial handshake.

[0071] In-Range Heuristics: A mathematical computation that determines the RSSI threshold to determine when a user is in the authorization zone 104 and/or the payment zone 102. This computation can take into consideration numerous historical data points as well as transaction specific information such as which the mobile device 150 is being used, payment accepting unit type, among other factors. Preferably the RSSI is logged while the user is making his selection (this is the one time in the entire process that the user definitely will be "in range" (e.g., they will be arm's length from the machine 120 because they are physically interacting with the machine 120). The type of user mobile device 150, accelerometer data (e.g., is the user moving or stationary), and/or other information may also be logged while the user is making his selection. The adapter module 100 can give a reference RSSI for the payment zone 102 for the machine 120, and the application 140 can make a +/- adjustment based on the specific mobile device 150 on which it is installed. Over a period of time, the payment processing system continues to improve itself based on additional data points.

[0072] Authorization Request ("AuthRequest:): When a user enters the authorization zone 104, the mobile device 150 notifies the adapter module 100 and the adapter module 100 sends a secured authorization request (e.g., the encrypted authorization request) as a "message" (also referred to as a communication or transmissions) to the server 130 via the mobile device 150. Encryption may be performed by a security unit 755 (Figure 20) with security technology (e.g., encryption and decryption means) that may be associated with the processing unit 750 and/or the memory 760. Significantly, the AuthRequest is a request for authorization of funds, not a request for authorization of a transaction. The purpose of the funds is irrelevant to the server 130.

[0073] Authorization Grant Token ("AuthGrant"): This is a "message" (also referred to as a communication or transmissions) encrypted by the security unit 955 (Figure 22) with security technology (e.g., encryption and decryption means) of the server 130 with the unique

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1359 of 1551

private key corresponding to the adapter module 100. The secured authorization grant (e.g., the encrypted authorization grant) is passed from the server 130 to the adapter module 100 via the mobile device 150 in the form of a message. The mobile device 150, however, is not able to decrypt and/or read the message. The authorization grant is in response to the authorization request. The amount of the funds granted by the AuthGrant may be determined by factors including, but not limited to, the amount of funds available (or, if funds are not available, a mini-loan could be granted), a pre-authorized amount (e.g., set by the server, set by the user during set-up, set by the funding source, or a standard amount), limited by time (e.g., only a certain amount per hour, or a predetermined amount at specific times of the day), limited to the maximum amount of an item on the machine (or enough for two or three items in the machine), or one or more of these and other factors. Significantly, the AuthGrant makes the funds available, but does not authorize a transaction. The AuthGrant may have an associated expiration period in that it may expire if it is not used in a pre-determined time period. The length of time before the AuthGrant expires may be determined by factors including, but not limited to, the trustworthiness of the user (e.g., the user has a long history with the payment processing system or some known provider (e.g., credit card provider, bank, or credit union), the user has a good credit rating, or the user has a large wallet balance), a pre-authorized time period (e.g., set by the server, set by the user during set-up, set by the funding source, or a standard time period), limited by time (e.g., predetermined time periods at specific times of the day such as longer times during breakfast, lunch, and dinner), limited by the machine or the products or services sold in the machine, limited by the number of other users near the machine (e.g., if it is a crowded machine, the AuthGrant may expire faster), or one or more of these and other factors. The AuthGrant remains valid until it expires or some other event occurs to end its validity (e.g., the user cancels it). This means that under normal circumstances the mobile device 150 will hold the AuthGrant authorizing use of funds for a pre-determined time period that will allow the user sufficient time to make a purchase. The authorized amount may be considered to be the "wallet balance" that is held in a virtual "wallet."

[0074] Synchronization: Time may be synchronized to the adapter module 100 from the server 130. The server 130 sends time information with encrypted messages and the adapter module 100 uses the time encoded in the messages for synchronization.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1360 of 1551

[0075] The mobile-device-to-machine payment processing system and components thereof may have associated hardware, software, and/or firmware (a variation, subset, or hybrid of hardware and/or software). The term "hardware" includes at least one "processing unit," "processor," "computer," "programmable apparatus," and/or other known or yet to be discovered technology capable of executing instructions or steps (shown as the processing unit 750 in Figure 20, the processing unit 850 in Figure 21, and the processing unit 950 in Figure 22). The term "software" includes at least one "program," "subprogram," "series of instructions," or other known or yet to be discovered hardware instructions or hardware-readable program code. Software may be loaded onto hardware (or firmware) to produce a "machine," such that the software executes on the hardware to create structures for implementing the functions described herein. Further, the software may be loaded onto the hardware (or firmware) so as to direct the mobile-device-to-machine payment processing system (and components thereof) to function in a particular manner described herein or to perform a series of operational steps as described herein. "Hardware" such as the adapter module 100, the mobile device 150, and the payment accepting unit 120 may have software (e.g., programs and apps) loaded thereon. The phrase "loaded onto the hardware" also includes being loaded into memory (shown as the memory 760 in Figure 20, the memory 860 in Figure 21, and the memory 960 in Figure 22) associated with or accessible by the hardware. The term "memory" is defined to include any type of hardware (or other technology) -readable media (also referred to as computer-readable storage medium) including, but not limited to, attached storage media (e.g., hard disk drives, network disk drives, servers), internal storage media (e.g., RAM, ROM, EPROM, FLASH-EPROM, or any other memory chip or cartridge), removable storage media (e.g., CDs, DVDs, flash drives, memory cards, floppy disks, flexible disks), firmware, and/or other known or yet to be discovered storage media. Depending on its purpose, the memory may be transitory and/or non-transitory. Appropriate "messages," "communications," "signals," and/or "transmissions" (that includes various types of information and/or instructions including, but not limited to, data, commands, bits, symbols, voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, and/or any combination thereof) over appropriate "communication paths," "transmission paths," and other means for signal transmission including any type of connection between two elements on the payment processing system (e.g., the adapter module 100, the mobile device 150, the

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1361 of 1551

payment accepting unit 120, hardware systems and subsystems, and memory) would be used as appropriate to facilitate controls and communications.

[0076] It should be noted that the terms "programs" and "subprograms" are defined as a series of instructions that may be implemented as software (i.e. computer program instructions or computer-readable program code) that may be loaded onto a computer to produce a "machine," such that the instructions that execute on the computer create structures for implementing the functions described herein or shown in the figures. Further, these programs and subprograms may be loaded onto a computer so that they can direct the computer to function in a particular manner, such that the instructions produce an article of manufacture including instruction structures that implement the function specified in the flow chart block or blocks. The programs and subprograms may also be loaded onto a computer to cause a series of operational steps to be performed on or by the computer to produce a computer implemented process such that the instructions that execute on the computer provide steps for implementing the functions specified in the flow chart block or blocks. The phrase "loaded onto a computer" also includes being loaded into the memory of the computer or a memory associated with or accessible by the computer. Separate, albeit interacting, programs and subprograms may be associated with the adapter modules 100, the server 130, and the mobile device 150 (including the mobile application 140) and these programs and subprograms may be divided into smaller subprograms to perform specific functions.

[0077] The terms "messages," "communications," "signals," and/or "transmissions" include various types of information and/or instructions including, but not limited to, data, commands, bits, symbols, voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, and/or any combination thereof. Appropriate technology may be used to implement the "communications," "signals," and/or "transmissions" including, for example, transmitters, receivers, and transceivers. "Communications," "signals," and/or "transmissions" described herein would use appropriate technology for their intended purpose. For example, hard-wired communications (e.g., wired serial communications) would use technology appropriate for hard-wired communications, short-range communications (e.g., Bluetooth) would use technology appropriate for close communications, and long-range communications (e.g., GSM, CDMA, Wi-Fi, or the like) would use technology appropriate for remote communications over a distance. Appropriate security (e.g., SSL or TLS) for each type of communication is

Draft Only

included herein. The security units 755 and 955 include technology for securing messages. The security technology may be, for example, encryption/decryption technology (e.g., software or hardware). Although encryption/decryption is discussed primarily as being performed using a unique private key, alternative strategies include, but are not limited to encryption/decryption performed using public/private keys (i.e., asymmetric cryptography), or other encryption/decryption strategies known or yet to be discovered. Appropriate input mechanisms and/or output mechanisms, even if not specifically described, are considered to be part of the technology described herein. The communications unit 770 (shown in Figure 20) of the adapter module 100 is shown as including appropriate input and output mechanisms 772, 774 that may be implemented in association (e.g., directly or indirectly in functional communication) with male and female adapters 720, 730 of the adapter module 100. The communications unit 870 (shown in Figure 21) of the mobile device 150 includes mechanisms for both long-range communications (shown as the long-range communication capability 872 such as cellular and/or Wi-Fi mechanisms) for communicating with the server 130 and short-range communications (shown as the short-range communication capability 876 such as Bluetooth mechanisms) for communicating with the adapter module 100.

[0078] When used in relation to "communications," "signals," and/or "transmissions," the terms "provide" and "providing" (and variations thereof) are meant to include standard means of provision including "transmit" and "transmitting," but can also be used for non-traditional provisions as long as the "communications," "signals," and/or "transmissions" are "received" (that can also mean obtained). The terms "transmit" and "transmitting" (and variations thereof) are meant to include standard means of transmission, but can also be used for non-traditional transmissions as long as the "communications," "signals," and/or "transmissions" are "sent." The terms "receive" and "receiving" (and variations thereof) are meant to include standard means of reception, but can also be used for non-traditional methods of obtaining as long as the "communications," "signals," and/or "transmissions" are "obtained."

[0079] The term "associated" is defined to mean integral or original, retrofitted, attached, connected (including functionally connected), positioned near, and/or accessible by. For example, if the user interface (e.g., a traditional display 122 (Figure 19), a touch screen display 124 (Figure 19), a key pad 126 (Figure 19), buttons 126 (Figure 19, shown as part of the key pad 126), a keyboard (not shown), and/or other input or output mechanism) is associated with a

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1363 of 1551

payment accepting unit 120, the user interface may be original to the payment accepting unit 120, retrofitted into the payment accepting unit 120, attached to the payment accepting unit 120, and/or a nearby the payment accepting unit 120. Similarly, adapter modules 100 may be associated with payment accepting units 120 in that the adapter modules 100 may be original to the payment accepting unit 120, retrofitted into the payment accepting unit 120, attached to the payment accepting unit 120, and/or a nearby the payment accepting unit 120.

SYSTEM OVERVIEW

[0080] Figures 5, 6, and 7 together show major components of the mobile-device-to-machine payment system and the interactions there-between.

[0081] As shown, the adapter module 100 functionally connected bi-directionally to the payment accepting unit 120 via a wired serial connection such that no security is necessary. The adapter module 100 is also functionally connected bi-directionally to the mobile device 150 (and its installed mobile application 140) via short-range communication technology (e.g., a Bluetooth connection). Because the mobile device 150 is not a "trusted" link (e.g., it could be hacked by a user), only secured communications (transmissions) are passed between the adapter module 100 and the mobile device 150. This keeps communications secured and safe from hacking. The mobile device 150 (and its installed mobile application 140) is also functionally connected bi-directionally to a system management server 130 and/or a funding source server 160 via long-range communication technology (e.g., Wi-Fi or Cellular connection) that preferably has appropriate security (e.g., SSL security). Security between the mobile device 150 and the system management server 130 has the advantage of protecting communications from the mobile device 150 to the system management server 130 that may include sensitive data and may not be encrypted. The system management server 130 and the funding source server 160 may be connected via a wired Internet connection with SSL security. The system management server 130 may be connected via a wired Internet connection with SSL security to an operators' server 170. Although not necessary to implement a purchase transaction, for other purposes (e.g., inventory), the operators' server 170 may be connected to the payment accepting unit 120 using a handheld computer sync or a cellular connection.

[0082] Also, a unique private key may be used to securely transmit encrypted messages between the adapter module 100 and the system management server 130 (although the encrypted

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1364 of 1551

transmissions would most likely be routed through the mobile device 150). The server 130 stores a private key for each adapter module 100, and this key is only known to the adapter module 100 and the server 130. No intermediary is privy to this key (especially not the mobile device 150). When the adapter module 100 and the server 130 communicate messages (e.g., AuthRequest and AuthGrant), the security unit 755 of the adapter module 100 encrypts the message with its private key and passes the message to the mobile device 150. The mobile device 150 (which preferably cannot decrypt the message) passes the encrypted message to the server 130. The server 130 is able to decrypt the message using the security unit 955 of the adapter module 100 and the unique private key. The security unit 955 of the server 130 uses this same unique private key to encrypt messages to the adapter module 100 and sends the message to the mobile device 150 to relay to the adapter module 100 that is able to decrypt the message using the security unit 755 of the adapter module 100 and the unique private key.

[0083] Figure 7 shows specific communications and messaging with a vending sequence (the numbers to the left of the communications and messaging) between the adapter module 100, the mobile device 150, and the system management server 130. These communications are discussed in more detail in the discussion pertaining to the schematic flow diagrams (Figures 8A-8G) and the flow charts (Figures 9A-9E).

[0084] It should be noted that Figures 5, 6, and 7 are examples, and are meant to help in the understanding of the mobile-device-to-machine payment system. For example, the shown long-range communications technology may be replaced with alternative long-range communications technology known or yet to be discovered, the shown short-range communication technology may be replaced with alternative short-range communication technology known or yet to be discovered, and the shown security may be replaced with alternative security known or yet to be discovered. The shown connections are meant to be examples, and there may be intermediaries that are not shown. The shown components have been simplified in that, for example, only one mobile device 150 (or machine 120, adapter module 100, or server 130) is shown where many may be included. Finally, the order of the steps may be changed and some steps may be eliminated.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1365 of 1551

ADAPTER MODULE

[0085] Figures 11-18 show views of adapter module 100a (referred to generally as adapter module 100). Adapter module 100 is a relatively low cost hardware component that is pre-configured to work with the industry standard multi-drop bus (MDB). On machines without MDB technology, the adapter module 100 can be configured or designed to work with other serial protocols or activate a switch. In essence the adapter module 100 simulates establishing payment on payment accepting unit 120 in much the same manner as other alternative forms of payment (e.g., cash).

[0086] The shown adapter modules 100 are preferably designed to be used as an in-line dongle for in-line insertion within, for example, a MDB of a machine 120. The wire used in MDB technology uses male and female connection ends or adapters to allow the attachment of peripherals. In the case of a vending machine, the wire with the connection ends or adapters would be present to allow the attachment of a payment receiving mechanism (e.g., a coin mechanism). The MDB male and female adapters 700, 710 may be separated (as shown in Figures 17-18). The adapter module 100a in Figures 11 and 17-18 has a male adapter 720 and a female adapter 730. The adapter module 100a may be plugged (inserted) in serial ("in-line") with the wire. For example, the MDB female adapter 710 may be connected to the male adapter 720 of the adapter module 100 and the MDB male adapter 700 may be connected to the female adapter 730 of the adapter module 100. The resulting in-line configuration is shown in Figure 19. It should be noted that the adapter modules 100 are designed to allow pass-through communications so that if the mobile-device-to-machine payment processing system is not enabled (e.g., for a particular purchase or simply turned off) the MDB functions as though the adapter module 100 is not there and the machine 120 can function normally.

Draft Only

HANDS-FREE MODE

[0087] Summarily, if it is available, a hands-free mode, from the user's perspective, would allow the user to approach a favorite payment accepting unit 120 and notice that the display (e.g., the displays 122 or 124 shown in Figure 19) associated with the payment accepting unit 120 shows funds available (e.g., the wallet balance), he would select the product or service using input mechanisms (e.g., buttons 126 or a touch screen display 124 shown in Figure 19)

CSC ServiceWorks - Ex. 1002
Page 1366 of 1551

associated with the payment accepting unit 120, and he would retrieve his dispensed services or products.

[0088] During an initial handshake with the mobile device 150 (when the user is within range), the adapter module 100 reports to the mobile device 150 whether or not hands-free mode is available. If it is available, the installed mobile application 140 automatically connects to the payment accepting unit 120 without the user having to interact with the mobile device 150. The user observes that funds are available on the display 122, 124 of the payment accepting unit 120 and completes the purchase transaction as if cash was inserted in the machine 120 by inputting his selection on the payment accepting unit 120. The payment accepting unit 120 dispenses the product or service. After the selection is made, the change is returned to the mobile device 150.

[0089] Whether hands-free payment is available is determined by factors including, but not limited to whether if other mobile devices 150 are in range, if other adapter modules 100 are in range, if there are any alerts, if the payment trigger threshold is having wide variances and so deemed unstable, or if the payment accepting unit operator (e.g., a vending machine operator) has opted to disable hands-free mode for the payment accepting unit 120. In the latter instance, operators can disable via a maintenance mobile device 150, as well as through the operators' server 170 and/or the system management server 130.

[0090] Figure 3 is a table that shows considerations, conditions, or factors that may be used to determine whether the hands-free pay feature is available. Starting at the "Favorite?" column, this indicates whether the payment accepting unit 120 is a favorite machine. Preferably the hands-free pay feature is only available for use with "favorite" payment accepting units 120 (e.g., a vending machine at work or school). The "Alert" column has to do with whether there is some reason (e.g., there are too many users in range) that the hands-free pay feature should not work and, if there is such a reason, the user will be notified (alerted) and may be able to use the manual mode to resolve the alert and/or complete the transaction. Figure 3 shows situations in which a user is or is not able to make hands-free purchases from a machine 120 using a mobile application 140 on his mobile device 150. It should be noted that the shown interface is an example. For example, some of the features could be automated or pre-selected. (It should be noted that the left hand column, the "Tab" column, relates to whether the selected tab on the mobile application 140 is "all" or "favorite." Figures 10A-10D all show these tabs. Unlike the

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1367 of 1551

other columns in Figure 3, this column has more to do with the functionality and view of the application 140 than specifically with the hands-free feature. The tabs would allow a user to select whether he wanted to be alerted when he was in range of all payment accepting units 120 or just "favorite" payment accepting units 120 and the application 140 would show the appropriate view.)

[0091] Balance Display: An optional feature of the mobile-device-to-machine payment system that is particularly helpful in the hands-free mode (although it may be available in the manual mode and/or in a multiple-vend scenarios) is when the user's mobile device 150 sends "credit" to the payment accepting unit 120 (either via hands-free payment or through a manual swipe), the wallet balance is sent to the payment accepting unit 120 that is then displayed to the user on a display 122, 124 of the machine 120. This is particularly beneficial during hands-free mode when the user does not retrieve the mobile device 150 and, therefore, may not know the balance. Also, in a multiple-vend scenario the user would not have to calculate a remaining balance.

[0092] An example of a hands-free, multiple-vend scenario where a balance is displayed by the payment accepting unit 120, follows: The user has $5.00 in his/her virtual wallet as that is the amount that has been authorized (the AuthGrant being stored on the mobile device 150). The user walks up to the payment accepting unit 120 and $5.00 is displayed on the display 122, 124 of the payment accepting unit 120 since hands-free mode was enabled and credit was sent (e.g., via the short-range communication capability) to the payment accepting unit 120. The user makes a selection of $1.50 by interacting (e.g., pressing buttons) with the machine 120. The item (product or service) is dispensed and the "change" is "returned" (e.g., via the short-range communication capability) to the virtual wallet. But since the user is still standing in the payment zone 102, the remaining wallet balance of $3.50 is sent to the payment accepting unit 120 and displayed so that the user can now see that he/she has a $3.50 balance. (It should be noted that the authorized funds may remain on the machine 120 and not be transferred back to the mobile device 150 between transactions.) The user decides to purchase a $1.50 item, and the transaction is completed as usual (e.g., by interacting with the machine 120). Now the user is still standing in the payment zone 102 and he/she sees the wallet balance of $2.00 on the display 122, 124 of the payment accepting unit 120. The user decides that he/she does not wish to purchase anything else and simply walks away. As he/she walks out of the payment zone 102, the credit is cleared from

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1368 of 1551

the machine 120, but he/she is left with the knowledge that his wallet balance is $2.00 even though he/she never touched the mobile device 150. Communications between the payment accepting unit 120 and the adapter module 100 (via the mobile device 150) handle the accounting incidental to the transaction. The remaining balance ($2.00) is technically stored on the server 130, and may be reflected on the application 140 on the mobile device 150.

MULTIPLE DISTINCT ZONES

[0093] As shown in Figures 1-2, the functions performed by the adapter module 100 can be divided into distinct zones: a first "communication zone" (e.g., "Bluetooth range" 106), a second "authorization zone" 104, and a third "payment zone" 102. The payment zone 102 is smaller than or equal to (overlapping completely) the authorization zone 104. Put another way, the payment zone 102 is within or coextensive with the authorization zone 104. The payment zone 102 is a subset of the authorization zone 104 with a ratio of the payment zone 102 to the authorization zone 104 ranging from 0.01:1 to 1:1. It is not necessarily a fixed ratio and can vary between different payment accepting units 120, different mobile devices 150, different users, and over time. While the zones 102, 104, 106 are depicted as having a uniform shape, the zones may not necessarily be uniform (or constant over time) in that the shape can vary. For example, the shape of the Bluetooth range 106 may vary depending on environmental conditions such as obstacles in the room and payment accepting unit 120 door/wall materials.

[0094] Bluetooth Range 106 (sometimes also herein called the "communication zone"): The outermost range is the Bluetooth range 106 (shown in Figures 1-2). This is the area in which the adapter module 100 is able to broadcast its presence. In most situations, the Bluetooth range 106 is a passive range in that no actual data is exchanged between the mobile device 150 and the adapter module 100. While in the Bluetooth range 106, the mobile device 150 monitors the RSSI (Received Signal Strength Indicator).

[0095] Authorization Zone 104: The middle region is the authorization zone 104 (shown in Figures 1-2). This is a computed area based on the RSSI. As mentioned, the mobile device 150 monitors the RSSI while it is in the Bluetooth range 106. When the RSSI reaches a certain predetermined threshold based on In-Range Heuristics, the mobile device 150 can be considered to be in the authorization zone 104. In the authorization zone 104 the mobile device 150 establishes a connection to the adapter module 100 (e.g., a Bluetooth connection (Figure 5) with

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1369 of 1551

SSL protection (Figure 6)) and informs the adapter module 100 of its presence. After a successful handshake with the adapter module 100, the mobile device 150 registers the adapter module 100 and the adapter module 100 requests an authorization to the server 130 via the mobile devices' network connection (e.g., a Wi-Fi or cellular connection (Figure 5) with SSL protection (Figure 6)). It is important to note the mobile device 150 and the adapter module 100 have a non-exclusive relationship at this point. The adapter module 100 may collect registrations for all mobile devices 150 that are within the authorization zone 104.

[0096] An authorization occurs in preparation for when the user enters the payment zone 102 (shown in Figures 1-2). An authorization expires in a set period of time (for example, five minutes), so if the mobile device 150 is still in the authorization zone 104 at the time of expiration, the adapter module 100 submits for and receives another authorization. This will continue for a set number of times (for example, the limit may be three times to limit cases of numerous authorizations for a mobile device that may remain in the authorization zone 104 for an extended period of time without completing a transaction). Should authorization fail (for instance if the limit had been reached) prior to the user entering the payment zone 102, the adapter module 100 will request authorization when the mobile device 150 enters the payment zone 102 (which adds a few seconds to the experience).

[0097] Payment Zone 102: As a user enters the payment zone 102, the mobile device 150 establishes exclusive control of the adapter module 100. Once established, any other user in the payment zone 102 is put into a "waiting" status.

[0098] In the payment zone 102, the payment can be triggered automatically if the payment processing system has and is in hands-free mode. In such instances, the mobile device 150 is running the application 140 in background mode and will send credit to the payment accepting unit 120 without any explicit user interaction. The user completes the transaction on the payment accepting unit 120 in much the same manner as if cash had been inserted into the payment accepting unit 120 to establish credit. After the user completes the transaction (that may include one or more purchases), details of the transaction are preferably returned to the mobile device 150 and server 130 in separate messages. The message to the server 130 is preferably encrypted with the adapter module's 100 private key (Figure 6) to ensure data integrity. As shown in Figure 7, the "private key" coded message (Encrypted VendDetails) is preferably sent

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1370 of 1551

via the mobile device 150. The message to the mobile device 150 may be sent solely for the purpose of closing the transaction. The transaction history and balance are updated server-side via the encrypted message sent to the server 130.

[0099] The other mode of operation is manual mode. In manual mode, the user launches the mobile device 150 and is able to swipe to send payment to the payment accepting unit 120. The user can also swipe back to cancel the payment. Like in hands-free mode, the purchase transaction is completed on the payment accepting unit 120 in the same manner as if cash were inserted into the payment accepting unit 120. The mobile device 150 is only used to send payment. Selection is made directly on the payment accepting unit 120.

[00100] Self-Calibrating Zone Threshold: A key, but optional feature, of the payment processing system is a self-calibrating payment zone RSSI threshold. Because RSSI can vary machine to machine, environment to environment, and device to device, having a fixed threshold at which payment is triggered can be problematic. The approach suggested herein is the creation of a self-calibrating threshold. When the user is interacting with the payment accepting unit 120 (such as when he makes his selection on the payment accepting unit 120), the payment accepting unit 120 notifies the adapter module 100 and the adapter module 100 logs the conditions such as RSSI, type of user mobile device 150, accelerometer data, and other information. It is at this point that it can be ascertained safely that the user is within arm's-length from the payment accepting unit 120 (by necessity the user is arm's-length because he is making some physical interaction with the payment accepting unit 120). This is the only point in the entire transaction in which it can be certain that the user is within arm's-length from the payment accepting unit 120.

[00101] Figure 4 shows a simplified set of steps involved when users enter the payment zone 102. Specifically, Figure 4 shows that credit is established 200 (this may have been done in the authorization zone 104, but if not it would be handled in the payment zone 102), that the user makes a selection using the machine 202, that the machine notifies the adapter module of the selection 204, that the adapter module (optionally) logs the RSSI 206, and that the purchase process(es) continues 208. Using the historically logged RSSI data, the adapter module 100 calculates one of several "average" RSSI using various mathematical models. This "average" could be a traditional average, a moving average, a weighted average, a median, or other similar

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1371 of 1551

summary function. The adapter module 100 could pre-process the historical data before running the function, such as to eliminate top and bottom data points, suspect data points, etc.

[00102] Optionally, during the handshake between the mobile device 150 and the adapter module 100, the information transmitted to the adapter module 100 may include, for example, the model of the mobile device 150. Using the received information pertaining to the mobile device models, the adapter module 100 can create multiple payment thresholds, one for each mobile device model. This allows for variances that may be inherent in different types of Bluetooth radios. An alternative to this method is for the adapter module 100 to broadcast a baseline payment zone threshold, and the mobile device 150 can use an offset from this baseline based on its specific model type. The payment zone thresholds (or baseline offsets) can be unique to specific types of mobile devices (e.g., by manufacturer, operating system, or component parts), models of mobile devices, or individual mobile devices (unique to each user).

[00103] In a typical scenario in which the payment zone threshold has been calibrated, the adapter module 100 advertises its presence along with the threshold at which it considers any mobile device 150 to be in the authorization zone 104. This is a one-way communication from adapter module 100 to mobile device 150. Once the mobile device 150 enters the authorization zone 104, there is a handshake that is established between the adapter module 100 and the mobile device 150. During this handshake, the mobile device 150 can share its model information with the adapter module 100, and the adapter module 100 can return the payment zone 102 threshold for that specific model.

[00104] Optionally, in addition to calibrating the payment zone threshold, the adapter module 100 can apply the self-calibrating model to the authorization zone 104 to calibrate the authorization zone threshold. As with the payment zone thresholds, the authorization zone thresholds can be unique to specific types of mobile devices, models of mobile devices, or individual mobile devices. In this scenario, the adapter module 100 would broadcast multiple thresholds by device type and the mobile device 150 would determine which threshold to apply (or alternatively broadcast a baseline and the mobile device 150 uses an offset based on its device model). Even in this scenario, the authorization zone 104 is a one-way communication.

[00105] Optionally, along with the threshold that is calculated (in the payment and/or the authorization zone(s)), a safety margin can be added to minimize scenarios in which a user is

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1372 of 1551

within range, but the mobile-device-to-machine payment processing system does not recognize it because the threshold may not have been reached. For example, if the calculated RSSI for an iPhone™ 5 on machine 4567 is -68 db, the mobile-device-to-machine payment processing system may add a safety margin of -5 db, and establish the threshold at -73 db. So when a user's phone is communicating with the adapter module 100 at an RSSI of -73 db or better, the mobile-device-to-machine payment processing system will allow the mobile device 150 to credit the payment accepting unit 120. The safety margin can be set on the server 130 and downloaded to the adapter module 100, or set on the mobile device 150, or set on the adapter module 100 itself.

[00106] Optionally, in the payment zone threshold, the mobile device 150 can use other data to determine when to cancel the exclusive control of the payment accepting unit 120, to identify when the user is moving out of the payment zone 102. External data could include accelerometer data from the mobile device 150. Using that data, the mobile device 150 can determine whether the user is standing relatively still in front of the payment accepting unit 120, or if the user is in motion – effectively walking away from the payment accepting unit 120.

SIGNAL UNAVAILABILITY ADAPTATION

[00107] The mobile-device-to-machine payment processing system described herein uses a mobile device's 150 short-range communication technology (e.g., Bluetooth mechanisms) (shown as short-range communication capability 876 in Figure 21) and a mobile device's 150 long-range communications technology (e.g., cellular and/or Wi-Fi mechanisms) (shown as long-range communication capability 872 in Figure 21). The short-range communication capability 876 communicates with the adapter module's 100 short-range communication technology (e.g., Bluetooth mechanisms) (shown as short-range communication capability 776 in Figure 20). The long-range communication capability 872 communicates with the server's 130 long-range communications technology (e.g., cellular and/or Wi-Fi mechanisms) (shown as long-range communication capability 972 in Figure 22). The mobile device 150 (with a mobile application 140 thereon) acts as a communication bridge between the adapter module 100 (associated with a payment accepting unit 120) and the server 130. This process is described herein and works properly if there is cellular or Wi-Fi coverage within the payment zone 102.

[00108] One option if there is no cellular or Wi-Fi coverage within the payment zone 102 is to determine whether there is cellular or Wi-Fi coverage within the authorization zone 104 or

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1373 of 1551

the Bluetooth range 106. If there is, then the sizes of the zones 102, 104, 106 could be adapted and the timing could be adapted. For example, if the mobile devices 150 detected problems with the cellular or Wi-Fi coverage within the payment zone 102, the user could carry his mobile device 150 into the other zones (or the mobile device 150 could use short-range communication technology to communicate with other mobile devices 150 within the authorization zone 104 or the Bluetooth range 106) to determine whether the zones have cellular or Wi-Fi coverage. If they do have coverage, communication between the mobile device 150 and the server 130 can be advanced (conducted earlier when the mobile device 150 is further from the machine 120) or delayed (conducted later when the mobile device 150 is further from the machine 120). This can be thought of as changing the size or shapes of the zones 102, 104, 106. The timing would also have to be adjusted so that the authorization of funds (AuthGrant) does not expire before the user has a chance to make a purchase. It also means that balance updates to the server 130 may happen after the user has moved away from the machine 120 and has cellular or Wi-Fi coverage again.

[00109] Another option if there is no cellular or Wi-Fi coverage within any of the zones 102, 104, 106 is for the user to obtain authorization while outside of the zones in a place with cellular or Wi-Fi coverage. This may occur, for example, if a user knows that he will be going to a place with a payment accepting unit 120 equipped with an adapter module 100 (perhaps to a favorite payment accepting unit 120) that does not have (or rarely has) cellular or Wi-Fi coverage. A user may also use the mobile application 140 to query payment accepting units 120 in a given range (e.g., within 50 miles) or at a given location (e.g., at a campground or in a particular remote city) to determine whether there is cellular or Wi-Fi coverage within the zones 102, 104, 106. The user can then obtain pre-authorization from the server 130 using the mobile application 140. Again, the timing would also have to be adjusted so that the authorization of funds (AuthGrant) does not expire before the user has a chance to make a purchase. It also means that balance updates to the server 130 may happen after the user has moved away from the machine 120 and has cellular or Wi-Fi coverage again. A mobile-device-to-machine payment system having the ability to implement this option would be able to accept cashless payments without requiring any network connection near the payment accepting unit 120. In some implementations, the mobile-device-to-machine payment processing systems described herein is

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1374 of 1551

located in a remote location where no signal is available, therefore, can accept cashless payments.

[00110] As an example of a situation in which there might be no cellular or Wi-Fi coverage within any of the zones 102, 104, 106 of a particular payment accepting unit 120, the user (a teenager) may be traveling to a remote location to attend summer camp where there is no cellular or Wi-Fi coverage. The camp may have several payment accepting units 120 (e.g., a machine that creates a dedicated "hot spot" that requires payment for use, vending machines, or machines for renting equipment such as bikes, kayaks, or basketballs). The camp facility might notify parents that the mobile-device-to-machine payment system is available. The parents, while at home, could obtain authorization for a particular amount (that could be doled out a certain amount per day or limited to type of machine or location) to be authorized and "loaded" into the user's mobile device 150 and specify that the authorization will not expire for a certain period or until a certain date. Thereafter, while at camp, the user could use the mobile application 140 on his mobile device 150 in a manner similar to those discussed elsewhere herein. Short-range communications may be used for communications between the adapter modules 100 (associated with the machines 120) and users' mobile devices 150.

[00111] One subtle but powerful component of the payment processing system described herein is that it requires a long-range communication capability (e.g., an Internet or cellular network connection) only in the authorization zone 104 and only for the time period required to send the AuthRequest and receive the AuthGrant. Once a valid AuthGrant is received by the mobile device 150, the long-range communication capability (e.g., an Internet or cellular network connection) is not required by either the mobile device 150 or the adapter module 100 in the payment zone 102 as long as the AuthGrant is valid (unexpired). This mechanism allows the system to seamlessly handle authenticated transactions in (temporary) offline mode, with the deferred acknowledgement and transaction messages performing the bookkeeping and cleanup when network connection is regained. The alternatives described above provide a unique way to artificially extend the authorization zone to include any location where the mobile device 150 can communicate with the server 130.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1375 of 1551

MULTIPLE USER RESOLUTION

[00112] As shown in Figure 2, in one practical scenario, multiple users are in the zones 102, 104, 106. As shown in Figure 2, users 1, 2, and 3 are in the payment zone 102 near the machine 120; users 5 and 6 are shown as positioned between the authorization zone 104 and the Bluetooth range 106; users 4 and 7 are in the Bluetooth range 106, user 10 is positioned on the edge of the Bluetooth range 106; and users 8 and 9 are positioned outside of Bluetooth range 106. In some implementations, the mobile-device-to-machine payment processing system manages and resolves issues pertaining to multiple users.

[00113] Users 4 and 7 are within the Bluetooth range 106 and the user 10 is either entering or leaving the Bluetooth range 106. Within the Bluetooth range 106 the users' mobile devices 150 are able to see the adapter module's 100 advertisement. In this zone, the mobile device 150 preferably does not initiate a connection. The adapter module 100 is preferably unaware of the users in the Bluetooth range 106. All the adapter module 100 is doing is advertising its presence to any multitude of users that may be in Bluetooth range 106.

[00114] The adapter module 100 begins to log users as the users (and their respective mobile devices 150) enter the authorization zone 104 (shown in Figure 2 as users 5 and 6). At this point, there is a non-exclusive connection initiated by the mobile device 150 to the adapter module 100. It does a handshake (e.g., to exchange information needed to obtain authorization and, optionally, to log information needed for a self-calibrating authorization zone threshold) and the mobile device 150 contacts the server 130 for an authorization (e.g., sending an AuthRequest and receiving an AuthGrant). The adapter module 100 registers all mobile devices 150 that have requested and received AuthGrants. The adapter module 100 continues communicating with any other mobile device 150 that enters the authorization zone 104. After initial contact, the adapter module 100 may provide the mobile device 150 with a deferral delay of when to check back in with the adapter module 100 allowing opportunity for other mobile devices 150 to communicate with the adapter module 100.

[00115] If there is only one user in the payment zone 102, a purchase transaction may be performed. If there are multiple users in the payment zone 102, the mobile-device-to-machine payment system must handle the situation.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1376 of 1551

[00116] One optional solution for handling the situation of the multiple users in the payment zone 102 is queuing users in the payment zone 102. Once any mobile device 150 enters the payment zone 102, it establishes exclusivity to a particular mobile device 150 (e.g., in a first-come-first-serve manner). Technically, however, the adapter module 100 is not establishing an exclusive connection to the mobile device 150. The adapter module 100 can still perform a round-robin poll and communicate with and advertise to other mobile devices 150. Instead, the adapter module 100 establishes a queue prioritized by RSSI and time (e.g., who was first and whether the authorization has expired) and it notifies (e.g., alerts) other mobile devices 150 to wait. The earliest valid (unexpired) authorization takes precedence when there is any tie in the RSSI. Otherwise, for example, the strongest average RSSI takes priority. Preferably the queue is not a static measure of the RSSI but an averaged measure over the period of time in the queue. This compensates for a scenario in which a user may be walking around in the queue and then shows up at the payment accepting unit 120 just as the previous user is finishing. If another user was also in the payment zone 102 and stood there the entire time, but may have newer authorization, he could win out.

[00117] Anytime that the adapter module 100 cannot determine exactly which user is in the payment zone 102 in front of the payment accepting unit 120, the adapter module 100 will disable hands-free payment. The mobile device 150 will send an alert to the user and he can use swipe to pay (manual mode). All users in payment zone 102 will show "Connected" and the first to swipe payment to the payment accepting unit 120 then locks out other users.

MULTIPLE MODULE RESOLUTION

[00118] In the scenario where there are multiple modules present, determining which payment accepting unit 120 a user is in front of can be a challenge. In some implementations, the mobile-device-to-machine payment processing system described herein allows adapter modules 100 to communicate to other adapter modules 100 in range via Bluetooth. Each user receives authorization grants for specific payment accepting units 120. This means if there are multiple adapter modules 100 within the same authorization zone 104, there will be multiple authorization grants for the user. When the user enters the payment zone 102, it can be difficult to differentiate which payment accepting unit 120 the user is in front of if the payment zones 102 overlap.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1377 of 1551

[00119] To solve this problem, when the user enters the payment zone 102, the adapter modules 100 communicate with each other to determine the RSSI for the particular user (based on the signal from his mobile device 150) to triangulate which adapter module 100 (and the associated payment accepting unit 120) is closer to the user. Optionally, the inter-module communications can restrict the user to establishing an exclusive connection with only one payment accepting unit 120.

[00120] Optionally, when the user connects to a payment accepting unit 120, the mobile device 150 can send a communication to the payment accepting unit 120 for momentary display to the user on the display 122, 124 of the payment accepting unit 120. For example, the mobile device 150 can send a communication (e.g., "connected" or "Fred's Mobile Device Connected") to the payment accepting unit's display 122, 124 for a predetermined period of time (e.g., 1-3 seconds) so when the user is in payment zone 102, it is clear which payment accepting unit 120 the user is connected to prior to making a purchase (either in hands-free or manual mode).

[00121] In addition, when the user is in manual mode, the mobile device 150 can display (e.g., on the touch screen 152 as shown in Figures 10A-10D) a visual indication of the payment accepting unit 120 (e.g., a picture and/or a payment accepting unit ID of the payment accepting unit 120) for visual confirmation. If the user is in manual mode, the user can manually change the payment accepting unit 120.

DESCRIPTIVE SCENARIO

[00122] Figure 7, Figures 8A-8G, and 9A-9E (as well as other figures) can be used to understand a detailed scenario of the mobile-device-to-machine payment processing system described herein. A flow of communications and steps are loosely described below with reference to these (and other figures). It should be noted that alternative scenarios could include, for example, a modified order of the steps performed.

[00123] Prior to vending transactions, a user downloads a mobile application 140 onto his mobile device 150, creates an account, and configures a funding source via, for example, a funding source server 160. A funding source may be, for example, a debit card, a credit card, campus cards, rewards points, bank accounts, payment services (e.g., PayPal™) or other payment option or combination of payment options known or yet to be discovered. The funding

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1378 of 1551

sources may be traditional and/or nontraditional payment sources that are integrated into the ecosystem described herein and then used indirectly as a source of funds. Funds from the funding source are preferably held on the server 130 such that when an AuthRequest is received by the server 130, the server 130 can send an AuthGrant authorizing funds for a purchase.

[00124] The user can specify one or more "favorite" adapter module(s) 100 (that has a one-to-one relationship to the payment accepting unit 120) that he may visit regularly, such as a vending machine at school or work. Favorite adapter modules 100 appear on a pre-filtered list and allow for additional rich features such as hands-free payment.

[00125] The payment accepting unit 120 may be equipped with an adapter module 100 that is constantly advertising its availability via Bluetooth (or other "signals," "communications," and/or "transmissions"). This ongoing advertising and scanning for adapter modules is shown in Figure 8A. As shown, the mobile device 150 is continuously scanning for any adapter module 100 within Bluetooth (or other "signal," "communication," and/or "transmission") range. When the user is within range of that adapter module 100, the mobile device 150 tracks and monitors the signal strength until a predetermined "authorization zone" threshold is achieved.

[00126] Figures 8B and 9A generally show that when the authorization zone threshold is reached, the mobile device 150 enters the authorization zone (block 302) and registers the adapter module 100. The mobile device 150 connects to the server 130 (block 304). The application 140 on the mobile device 150 creates a request for authorization (AuthRequest) and passes the AuthRequest to the server 130 using appropriate communication technology (e.g., GSM, CDMA, Wi-Fi, or the like) (block 306). The server 130 responds with an authorization grant (AuthGrant) encrypted with the specific adapter module's private key (block 306). This authorization token may minimally include the User identifier (ID), Apparatus ID (for the adapter module 100), authorization amount, and expiration time. The mobile device 150 receives the AuthGrant from the server 130, and retains it until the mobile device 150 is ready to issue payment to an adapter module 100. The mobile device 150 collects all pending AuthGrants that may be one or more depending on how many adapter modules 100 are in-range. Unused AuthGrants that expire are purged from the mobile device 150 and the server 130. It is important to note that the mobile device 150 is unable to read the AuthGrant because it is encrypted with the adapter module's unique private key that is only known to server 130 and adapter module

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1379 of 1551

100. This provides a preferred key element of security in the system as the adapter module 100 only trusts AuthGrants that are issued by the server 130, and the AuthGrants cannot be read or modified by the mobile device 150 or any other party in between the server and the adapter module 100. Additional mobile devices 150 may enter the authorization zone 104 (block 308).

[00127] As the user approaches a specific adapter module 100, the user enters the payment zone 102 and an event threshold is triggered based on heuristics performed by the mobile device 150. Blocks 310 and 312 show the loop steps of waiting for a mobile device 150 from the authorization zone 104 to enter the payment zone 102. If the user leaves the authorization zone 104 without entering the payment zone 102, the adapter module 100 returns to advertising its presence (block 300).

[00128] Figures 8C and 9B generally show the user entering the payment zone. The mobile device 150 verifies that it has an unexpired and valid AuthGrant. If the AuthGrant is not good, it may be requested again, repeating the Authorization Request process (block 315). If the AuthGrant is good, the mobile device 150 sends the valid AuthGrant (including the wallet balance (block 322)) to the adapter module 100 to initiate a transaction. The mobile device 150 may issue the AuthGrant automatically without specific user interaction if the hands-free mode is supported (and the device is a favorite (block 318), there is only one device in the payment zone 102 (block 318), and (optionally) there is only one user in the authorization zone 104 (block 320). If any of these factors are not present, the mobile device 150 will prompt and/or wait for the user to begin the transaction manually (block 324).

[00129] Figures 8D, 9C, and 9D generally show the transaction process. As shown in Figure 9C, the adapter module 100 runs through a series of questions to determine if there are any issues that would prevent vending including: has the user canceled in-app? (block 326), has the user walked away? (block 328), is the coin return pressed? (block 330), has more than a predetermined period of time elapsed? (block 332). If the answer to any of these questions is "yes," the transaction does not proceed. If the answers to all of these questions is "no," the user makes a selection (block 334) on the payment accepting unit 120 in the same or similar manner as compared to if cash or credit were presented to the payment accepting unit 120. If the machine 120 is able to vend (block 336), it attempts to release the product. If the vend fails (block 338) it is reported by the machine (block 340) and a credit is returned to the virtual wallet (block 342).

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1380 of 1551

If the vend is successful (block 338) it is reported by the machine (block 344). Put another way, after the transaction is complete, the adapter module 100 returns to the mobile device 150 the details of the transaction as well as an encrypted packet containing the vend details to be sent to the server 130 via the mobile device 150. Optionally, the adapter module 100 can pass additional information not directly related to the transaction such as payment accepting unit health, sales data, error codes, etc.

[00130] Figures 8D and 9E generally show the multi-vend function. If the machine has enabled multi-vend capabilities (block 350) and the multi-vend limit has not been reached, the process returns to the question of whether the user is in the payment zone (block 310 of Figure 9A). If the machine does not have enabled multi-vend capabilities (block 350) or the multi-vend limit has been reached, the wallet is decremented by the vend amount(s) and "change" is returned to the virtual wallet (block 354) and the process ends (block 356).

[00131] Figure 8E is a schematic flow diagram of an example login process. Figure 8F is a schematic flow diagram of an example boot-up process. Figure 8G is a schematic flow diagram of an example account check/update process.

[00132] Several of the figures are flow charts (e.g., Figures 9A-9E) illustrating methods and systems. It will be understood that each block of these flow charts, components of all or some of the blocks of these flow charts, and/or combinations of blocks in these flow charts, may be implemented by software (e.g., coding, software, computer program instructions, software programs, subprograms, or other series of computer-executable or processor-executable instructions), by hardware (e.g., processors, memory), by firmware, and/or a combination of these forms. As an example, in the case of software, computer program instructions (computer-readable program code) may be loaded onto a computer to produce a machine, such that the instructions that execute on the computer create structures for implementing the functions specified in the flow chart block or blocks. These computer program instructions may also be stored in a memory that can direct a computer to function in a particular manner, such that the instructions stored in the memory produce an article of manufacture including instruction structures that implement the function specified in the flow chart block or blocks. The computer program instructions may also be loaded onto a computer to cause a series of operational steps to be performed on or by the computer to produce a computer implemented process such that the

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1381 of 1551

instructions that execute on the computer provide steps for implementing the functions specified in the flow chart block or blocks. Accordingly, blocks of the flow charts support combinations of steps, structures, and/or modules for performing the specified functions. It will also be understood that each block of the flow charts, and combinations of blocks in the flow charts, may be divided and/or joined with other blocks of the flow charts without affecting the scope of the invention. This may result, for example, in computer-readable program code being stored in whole on a single memory, or various components of computer-readable program code being stored on more than one memory.

ADDITIONAL IMPLEMENTATIONS

[00133] Figure 23 illustrates a schematic flow diagram of a process 1000 of authenticating a user to perform a transaction in the payment processing system in accordance with some implementations. In some implementations, the payment processing system includes one or more payment modules 100 (e.g., each associated with a respective payment accepting unit 120 such an automatic retailing machine for dispensing goods and/or services), one or more mobile devices 150 (e.g., each executing the application 140 for the payment processing system either as a foreground or background process), and the server 130. The server 130 manages the payment processing system and, in some cases, is associated with an entity that supplies, operates, and/or manufactures the one or more payment modules 100. For brevity, the process 1000 will be described with respect to a respective payment module 100 and a respective mobile device 150 in the payment processing system.

[00134] The payment module 100 broadcasts (1002), via a short-range communication capability (e.g., BLE), a packet of information (sometimes also herein called "advertised information"). The packet of information at least includes an authorization code and an identifier associated with the payment module 100 (module ID). In some implementations, the packet of information further includes a firmware version of the payment module 100 and one or more status flags corresponding to one or more states of the payment module 100 and/or the payment accepting unit 120. The information included in the packet broadcast by the payment module 100 is further discussed below with reference to Figure 24A.

[00135] In some implementations, the payment module 100 sends out a unique authorization code every X seconds (e.g., 100 ms, 200 ms, 500 ms, etc.). In some

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1382 of 1551

implementations, the unique authorization codes are randomly or pseudo-randomly generated numbers. In some implementations, the payment module 100 stores broadcasted authorization codes until a received authorization grant token matches one of the stored authorization codes. In some implementations, the payment module 100 stores broadcasted authorization codes for a predetermined amount of time (e.g., Y minutes) after which time an authorization code expires and is deleted. In some implementations, the authorization code is encrypted with a shared secret key known by the server 130 but unique to the payment module 100. In some implementations, the payment module 100 initializes a random number and then the authorization codes are sequential counts from this random number. In such implementations, the payment module 100 stores the earliest valid (unexpired) counter without a need to store every valid authorization code. In some implementations, the authentication code included in the broadcast packet of information is a hash value of the randomly or pseudo-randomly generated number or the sequential number.

[00136] The mobile device 150 receives the broadcasted packet of information, and the mobile device 150 sends (1004), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), an authorization request to the server 130. For example, an application 140 that is associated with the payment processing system is executing as a foreground or background process on the mobile device 150. In this example, the application 140 receives the broadcasted packet of information when the mobile device 150 is within the communication zone of the payment module 100 (i.e., BLE range) and either automatically sends the authorization request to the server 130 or sends the authorization request to the server 130 when the mobile device 150 is within the authorization zone of the payment module 100. In some implementations, the broadcasted packet of information includes a baseline authorization zone threshold (i.e., an authorization zone criterion) indicating a baseline RSSI that the mobile device 150 (or the application 140) is required to observe before being within the authorization zone of the payment module 100. In some implementations, the mobile device 150 (or the application 140) offsets the baseline authorization zone threshold based on the strength and/or reception of the short-range communication capability (e.g., BLE radio/transceiver) of the mobile device 150. In some implementations, the authorization request at least includes the authorization code which was included in the broadcasted packet of information, an identifier associated with the user of the mobile device 150 or the user account under which the user of the mobile device 150 is

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1383 of 1551

logged into the application 140 (user ID), and the identifier associated with the payment module 100 (module ID). In some implementations, the authentication code included in authorization request is the hash value in cleartext. The authorization request is further discussed below with reference to Figure 24B.

[00137] After receiving the authorization request, the server 130 processes (1006) the authorization request. In some implementations, the server 130 decrypts the authorization code included in the authorization request with the shared secret key corresponding to the payment module 100. In some implementations, the server 130 determines whether the user associated with the user ID in the authorization request has sufficient funds in his/her account for the payment processing system to perform a transaction at the machine 120 that is associated with the payment module 100 corresponding to the module ID in the authorization request.

[00138] The server 130 sends (1008), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), an authorization grant token to the mobile device 150. In some implementations, the server 130 does not send the authorization grant token if the authorization code in the authorization request cannot be decrypted with the shared secret key corresponding to the payment module 100 (e.g., the authorization code is corrupted or hacked). In some implementations, the server 130 does not send the authorization grant token if the user associated with the user ID in the authorization request does not have sufficient funds in his/her account. In some implementations, in addition to the authorization grant token, the server 130 sends a message directly to the mobile device 150 which is not encrypted with the shared secret key corresponding to the payment module 100. After receiving the message, the mobile device 150 displays an appropriate message to the user such as insufficient balance or declined authorization. In some implementations, the server 130 sends an authorization grant token for an amount equal to zero; in which case, the payment module 100 interprets this as a declined or failed authorization which can result for any number of reasons including, but not limited to, insufficient balance or credit.

[00139] The mobile device 150 receives the authorization grant token, and, subsequently, the mobile device 150 detects (1010) a trigger condition. In some implementations, the mobile device 150 (or the application 140) detects the trigger condition via the hand-free mode (e.g., upon entrance into the payment zone of the payment module 100) or manual mode (e.g.,

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1384 of 1551

interacting with the user interface of the application 140 to initiate a transaction with the payment accepting unit associated with the payment module 100).

[00140] In some implementations, unused authorization grants (e.g., if there was no trigger condition or it expired) are canceled by the mobile device 150 by sending a cancellation message to the server 130 corresponding to the unused authorization grant. In some implementations, the server 130 denies or limits the number of authorization grants sent to the mobile device 150 until it has received transaction information or cancellation of authorization outstanding authorization grants sent to the mobile device 150.

[00141] In response to detecting the trigger condition, the mobile device 150 sends (1012), via a short-range communication capability (e.g., BLE), the authorization grant token to the payment module 100. Subsequently, the machine 120 displays credit to the user (e.g., via one of the displays 122 or 124 shown in Figure 19) and the user interacts with the input mechanisms of the machine 120 (e.g., via the buttons 126 or a touch screen display 124 shown in Figure 19) to purchase products and/or services.

[00142] Figure 24A illustrates a block diagram of a packet 1100 of information broadcast by the payment module 100 (e.g., in step 1002 of the process 1000 in Figure 23) in accordance with some implementations. In some implementations, the packet 1100 at least includes: module ID 1102 and authorization code 1104. In some implementations, the packet 110 additional includes: a firmware version 1106 and one or more status flags 1108.

[00143] In some implementations, the module ID 1102 is a unique identifier corresponding to the payment module 100 (sometimes also herein called the "adapter module 100") that broadcast the packet 1100.

[00144] In some implementations, the authorization code 1104 is a hash value in cleartext. In some implementations, the payment module 100 randomly or pseudo-randomly generates a number or determines a sequential number (*See* step 1002 of process 1000 in Figure 23) and performs a predetermined hash function (e.g., SHA-256) on the number to produce the hash value as the authorization code 1104. In some implementations, the authorization code 1104 is a unique code that is encrypted with a secret encryption key corresponding to the payment module 100. The secret encryption key is shared with the server 130, which enables the server 130 to decrypt the authorization code 1104 and encrypt the authorization grant token but not the mobile

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1385 of 1551

device 150. In some implementations, the encryption between server 130 and payment module 100 is accomplished by two pairs of public/private keys.

[00145] In some implementations, the firmware version information 1106 identifies a current firmware version 1112 of the payment module 100. In some implementations, the firmware version information 1106 also includes update status information 1114 indicating one or more packets received by the payment module 100 to update the firmware or one or more packets needed by the payment module 100 to update the firmware. In some implementations, the one or more status flags 1108 indicate a state of the payment module 100 and/or the payment accepting unit 120 associated with the payment module 100. In some implementations, the one or more status flags 1108 indicate a state of the payment module 100 such upload information indicator 1116 indicating that that the payment module 100 has information to be uploaded to the server 130 (e.g., transaction information for one or more interrupted transactions). In some implementations, upload information indicator 1116 triggers the mobile device 150 to connect to payment module 100 immediately (e.g., if it has interrupted transaction information to be uploaded to the server 130). In some implementations, the one or more status flags 1108 indicate a state of the payment accepting unit 120 including one or more of an error indicator 1118 (e.g., indicating that a bill and/or coin acceptor of the payment accepting unit 120 is experiencing a jam, error code, or malfunction), a currency level indicator 1120 (e.g., indicating that the level of the bill and/or coin acceptor reservoir of the payment accepting unit 120 is full or empty), and/or inventory level(s) indicator 1122 (e.g., indicating that one or more products of the payment accepting unit 120. In some implementations, the one or more status flags 1108 are error codes issued by payment accepting unit 120 over the MDB.

[00146] In some implementations, the zone criteria information 1110 specifies an authorization zone criterion 1124 (e.g., a baseline authorization zone threshold indicating a baseline RSSI that the mobile device 150 (or the application 140) is required to observe before being within the authorization zone of the payment module 100) and/or a payment zone criterion 1126 (e.g., a baseline payment zone threshold indicating a baseline RSSI that the mobile device 150 (or the application 140) is required to observe before being within the payment zone of the payment module 100). In some implementations, the baseline authorization zone threshold and the baseline payment zone threshold are default values determined by the server 130 or stored as variables by the application 140, in which case the authorization zone criterion 1124 and

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1386 of 1551

payment zone criterion 1126 are offsets to compensate for the strength and/or reception of the short-range communication capability (e.g., BLE radio/transceiver) of the payment module 100. Alternatively, zone criteria information 1110 includes a spread between the baseline authorization zone threshold and the baseline payment zone threshold. Thus, the mobile device 150 (or the application 140) determines the baseline authorization zone threshold and the baseline payment zone threshold based on the spread value and a default value for either the baseline authorization zone threshold or the baseline payment zone threshold. For example, the spread indicates -10 db and the default baseline payment zone threshold is -90 db; thus, the baseline authorization zone threshold is -80 db. Continuing with this example, after determining the baseline authorization zone threshold and the baseline payment zone threshold, the mobile device 150 (or the application 140) may further adjust the authorization zone threshold and/or the payment zone threshold based on the strength and/or reception of its short-range communication capability (i.e., BLE radio/transceiver).

[00147] Figure 24B is a block diagram of an authorization request 1130 sent by the mobile device 150 to the server 130 (e.g., in step 1004 of the process 1000 in Figure 23) in accordance with some implementations. In some implementations, the authorization request 1130 at least includes: a module ID 1102, a user ID 1134, and an authorization code 1104.

[00148] In some implementations, the module ID 1102 is a unique identifier corresponding to the payment module 100 that broadcast the 1100 that included the authorization code 1104.

[00149] In some implementations, the user ID 1134 is an identifier associated with the user of the mobile device 150 sending the authorization request 1130 to the server 130. In some implementations, the user ID 1134 is associated with the user account under which the user of the mobile device 150 is logged into the application 140.

[00150] In some implementations, the authorization code 1130 includes the authorization code 1104 included in the packet 1100 of information that was broadcast by the payment module 100.

[00151] Figure 24C is a block diagram of an authorization grant token 1140 sent by the server 130 to the mobile device 150 (e.g., in step 1008 of the process 1000 in Figure 23) in accordance with some implementations. In some implementations, in accordance with a

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1387 of 1551

determination that the authorization code 1136 included in the authorization request 1130 from the mobile device 150 is valid and that the user associated with the mobile device 150 has sufficient funds in his/her account for the payment processing system, the server 130 generates the authorization grant token 1140. In some implementations, the authorization grant token 1140 at least includes: a module ID 1102, a user ID 1134, an authorized amount 1146, (optionally) an expiration period offset 1148, and (optionally) the authorization code 1104.

[00152] In some implementations, the module ID 1102 is a unique identifier corresponding to the payment module 100 that broadcast the packet 1100 that included the authorization code 1104.

[00153] In some implementations, the user ID 1134 is an identifier associated with the user of the mobile device 150 that sent the authorization request 1130 to the server 130.

[00154] In some implementations, the authorized amount 1146 indicates a maximum amount for which the user of the mobile device 150 is authorized for a transaction using the authorization grant token 1140. For example, the authorized amount 1146 is predefined by the user of the mobile device 150 or by the server 130 based on a daily limit or based on the user's total account balance or based on a risk profile of the user correspond to the user ID 1134.

[00155] In some implementations, the expiration period 1148 offset indicates an offset to the amount of time that the payment module 100 holds the authorization grant token 1140 valid for initiation of a transaction with the machine 120 associated with the payment module 100. For example, the expiration period offset 1148 depends on the history and credit of the user of mobile device 150 or a period predefined by the user of mobile device 150.

[00156] In some implementations, the authorization grant token 1140 further includes the authorization code 1104 that was included in the authorization request 1130. In some implementations, when the authorization code 1104 is the hash value, the server 130 encrypts the authorization grant token 1140 including the hashed value with the shared secret encryption key associated with payment module 100. Subsequently, when mobile device 150 sends the authorization grant token 1140 to payment module 100 after detecting a trigger condition, the payment module 100 decrypts the authorization grant token 1140 using the secret key known only to server 130 and payment module 100 (which authenticates the message and the authorization grant), and then matches the hash value included in the decrypted authorization

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1388 of 1551

grant token 1140 to previously broadcast valid (unexpired) hash values (i.e., auth codes) to determine validity of the (which was known only by payment module 100).

[00157] Figure 24D illustrates a block diagram of transaction information 1150 generated by the payment module 100 (e.g., in step 1254 of the process 1250 in Figure 25B) in accordance with some implementations. In some implementations, the transaction information 1150 includes: a transaction ID 1152 for the respective transaction, a module ID 1154, a user ID 1156, (optionally) the authorization code 1158, transaction status information 1160, the transaction amount 1162, and other information 1164.

[00158] In some implementations, the transaction ID 1152 is a unique identifier corresponding to the respective transaction. In some implementations, the transaction ID 1152 is encoded based on or associated with the time and/or date on which and the location at which the respective transaction took place.

[00159] In some implementations, the module ID 1154 is a unique identifier corresponding to the payment module 100 that performed the respective transaction.

[00160] In some implementations, the user ID 1156 is an identifier associated with the user of the mobile device 150 that initiated the respective transaction.

[00161] In some implementations, the authorization code 1158 corresponds to the original authorization code (e.g., auth code 1104, Figures 24 A-24C) and/or authorization grant token (e.g., auth grant token 1140, Figure 24C) that was used to initiate the respective transaction. In some implementations, the authorization code 1156 is encrypted with a unique encryption key corresponding to the payment module 100.

[00162] In some implementations, the transaction status information 1160 includes an indication whether the respective transaction was completed, not-completed, or aborted. For example, the respective transaction is incomplete if a jam occurred at the payment accepting unit 120 and the user did not receive the product associated with the respective transaction. For example, if the user walks away from the payment accepting unit 120 after money was credited for the respective transaction, the respective transaction is aborted. In another example, if respective transaction times out after a predetermined time period because the user failed to select a product at the payment accepting unit 120, the respective transaction is aborted. In

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1389 of 1551

another example, if the user actuates a bill or coin return mechanism of the payment accepting unit 120, the respective transaction is aborted.

[00163] In some implementations, the transaction amount 1162 indicates the amount of the respective transaction or the amount of each of multiple transactions (e.g., in a multi-vend scenario). In some implementations, the transaction amount 1162 is encrypted with a unique encryption key corresponding to the payment module 100.

[00164] In some implementations, the other information 1164 includes other information related to the respective transaction such as the items dispensed by the payment accepting unit 120 and the type of transaction (e.g., coins, bills, credit card, manual mode, hands-free mode, etc.). In some implementations, the other information 1164 includes other information related to the payment module 100 and/or the payment accepting unit 120 associated with the payment module 100. For example, the other information 1164 includes a verification request to the server 130 in order to implement new firmware. In another example, the other information 1164 includes transaction information from one or more previous interrupted transactions. In another example, the other information 1164 includes transaction information for one or more transactions paid via bills and/or coins. In another example, the other information 1164 includes inventory information as to one or more products of the payment accepting unit 120.

[00165] Figure 25A illustrates a schematic flow diagram of a process 1200 for providing a representation of a machine event at a mobile device in accordance with some implementations. In some implementations, the payment processing system includes one or more payment modules 100 (e.g., each associated with a respective payment accepting unit 120 such an automatic retailing machine for dispensing goods and/or services), one or more mobile devices 150 (e.g., each executing the application 140 for the payment processing system either as a foreground or background process), and the server 130. The server 130 manages the payment processing system and, in some cases, supplies, operates, and/or manufactures the one or more payment modules 100. For brevity, the process 1200 will be described with respect to a respective payment module 100 associated with a respective payment accepting unit 120 (sometimes also herein called the "machine 120") and a respective mobile device 150 in the payment processing system.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1390 of 1551

[00166] In some implementations, the process 1200 occurs after the mobile device 150 sends the AuthGrant in Figure 8C. In some implementations, the process 1200 occurs after the mobile device 150 sends the authorization grant to the payment module 100 in operation 1012 of process 1000 in Figure 23.

[00167] The payment module 100 obtains (1202) an indication corresponding to an event at the machine 120. For example, after the process 1000 in Figure 23, the user of the mobile device 150 selects a product to purchase from the machine 120 by interacting with one or more input mechanisms of the machine 120 (e.g., buttons 126 or a touch screen display 124 shown in Figure 19), and the machine 120 dispenses the selected product. Continuing with this example, after the product is dispensed, the transaction is complete and the payment module 100 obtains an indication from the machine of the completed transaction. In some implementations, the indication includes the amount of the transaction and (optionally) machine status information associated with the machine 120 such as inventory information as to one or more products of the payment accepting unit 120 and/or the like. In some implementations, the indication includes status information indicating that the transaction was aborted (e.g., via actuation of a coin return mechanism at the machine 120) or that there was an error with the transaction (e.g., a vending jam or other malfunction with the machine 120).

[00168] After obtaining the indication corresponding to completion of the first transaction, the payment module 100 generates (1204) a notification corresponding to the event at the machine 120.

[00169] The payment module 100 sends (1206), via a short-range communication capability (e.g., BLE), the notification to the mobile device 150. In some embodiments, in addition to the notification corresponding to the event at machine 120, the payment module 100 sends a promotion or advertisement to the mobile device 150 that is targeted to the user of the mobile device 150 based on the transaction or the user ID included in the AuthGrant or authorization grant token that initiated the transaction. In some embodiments, in addition to the notification corresponding to the event at machine 120, the payment module 100 sends a pseudo randomly selected promotion or advertisement to the mobile device 150 that is selected from a set of promotions or advertisements stored by the payment module 100. For example, the promotion is a coupon for a free soda following the purchase of ten sodas from the machine 120

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1391 of 1551

by the user of the mobile device 150. For example, the promotion is a random 50% off coupon or free soda coupon. For example, the transaction corresponds to a vended soda and the advertisement corresponds to a new soda from the same company that produces the vended soda.

[00170] The mobile device 150 provides (1208) a representation of the notification. For example, in Figure 26A, the mobile device 150 displays user interface 1302 on touch screen 152 with a message 1306 that indicates that the first transaction is complete. For example, in Figure 26C, the mobile device 150 displays user interface 1320 on touch screen 152 with a message 1322 that indicates that the transaction was aborted. For example, in Figure 26D, the mobile device 150 displays user interface 1330 on touch screen 152 with a message 1332 that indicates that there was an error with the transaction. For example, the mobile device 150 also displays a representation of the promotion of advertisement on the user interface for the application 140.

[00171] Figure 25B illustrates a schematic flow diagram of a process 1250 for processing acknowledgement information in accordance with some implementations. In some implementations, the payment processing system includes one or more payment modules 100 (e.g., each associated with a respective payment accepting unit 120 such an automatic retailing machine for dispensing goods and/or services), one or more mobile devices 150 (e.g., each executing the application 140 for the payment processing system either as a foreground or background process), and the server 130. The server 130 manages the payment processing system and, in some cases, supplies, operates, and/or manufactures the one or more payment modules 100. For brevity, the process 1250 will be described with respect to a respective payment module 100 associated with a respective payment accepting unit 120 (machine 120) and a respective mobile device 150 in the payment processing system.

[00172] In some implementations, the process 1250 occurs after the mobile device 150 sends the AuthGrant in Figure 8C. In some implementations, the process 1250 occurs after the mobile device 150 sends the authorization grant to the payment module 100 in operation 1012 of process 1000 in Figure 23.

[00173] The payment module 100 obtains (1252) an indication corresponding to completion of a first transaction from the machine 120. For example, after the process 1000 in Figure 23, the user of the mobile device 150 selects a product to purchase from the machine 120 by interacting with one or more input mechanisms of the machine 120 (e.g., buttons 126 or a

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1392 of 1551

touch screen display 124 shown in Figure 19), and the machine 120 dispenses the selected product. Continuing with this example, after the product is dispensed, the transaction is complete and the payment module 100 obtains an indication from the machine of the completed transaction. In some implementations, the indication includes the amount of the transaction and (optionally) machine status information associated with the machine 120 such as inventory information as to one or more products of the payment accepting unit 120 and/or the like.

[00174] After obtaining the indication corresponding to completion of the first transaction, the payment module 100 generates (1254) a first notification with first transaction information based on the indication, and the payment module 100 stores the first transaction information. In some implementations, the first transaction information includes a transaction ID for the first transaction, a module ID corresponding to payment module 100, a user ID corresponding to the mobile device 150, transaction status information indicating that the first transaction is complete, and the transaction amount indicated by the indication. In some implementations, the payment module 100 retains the authorization code included in the original broadcasted packet and/or the authorization grant token and includes the authorization code in the first transaction information. In some implementations, the authorization code is encrypted with a secret key corresponding to the payment module 100, which is shared with the server 130 but not the mobile device 150. In some implementations, the first transaction information further includes other information such as the machine status information included in the first notification or transaction information corresponding to previous interrupted transaction(s). See Figure 24D and the accompanying text for further discussion regarding transaction information 1150.

[00175] The payment module 100 sends (1256), via a short-range communication capability (e.g., BLE), the first notification with first transaction information to the mobile device 150. In some embodiments, in addition to first transaction information corresponding to completion of the first transaction at machine 120, the first notification includes a promotion or advertisement to the mobile device 150 that is targeted to the user of the mobile device 150 based on the transaction or the user ID included in the AuthGrant or authorization grant token that initiated the transaction. In some embodiments, in addition to first transaction information corresponding to completion of the first transaction at machine 120, the first notification includes a pseudo randomly selected promotion or advertisement to the mobile device 150 that is selected from a set of promotions or advertisements stored by the payment module 100. For example, the

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1393 of 1551

promotion is a coupon for a free soda following the purchase of ten sodas from the machine 120 by the user of the mobile device 150. For example, the promotion is a random 50% off coupon or free soda coupon. For example, the transaction corresponds to a vended soda and the advertisement corresponds to a new soda from the same company that produces the vended soda.

[00176] The mobile device 150 provides (1258) a representation of the first notification. For example, in Figure 26A, the mobile device 150 displays user interface 1302 on touch screen 152 with a message 1306 that indicates that the first transaction is complete. For example, the mobile device 150 also displays a representation of the promotion of advertisement on the user interface for the application 140.

[00177] The mobile device 150 sends (1260), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), the first transaction information to the server 130.

[00178] The server 130 processes (1262) the first transaction information. For example, the server 130 debits the account of the user associated with the user ID in the first transaction information in the amount indicated by the first transaction information.

[00179] The server 130 sends (1264), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), first acknowledgment information to the mobile device 150. In some implementations, the first acknowledgment information acknowledges that the server 130 received the first transaction information. In some implementations, the first acknowledgment information includes the user ID, the module ID, the transaction ID, and (optionally) the authorization grant included in the transaction information (e.g., auth grant 1158, Figure 24D).

[00180] After receiving the first acknowledgement information, the mobile device 150 sends (1266), via a short-range communication capability (e.g., BLE), the first acknowledgment information to the payment module 100.

[00181] After receiving the first acknowledgment information, the payment module 100 deletes (1268) the stored first transaction information.

[00182] Attention is now directed towards implementations of user interfaces and associated processes that may be implemented on the mobile device 150 with zero or more speakers, zero or more microphones, and a display. For example, the display is a touch screen

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1394 of 1551

(sometimes also herein called a "touch screen display") enabled to receive one or more contacts and display information (e.g., media content, websites and web pages thereof, user interface for the application 140, and/or user interfaces for applications). Figures 26A-26D illustrate example user interfaces for providing a representation of a machine event at a mobile device in accordance with some implementations.

[00183] Figures 26A-26D show user interfaces displayed on mobile device 150 (e.g., a mobile phone); however, one skilled in the art will appreciate that the user interfaces shown in Figures 26A-26D may be implemented on other similar computing devices. The user interfaces in Figures 26A-26D are used to illustrate the processes described herein, including the process described with respect to Figures 25A-25B and 27A-27B.

[00184] For example, a user of the mobile device 150 approaches a machine 120 (e.g., vending machine 78x928 as shown in Figures 10A-10D) and executes application 140 on the mobile device 150 so as to perform an electronic transaction with the machine 120. For example, with reference to Figures 10C-10D, the user of the mobile device 150 initiates a transaction with the machine 120 (e.g., vending machine 78x928) by performing a swipe gesture at a location corresponding to the representation of the dollar bill (e.g., a substantially vertical swipe gesture from a location corresponding to the representation of the dollar bill to the top edge of the mobile device 150).

[00185] Figure 26A illustrates the mobile device 150 displaying a user interface 1302 of the application 140 on touch screen 152 after the user of the mobile device 150 initiates and performs a transaction with the machine 120. In Figure 26A, the user interface 1302 includes prepaid balance 1304 which indicates that $1.00 has been deducted from the prepaid balance after performing a transaction with the machine 120 as compared to the prepaid balance in Figure 10C-10D (i.e., $9.00 in Figures 10C-10D and $8.00 in Figure 26A). In Figure 26A, the user interface 1302 also includes a message 1306 indicating that the transaction with the machine 120 is complete.

[00186] Figure 26B illustrates the mobile device 150 displaying a user interface 1310 of the application 140 on touch screen 152 after the user of the mobile device 150 initiates a transaction with the machine 120 and an error with the transaction occurs or the transaction is aborted. In Figure 26B, the user interface 1310 shows the representation of the dollar bill sliding

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1395 of 1551

onto the touch screen 152 (e.g., in a substantially top to bottom manner). In Figure 26B, the interface 1310 includes prepaid balance 1312 which indicates that no money has been deducted from the prepaid balance after performing a transaction with the machine 120 as compared to the prepaid balance in Figure 10C-10D (i.e., $9.00 in Figures 10C-10D and $9.00 in Figure 26B).

[00187] Figure 26C illustrates the mobile device 150 displaying a user interface 1320 of the application 140 on touch screen 152 after the representation of the dollar bill slides onto the touch screen 152 in Figure 26B due to the transaction being aborted. For example, the user aborts the transaction by actuating a coin return mechanism of the machine 120. In another example, the user aborts the transaction by selection an abort affordance on the interface of the application 140 (not shown). In Figure 26C, the user interface 1320 includes a message 1322 indicating that the transaction with the machine 120 was aborted and that the user's account was not debited for the aborted transaction.

[00188] Figure 26D illustrates the mobile device 150 displaying a user interface 1330 of the application 140 on touch screen 152 after the representation of the dollar bill slides onto the touch screen 152 in Figure 26B due to the occurrence of an error with the transaction. For example, a malfunction with the machine 120 (e.g., a vending jam or stuck item) causes the error to occur. In Figure 26D, the user interface 1330 is associated with the application 140 executed on the mobile device 150. In Figure 26D, the user interface 1330 includes a message 1332 indicating that an error occurred during the transaction with the machine 120 and that the user's account was not debited for the transaction.

[00189] Figures 27A-27B illustrate a flowchart diagram of a method 1400 of presenting representations of payment accepting unit events in accordance with some implementations. In some implementations, the method 1400 is performed by a device with one or more processors, memory, one or more output devices, and two or more communication capabilities. For example, in some implementations, the method 1400 is performed by the mobile device 150 (Figures 5 and 21) or a component thereof (e.g., the application 140). In some implementations, the method 1400 is governed by instructions that are stored in a non-transitory computer readable storage medium (e.g., the memory 860, Figure 21) and the instructions are executed by one or more processors (e.g., the processing unit 850, Figure 21) of the device. Optional operations are indicated by dashed lines (e.g., boxes with dashed-line borders).

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1396 of 1551

[00190] After sending a request to a payment module via a first communication capability transaction to initiate a transaction with a payment accepting unit (e.g., an offline-payment operated machine such as a vending machine or kiosk) associated with the payment module, the mobile device obtains (1402) a notification from the payment module via the first communication capability, where the notification indicates an event at the payment accepting unit associated with the payment module. In some implementations, method 1400 occurs after the mobile device 150 sends the AuthGrant in Figure 8C. In some implementations, method 1400 occurs after the mobile device 150 sends the authorization grant to the payment module 100 in operation 1012 of process 1000 in Figure 23. Operation 1206 of Figure 25A, for example, shows the mobile device 150 receiving a notification sent by the payment module 100 (e.g., the adapter module 100, Figures 5 and 20) sent via the first communication capability (e.g., a short-range communication technology/protocol such as BLE). The notification indicates an event at the payment accepting unit (e.g., the payment accepting unit 120, Figures 5 and 19) (sometimes also herein called "machine 120") associated with the payment module 100.

[00191] In some implementations, the first communication capability corresponds (1404) to a short-range communication protocol. As described above, the short-range communication protocols include BLE, NFC, and/or other protocols utilizing non-persistent communication channels.

[00192] In response to obtaining the notification, the mobile device provides (1406) a representation of the notification to a user of the mobile device via the one or more output devices of the mobile device. For example, in Figure 26A, the mobile device 150 displays user interface 1302 on touch screen 152 with a message 1306 that indicates that the first transaction is complete. For example, in Figure 26C, the mobile device 150 displays user interface 1320 on touch screen 152 with a message 1322 that indicates that the transaction was aborted. For example, in Figure 26D, the mobile device 150 displays user interface 1330 on touch screen 152 with a message 1332 that indicates that there was an error with the transaction.

[00193] In some implementations, the one or more output devices of the mobile device include (1408) at least one of: a display, one or more speakers, one or more LEDs, and a vibration mechanism. For example, the mobile device 150 includes one or more of a display

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1397 of 1551

(e.g., the touch screen 152, Figures 10A-10D), one or more speakers, one or more LEDs, and a vibration mechanism.

[00194] In some implementations, the representation of the notification is at least one of (1410): a message displayed on the display of the mobile device; a banner notification displayed on a display of the mobile device; a vibration alert from the vibration mechanism of the mobile device; an aural alert from the one or more speakers of the mobile device; and a visual alert from the one or more LEDs of the mobile device. For example, in Figures 26B-26D, the representation of the notification includes messages 1306, 1322, and 1332 displayed on the touch screen 152 of the mobile device 150. In another example, the representation of the notification is a predefined sequence of vibrations provided by the vibration mechanism of the mobile device 150. In another example, the representation of the notification is a predefined sequence of tones provided by the one or more speakers of the mobile device 150. In another example, the representation of the notification is a predefined sequence of blinking LEDs of the mobile device 150.

[00195] In some implementations, the notification indicates (1412) abortion of a transaction initiated by the user of the mobile device. In Figure 26C, for example, the user interface 1320 includes the message 1322 indicating that the transaction has been aborted. For example, the user aborts the transaction by actuating a coin return mechanism of the machine 120. In another example, the user aborts the transaction by selection an abort affordance on the interface of the application 140 (not shown).

[00196] In some implementations, the notification indicates (1414) completion of a transaction between the user of the mobile device and the payment accepting unit. In Figure 26A, for example, the user interface 1302 includes the message 1306 indicating that completion of the transaction with the machine 120 initiated by the user of the mobile device 150.

[00197] In some implementations, the notification indicating completion of the transaction at least includes (1416) an amount of the completed transaction. In Figure 26A, for example, the user interface 1302 includes prepaid balance 1304 which indicates that $1.00 has been deducted from the prepaid balance after performing a transaction with the machine 120 as compared to the prepaid balance in Figure 10C-10D (i.e., $9.00 in Figures 10C-10D and $8.00 in Figure 26A).

[00198] In some implementations, the mobile device sends (1418) at least a portion of the notification to a server via a second communication capability distinct from the first

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1398 of 1551

communication capability. Operation 1260 of Figure 25B, for example, shows the mobile device 150 sending first transaction information to the server 130 for a completed transaction via the second communication capability (e.g., a long-range communication protocols such as Wi-Fi, CDMA, GSM, and/or the like). For example, the first transaction information at least includes the amount of the first completed transaction.

[00199] In some implementations, the first communication capability corresponds (1420) to a short-range communication protocol and the second communication capability corresponds to a long-range communication protocol. For example, the first communication capability of the mobile device 150 is a radio/transceiver means for communicating via one or more short-range communication protocols such as BLE, NFC, and/or the like (i.e., a non-persistent communication channel). For example, the second communication capability of the mobile device 150 is a radio/transceiver means for communicating via one or more long-range communication protocols such as Wi-Fi, CDMA, GSM, and/or the like.

[00200] In some implementations, the notification indicates (1422) failure of a transaction initiated by the user of the mobile device or a malfunction associated with the payment accepting unit. In Figure 26D, for example, the user interface 1330 includes the message 1332 indicating that there was an error with the transaction. For example, the transaction fails due to a vending jam or other malfunction. In another example, the payment accepting unit experiences a malfunction due to an open door or the like. In some implementations, at least a portion of the failure/malfunction notification is sent to the sever 130 and an alert is subsequently sent to the operator of the payment accepting unit (e.g., the machine 120) by the server 130.

[00201] It should be understood that the particular order in which the operations in Figures 27A-27B have been described is merely for example purposes and is not intended to indicate that the described order is the only order in which the operations could be performed. One of ordinary skill in the art would recognize various ways to reorder the operations described herein. Additionally, it should be noted that details of other processes described herein with respect to other methods described herein are also applicable in an analogous manner to the method 1400 described above with respect to Figures 27A-27B.

[00202] Figure 28A illustrates a block diagram of an offline-payment operated machine 1500 in accordance with some implementations. For example, the offline-payment operated

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1399 of 1551

machine 1500 (e.g., a form of the machine 120) is an electro-mechanical machine capable of accepting currency (e.g., coins), which is not connected to any networks (e.g., telephone, cellular, or Wi-Fi). For example, the offline-payment operated machine 1500 is a washer or dryer at a laundromat, a parking meter, a car wash payment kiosk, or other offline-payment operated machine that dispenses goods and/or services.

[00203] In Figure 28A, the offline-payment operated machine 1500 includes a microswitch 1502, a control unit 1506, a power supply 1508, a transistor 1510, and an operation unit 1512. The components of the offline-payment operated machine 1500 in Figure 28A are examples and one of skill in the art will appreciate that various other components may be included in or excluded from the offline-payment operated machine 1500.

[00204] In Figure 28A, the microswitch 1502 is a leveraged microswitch with lever 1504. For example, the microswitch 1502 is a CHERRY BRAND™ microswitch with a normally open terminal ("NO"), a normally closed terminal ("NC"), and a common terminal. For example, the lever 1504 is incorporated into a coin slot of the offline-payment operated machine 1500 and is depressed whenever a coin slides down the coin slot into a coin reservoir of the offline-payment operated machine 1500 (not shown). For example, when the lever 1504 is depressed and the microswitch 1502 is wired in the NO configuration as shown in Figure 28A, the switch is closed. Continuing with this example, when the switch is closed, control unit 1506 receives a pulse (i.e., a payment acceptance signal) from the common terminal of the microswitch 1502 indicating depression of the lever 1504 from the reception of a US quarter (i.e., $0.25) or coin of another value.

[00205] In some implementations, when the control unit 1506 receives a preset sequence of payment acceptance signals indicative of a preset number of coins being received by the microswitch 1502, the control unit 1506 initiates the operation of the offline-payment operated machine 1500. For example, after receiving the preset sequence of payment acceptance signals (e.g., three pulses indicating reception of three US quarters), the control unit 1506 initiates operation of the offline-payment operated machine 1500 by applying current to the gate of the transistor 1510 which allows current to flow from the power supply 1508 to operation unit 1512. For example, the operation unit 1512 is a motor of a dryer which begins spinning once current flows from the power supply 1508.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1400 of 1551

[00206] In Figure 28A, payment module 1520 (e.g., a form of the adapter module 100, Figures 5 and 20) is configured to be installed in the offline-payment operated machine 1500 so as to retrofit the offline-payment operated machine 1500 to be able to accept electronic payments. In some implementations, the payment module 1520 includes all or some of the components included adapter module 100 in Figure 20 such as processing unit 750, memory 760, a security unit 755, and a communications unit 770. In some implementations, the payment module 1520 also includes a first interface module 1522, a second interface module 1524, and a lead 1536 for drawing power from power supply 1508 of the offline-payment operated machine 1500.

[00207] In Figure 28A, the first interface module 1522 is configured to sample payment acceptance signals from the microswitch 1502 (e.g., a coin receiving switch) via lead 1532 of the offline-payment operated machine 1500. For example, the payment acceptance signals are indicative of a coin being received by the microswitch 1502 which depress lever 1504. In Figure 28A, the second interface module 1524 is configured to sample control signals from the control unit 1506 of the offline-payment operated machine 1500 via lead 1534 that initiate an operation of the offline-payment operated machine (e.g., the application of current to the gate of the transistor 1510) in response to receiving a preset sequence of payment acceptance signals from the microswitch 1502 (e.g., the coin receiving switch) indicative of the preset number of coins.

[00208] Figure 28B illustrates signals sampled by the payment module 1520 in accordance with some implementations. In Figure 28B, sample 1550 represents a preset sequence of payment acceptance signals sampled by the first interface module 1522 via lead 1532 that are sent from the microswitch 1502 to the control unit 1506. For example, the preset sequence of payment acceptance signals indicative of the preset number of coins include pulses (i.e., payment acceptance signals) 1552, 1554, 1556, and 1558. For example, the leading edges of pulses 1552, 1554, 1556, and 1558 at times 1582, 1584, 1586, and 1588 indicate reception of a coin by microswitch 1502 which causes the switch to close when wired in the NO configuration as shown in Figure 28A. In Figure 28B, sample 1570 represents a control signal sampled by the second interface module 1524 via lead 1534 that is sent from the control unit 1506 to transistor 1510. In Figure 28B, the sample 1570 includes a pulse 1572 that is sent from the control unit 1506 to transistor 1510 at time 1590 after receiving the preset sequence of payment acceptance signals from the microswitch 1502 (i.e., pulses 1552, 1554, 1556, and 1558).

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1401 of 1551

[00209] Figures 29A-29B illustrate a flowchart diagram of a method of retrofitting an offline-payment operated machine to accept electronic payments in accordance with some implementations. In some implementations, the method 1600 is performed by a payment module with one or more processors and memory. In some implementations, the payment module also includes a short-range communication capability corresponding to a short-range communication protocol (e.g., a non-persistent communication channel such as BLE, NFC, and/or the like), where the short-range communication capability is configured to communicate with one or more mobile devices, where each of the one or more mobile devices is configured with a complimentary short-range communication capability and a long-range communication capability corresponding to a long-range communication protocol (e.g., Wi-Fi, CDMA, GSM, and/or the like).

[00210] In some implementations, the payment module is coupled with an offline-payment operated machine (e.g., the payment accepting unit 120, Figures 5 and 19 (sometimes also herein called "machine 120"), or the offline-payment operated machine 1500, Figure 28A) such as dryer or washer in a laundromat, a parking meter, a car wash payment kiosk, or the like. In some implementations, the offline-payment operated machine includes a coin receiving switch (e.g., the microswitch 1502, Figure 28A) and a control unit (e.g., the control unit 1506, Figure 28A). In some implementations, the payment module further includes: (A) a first interface module (e.g., the first interface module 1522, Figure 28A) configured to sample payment acceptance signals from the coin receiving switch of the offline-payment operated machine, where the signals are indicative of a coin being received by the coin receiving switch; and (B) a second interface module (e.g., the second interface module 1524, Figure 28A) configured to sample control signals from the control unit of the offline-payment operated machine that initiate an operation of the offline-payment operated machine in response to receiving a preset sequence of payment acceptance signals from the coin receiving switch indicative of the preset number of coins. By sampling and storing these signals, the payment module 1520 is able to simulate operation of a respective coin receiving switch in response to receiving the correct/preset number of coins so as to trigger operation of the offline-payment operated machine in response to completion of an electronic payment.

[00211] For example, in some implementations, the method 1600 is performed by the adapter module 100 (Figures 5 and 20) or payment module 1520 (Figure 28A). In some

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1402 of 1551

implementations, the method 1600 is governed by instructions that are stored in a non-transitory computer readable storage medium (e.g., the memory 760, Figure 20) and the instructions are executed by one or more processors (e.g., the processing unit 750, Figure 20) of the payment module. Optional operations are indicated by dashed lines (e.g., boxes with dashed-line borders).

[00212] In some implementations, the payment module detects (1602), via the first interface module, a preset sequence of payment acceptance signals from the coin receiving switch that causes the control unit to initiate the operation of the offline-payment operated machine, where the preset sequence of payment acceptance signals are indicative of a preset number of coins received by the coin receiving switch. For example, with reference to Figures 28A-28B, the first interface module 1522 of the payment module 1520 samples payment acceptance signals via lead 1532 from the microswitch 1502 to the control unit 1506. For example, each of the payment acceptance signals is indicative of reception of a coin by the microswitch 1502. Continuing with this example, the second interface module 1524 of the payment module 1520 samples control signals via lead 1534 from the control unit 1506 to the transistor 1510. The payment module 1520 detects a preset sequence of payment acceptance signals from the microswitch 1502 that causes the control unit 1506 to apply a current to the gate of the transistor 1510 (e.g., the control signals). For example, the preset sequence of payment acceptance signals is indicative of a preset number of coins received by the microswitch 1502 to cause operation of the offline-payment operated machine 1500. For example, the application of current to the gate of the transistor 1510 allows current to flow from the power supply 1508 to the operation unit 1512 so that the operation. For example, the operation unit 1512 is a motor of a dryer which begins spinning once current flows from the power supply 1508.

[00213] In some implementations, the payment module determines (1604) the predefined signal sequence to emulate the preset sequence of payment acceptance signals from the coin receiving switch. In some implementations, after detecting the preset sequence of payment acceptance signals that causes the control unit 1506 to initiate the operation of the offline-payment operated machine 1500, the payment module 1520 determines a predefined signal sequence to emulate the preset sequence of payment acceptance signals. In some implementations, the money value associated with each pulse in the preset sequence of payment acceptance signals from the microswitch 1502, indicative of the preset number of coins to initiate the operation of the offline-payment operated machine 1500, is a default currency (e.g., USD)

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1403 of 1551

and amount (e.g., $0.25) set in the firmware of the payment module 1520. In some implementations, the money value associated with the each pulse in the preset sequence of payment acceptance signals from the microswitch 1502, indicative of the preset number of coins to initiate the operation of the offline-payment operated machine 1500, is set by the server 130 and can be changed remotely by using the mobile device 150 as a communications bridge to send information indicating the value of a pulse from the server 130 to the mobile device 150 via the second communication capability (e.g., GSM, CDMA, or Wi-Fi) and forwarding the information from the mobile device to the payment module 1520 via the first communication capability (e.g., BLE). For instance, in most cases, each pulse is US $0.25.

[00214] In some implementations, determining the predefined signal sequence includes (1606) at least one of: identifying a count of pulses in the present sequence of payment acceptance signals; identifying amplitude of pulses in the present sequence of payment acceptance signals; identifying shape of pulses in the present sequence of payment acceptance signals; and identifying an interval between pulses. In some implementations, after detecting the preset sequence of payment acceptance signals (e.g., the sample 1550, Figure 28B), the payment module 1520 determines a predefined signal sequence to emulate the preset sequence of payment acceptance signals by identifying a count of pulses in the preset sequence of payment acceptance signals, an interval between pulses in the preset sequence of payment acceptance signals, the shape of pulses in the preset sequence of payment acceptance signals, and an amplitude of pulses in the preset sequence of payment acceptance signals.

[00215] The payment module receives (1608) a request via the short-range communication capability from a respective mobile device to perform an operation of the offline-payment operated machine. For example, with reference to Figure 8C, the payment module 1520 (Figure 28A) receives the AuthGrant from the mobile device 150 via the short-range communication capability (e.g., BLE) indicating that the user of the mobile device 150 wishes to perform the operation of the offline-payment operated machine 1500 (Figure 28A). For example with reference to operation 1012 in Figure 23, the payment module 1520 (Figure 28A) receives an authorization grant token from the mobile device 150 via the short-range communication capability (e.g., BLE) indicating that the user of the mobile device 150 wishes to perform the operation of the offline-payment operated machine 1500 (Figure 28A).

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1404 of 1551

[00216] The payment module validates (1610) the request. Validation of the request indicates (1612) that the respective mobile device is authorized to initiate payment for the operation by a remote server via the long-range communication capability. In some implementations, the payment module 1520 validates the request from the mobile device 150 by determining whether the AuthGrant or the authorization grant token includes a valid authorization code.

[00217] In accordance with a determination that the request is valid, the payment module causes (1614) the payment operated machine to perform the operation by issuing a predefined signal sequence to the control unit, where the predefined signal sequence emulates a signal sequence that would be issued by the coin receiving switch in response to receiving a preset number of coins. For example, with reference to Figure 28B, the payment module 1520 issues a predefined signal sequence with first interface module 1522 to the control unit 1506 that emulates sample 1550 in Figure 28B. Continuing with this example, in response to receiving the predefined signal sequence from the payment module 1520 control unit 1506 causes initiation of the operation of the offline-payment operated machine 1500 by applying current to the gate of the transistor 1510 which allows current to flow from the power supply 1508 to operation unit 1512. In some implementations, the control unit 1506 causes initiation of the operation by setting a timer to an amount of time corresponding to the preset number of coins whereby current flows to the gate of the transistor 1510 for the set amount of time. For example, the preset number of coins is a number of a coins required to run the offline-payment operated machine 1500 by for a default amount of time and subsequent coins may be added to extend the amount of time that the offline-payment operated machine 1500 by will run. In some implementations, the preset number of coins is a number of a coins required to cause the offline-payment operated machine 1500 to dispense a purchased item, such as laundry detergent.

[00218] Alternatively, in some implementations, in accordance with a determination that the request is valid, the offline-payment operated machine 1500 displays credit to the user (e.g., via one of the displays 122 or 124 shown in Figure 19) and the user interacts with the input mechanisms of the offline-payment operated machine 1500 120 (e.g., via the buttons 126 or a touch screen display 124 shown in Figure 19) to perform the operation of the machine. For example, if the offline-payment operated machine 1500 is a dryer, the user of the mobile device 150 selects the appropriate spin cycle via input mechanisms of the dryer, and when the user of

Draft Only

the mobile device 150 selects a start/run input mechanism of the dryer, control unit 1506 of the dryer causes initiation of the operation of the dryer (e.g., starting a motor that corresponds to operation unit 1512 in Figure 28A).

[00219] In some implementations, prior to sending the operation information and after causing the offline-payment operated machine to perform the operation by issuing the predefined signal sequence to the control unit, the payment module obtains (1616) a notification from the offline-payment operated machine indicating initiation of the operation of the offline-payment operated machine and the preset number of coins. For example, after issuing the preset signal sequence to control unit 1506, the payment module 1520 (Figure 28A) obtains a notification indicating that the control unit 1506 sent control signals to initiate operation of the offline-payment operated machine 1500 in response to receiving the predefined signal sequence. For example, the notification is obtained by the second interface module 1524 (e.g., the sample 1570, Figure 28B) sampling controls signals sent by control unit 1506 (e.g., application of current to the gate of the transistor 1510 which allows current to flow from the power supply 1508 to operation unit 1512).

[00220] In response to receiving the notification, the payment module (1618): generates the operation information based at least in part on the notification; and stores the generated operation information in the memory. For example, after obtaining the notification, the payment module 1520 (Figure 28A) generates operation information corresponding to performance of the operation and the preset number of coins associated with the predefined signal sequence (e.g., the amount required to initiate operation of the offline-payment operated machine 1500) and stores the operation information in memory local to the payment module 1520 (e.g., the memory 760, Figure 20).

[00221] In some implementations, the payment module sends (1620) operation information corresponding to the operation to the respective mobile device via the short-range communication capability. For example, after operation 1618, the payment module 1520 (Figure 28A) sends the operation information to the mobile device 150 via the first communication capability of the mobile device 150 such as a radio/transceiver means for communicating via one or more short-range communication protocols such as BLE, NFC, and/or the like (i.e., a non-persistent communication channel)

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1406 of 1551

[00222] It should be understood that the particular order in which the operations in Figures 29A-29B have been described is merely for example purposes and is not intended to indicate that the described order is the only order in which the operations could be performed. One of ordinary skill in the art would recognize various ways to reorder the operations described herein. Additionally, it should be noted that details of other processes described herein with respect to other methods described herein (e.g., the method 1700 in Figure 30) are also applicable in an analogous manner to the method 1600 described above with respect to Figures 29A-29B.

[00223] Figure 30 illustrates a flowchart diagram of a method 1700 of enabling a payment operated machine to accept electronic payments in accordance with some implementations. In some implementations, the method 1700 is performed by an offline-payment operated machine (e.g., the payment accepting unit 120, Figures 5 and 19 (sometimes also herein called "machine 120"), or the offline-payment operated machine 1500, Figure 28A) such as dryer or washer in a laundromat, a parking meter, a car wash payment kiosk, or the like.

[00224] In some implementations, the offline-payment operated machine includes a control unit (e.g., the control unit 1506, Figure 28A), memory, and a coin receiving switch (e.g., the microswitch 1502, Figure 28A). In some implementations, the offline-payment operated machine also includes a short-range communication capability corresponding to a short-range communication protocol (e.g., a non-persistent communication channel such as BLE, NFC, and/or the like), where the short-range communication capability is configured to communicate with one or more mobile devices, where each of the one or more mobile devices is configured with a complimentary short-range communication capability and a long-range communication capability corresponding to a long-range communication protocol (e.g., Wi-Fi, CDMA, GSM, and/or the like). For example, in some implementations, the method 1700 is performed by the machine 120, (Figures 5 and 19). In some implementations, the method 1700 is governed by instructions that are stored in a non-transitory computer readable storage medium and the instructions are executed by the control unit of the offline-payment operated machine.

[00225] The offline-payment operated machine receives (1702) a request via a short-range communication capability from a respective mobile device to perform an operation of the offline-payment operated machine. For example, with reference to Figure 8C, the payment module 1520 (Figure 28A) receives the AuthGrant from the mobile device 150 via the short-

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1407 of 1551

range communication capability (e.g., BLE) indicating that the user of the mobile device 150 wishes to perform the operation of the offline-payment operated machine 1500 (Figure 28A). For example with reference to operation 1012 in Figure 23, the payment module 1520 (Figure 28A) receives an authorization grant token from the mobile device 150 via the short-range communication capability (e.g., BLE) indicating that the user of the mobile device 150 wishes to perform the operation of the offline-payment operated machine 1500 (Figure 28A).

[00226] The offline-payment operated machine validates (1704) the request. Validation of the request indicates (1706) that the respective mobile device is authorized to initiate payment for the operation by a remote server via the long-range communication capability. In some implementations, the payment module 1520 validates the request from the mobile device 150 by determining whether the AuthGrant or the authorization grant token includes a valid authorization code.

[00227] In accordance with a determination that the request is valid, the offline-payment operated machine performs (1708) the operation by issuing a predefined signal sequence to the control unit, where the predefined signal sequence emulates a preset number of coins received by the coin receiving switch. For example, in accordance with a determination that the request is valid, the offline-payment operated machine or a component thereof issues a predefined signal sequence to the control unit 1506 that emulates sample 1550 in Figure 28B. Continuing with this example, in response to receiving the predefined signal sequence from the payment module 1520, control unit 1506 causes initiation of the operation of the offline-payment operated machine 1500 by applying current to the gate of the transistor 1510 which allows current to flow from the power supply 1508 to operation unit 1512. In another example, in accordance with a determination that the request is valid, the control unit 1506 causes initiation of the operation of the offline-payment operated machine 1500 by applying current to the gate of the transistor 1510 which allows current to flow from the power supply 1508 to operation unit 1512.

[00228] It should be understood that the particular order in which the operations in Figure 30 have been described is merely for example purposes and is not intended to indicate that the described order is the only order in which the operations could be performed. One of ordinary skill in the art would recognize various ways to reorder the operations described herein. Additionally, it should be noted that details of other processes described herein with respect to

Draft Only

other methods described herein (e.g., the method 1600 in Figures 29A-29B) are also applicable in an analogous manner to the method 1700 described above with respect to Figure 30.

MISCELLANEOUS

[00229] It should be noted that relative terms are meant to help in the understanding of the technology and are not meant to limit the scope of the invention. Similarly, unless specifically stated otherwise, the terms used for labels (e.g., "first," "second," and "third") are meant solely for purposes of designation and not for order or limitation. The term "short" in the phrase "short-range" (in addition to having technology specific meanings) is relative to the term "long" in the phrase "long-range."

[00230] The terms "may," "might," "can," and "could" are used to indicate alternatives and optional features and only should be construed as a limitation if specifically included in the claims.

[00231] It should be noted that, unless otherwise specified, the term "or" is used in its nonexclusive form (e.g., "A or B" includes A, B, A and B, or any combination thereof, but it would not have to include all of these possibilities). It should be noted that, unless otherwise specified, "and/or" is used similarly (e.g., "A and/or B" includes A, B, A and B, or any combination thereof, but it would not have to include all of these possibilities). It should be noted that, unless otherwise specified, the terms "includes" and "has" mean "comprises" (e.g., a device that includes, has, or comprises A and B contains A and B, but optionally may contain C or additional components other than A and B). It should be noted that, unless otherwise specified, the singular forms "a," "an," and "the" refer to one or more than one, unless the context clearly dictates otherwise.

[00232] It is to be understood that the inventions, examples, and implementations described herein are not limited to particularly exemplified materials, methods, and/or structures. It is to be understood that the inventions, examples, and implementations described herein are to be considered preferred inventions, examples, and implementations whether specifically identified as such or not.

[00233] The terms and expressions that have been employed in the foregoing specification are used as terms of description and not of limitation, and are not intended to exclude equivalents

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1409 of 1551

of the features shown and described. While the above is a complete description of selected implementations of the present invention, it is possible to practice the invention using various alternatives, modifications, adaptations, variations, and/or combinations and their equivalents. It will be appreciated by those of ordinary skill in the art that any arrangement that is calculated to achieve the same purpose may be substituted for the specific embodiment shown. It is also to be understood that the following claims are intended to cover all of the generic and specific features of the invention herein described and all statements of the scope of the invention that, as a matter of language, might be said to fall therebetween.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1410 of 1551

Electronically filed via EFS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Paresh K. Patel	Confirmation No.:	To be assigned
Serial No.:	To be assigned	Art Unit	To be assigned
Filed:	March 14, 2022	Examiner:	To be assigned
Title:	*METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS*	Attorney Docket No.:	104402-5065-US

STATEMENT UNDER 37 C.F.R. § 3.73(c)

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

Sir:

PAYRANGE INC., a Corporation, states that it is the assignee of the entire right, title and interest in the patent application identified above by virtue of an assignment from the inventors of the parent of the patent application identified above.

The assignment was recorded in the United States Patent and Trademark Office on November 21, 2014 at Reel 034236, Frame 0376, or for which a copy thereof is attached.

The undersigned is authorized to act on behalf of the assignee.

Date: March 14, 2022

/Benjamin Pezzner/ 70711
Benjamin Pezzner (Reg. No.)

MORGAN, LEWIS & BOCKIUS LLP
1400 Page Mill Road
Palo Alto, CA 94304
(650) 843-4000

Draft Only

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE UNITED STATES PATENT AND TRADEMARK OFFICE

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

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint the practitioners of Morgan, Lewis & Bockius LLP, Customer Number **24341** as attorneys or agents to represent the undersigned and to transact all business before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications and patents assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 C.F.R. § 3.73(c), said appointment to be to the exclusion of the inventor(s) and their attorney(s) in accordance with the provisions of 37 C.F.R. § 3.71, provided that, if any one of these attorneys ceases being affiliated with the law firm of Morgan, Lewis & Bockius LLP as partner, counsel, or employee, then the appointment of that attorney and all powers derived therefrom shall terminate on the date such attorney ceases being so affiliated.

Assignee Name and Address: PAYRANGE INC.
9600 NE Cascades Pkwy, Suite 280
Portland, OR 97220

Draft Only

SIGNATURE of Assignee of Record

The undersigned whose signature and title is supplied below is authorized to act on behalf of the assignee.

Signature			
Name	Paresh K. Patel, Ph.D., MBA	Date	February 9, 2018
Title	CEO, PayRange Inc.	Telephone	(855) 856-6398

A copy of this form, together with a statement under 37 C.F.R. § 3.73(c) (Form PTO/SB96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 C.F.R. § 3.73(c) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee and must identify the application in which this Power of Attorney is to be filed.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	**METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS**

As the below named inventor, I hereby declare that:

This declaration is directed to:

- ☐ The attached application, or
- ☒ United States application or PCT international application number 14/458,199 filed on August 12, 2014

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby state that I have reviewed and understand the contents of the above identified application, including the claims.

I acknowledge the duty to disclose information known to me to be material to patentability as defined by 37 CFR 1.56.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

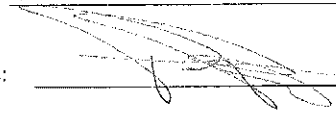
WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

Draft Only

LEGAL NAME OF INVENTOR

Inventor: **Dr. Paresh K. Patel** Date: 10/16/2014

Signature: 

UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/654,732	**03/14/2022 05:29:01 PM ET**	**104402-5065-US**

Title of Invention

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	5715	FILED BY	Benjamin Pezzner
PATENT CENTER #	60571795	FILING DATE	-
CUSTOMER #	24341	FIRST NAMED INVENTOR	Dr. Paresh K. Patel
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 5

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
generatedADS60571795.pdf	6	Application Data Sheet	156 KB
104402-5065-US Specification-APP.TEXT.DOCX	74	Application body structured text document	68 KB
104402-5065-US Drawings.pdf	45	Drawings-only black and white line drawings	5640 KB
104402-5065-US Declaration.pdf	1	Oath or Declaration filed	62 KB
104402-5065-US Track One.pdf	1	Track One Request	112 KB

Draft Only

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
generatedADS60571795.pdf	B183DDA9BED6A12778C5510531C12A27F6BB58136CEF70D139BF8123C53F4D33A0110DC1BBFDB8260B26A01A723135B7E7FA8CB1FBD8A2B2FF7F183C4CE30731
104402-5065-US Specification-APP.TEXT.DOCX	395190EDDD6541CA552270417EEE3C35F8CB4FF7605092A9F637019AC6A993574C1873ADF315B0C96CB8AD9125C2823A5A1DA85EB3824BCC158345AA62E9A33E
104402-5065-US Drawings.pdf	A624F9CAF1E055DE1F0E401B6A38F475E89EC651B42BDA621172D2499A8633E189E2EC1BB816B9F8428FD2F7251D66BB1899F2CA4147853D4A41907BC97C33CA
104402-5065-US Declaration.pdf	978D07FEF3C828E76EB5300C7C3562FE7146194B4C69E730E182D33C494E8E9ADFF99EC0BC4D349D9DD20A3646796981CFB444E92627B1C85045668F9A9BD6EE
104402-5065-US Track One.pdf	BA42EE936AB5D3D6BF39DFDFA34A69FB784C69DB7B8DD52018E33B63B0FF24F2FF460D95DBE873078B221FE2932A86230C82C5A03F8EDB24BD330FA04C4E1543

Draft Only

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/654,732	**03/14/2022 05:51:21 PM ET**	**104402-5065-US**

Title of Invention

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	5715	FILED BY	Benjamin Pezzner
PATENT CENTER #	60572224	FILING DATE	-
CUSTOMER #	24341	FIRST NAMED INVENTOR	Paresh K. Patel
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
104402-5065-US 373c.pdf	1	Assignee showing of ownership per 37 CFR 3.73	109 KB
104402-5065-US POA.pdf	1	Power of Attorney	41 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
104402-5065-US 373c.pdf	C6A7E89B36F94FD945D610B1C8E1511BFA459450CE07AADA 7A7ADEB532E694E1C73A743DF203EA751C8835E1C61E5A571 9D7A7A8CB978A5278C840135A4EDA44

Draft Only

104402-5065-US POA.pdf

8930191AF0A85473DA115B0CB04535A15CB813495ADF9D9CA
296186550F3C5FDE1CAB38CD85C9A66BCB9957FDE0B877081
ACB841DA7614DB8E4E3C438EEDA77C

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

Draft Only

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/654,732	03/14/2022 05:29:01 PM ET	104402-5065-US

Title of Invention

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	5715	FILED BY	Benjamin Pezzner
PATENT CENTER #	60571795	AUTHORIZED BY	-
CUSTOMER #	24341	FILING DATE	-
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Dr. Paresh K. Patel

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 8177	E202230H29470338	Benjamin Pezzner

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
2830	PROCESSING FEE, EXCEPT IN PROVISIONAL APPLICATIONS	70.00	1	70.00
2817	REQUEST FOR PRIORITIZED EXAMINATION	2100.00	1	2100.00
2111	UTILITY PATENT APPL. SEARCH FEE	350.00	1	350.00
4011	BASIC FILING FEE- UTILITY	80.00	1	80.00
2311	EXAMINATION OF ORIGINAL PATENT APPLICATION	400.00	1	400.00

Draft Only

TOTAL AMOUNT:	**$3,000.00**

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

Draft Only

Figure 1

Figure 2

Draft Only

Tab	Favorite?	Alert	View to User
All	Yes	No	User can make Hands-free Credit with the connected vending machine
All	No	Yes	User needs to launch Mobile Device and then swipe to make transaction manually
Favorite	Yes	No	Hands-free transction will be available to the user via vending machine
Favorite	No	No	User is not alerted for the vending machine which is not a favorite machine. Hands-free mode will not work, manual swipe for transaction required by user.
Either All or Favorite	Yes	Yes	BUT Hands-free Credit is not available (disabled by module, expired AuthGrant, insufficient balance, or other issue), then user will get an alert so that user can swipe credit manually.

Figure 3

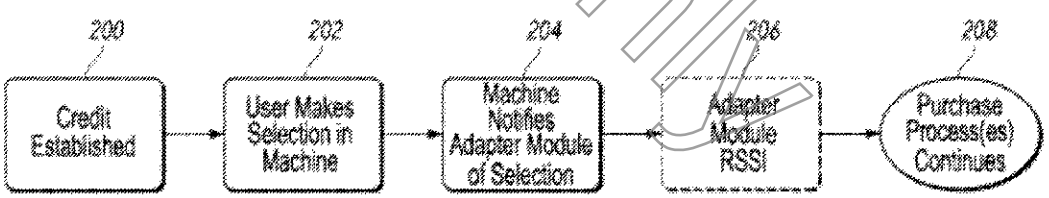


Figure 4

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1421 of 1551

Figure 5

Draft Only

Figure 6

Draft Only

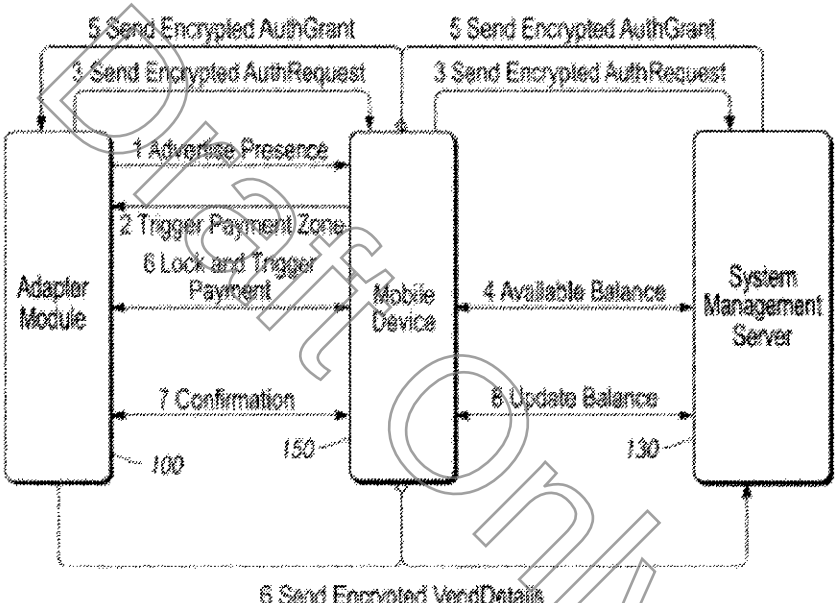


Figure 7

Patent Only

CSC ServiceWorks - Ex. 1002
Page 1424 of 1551

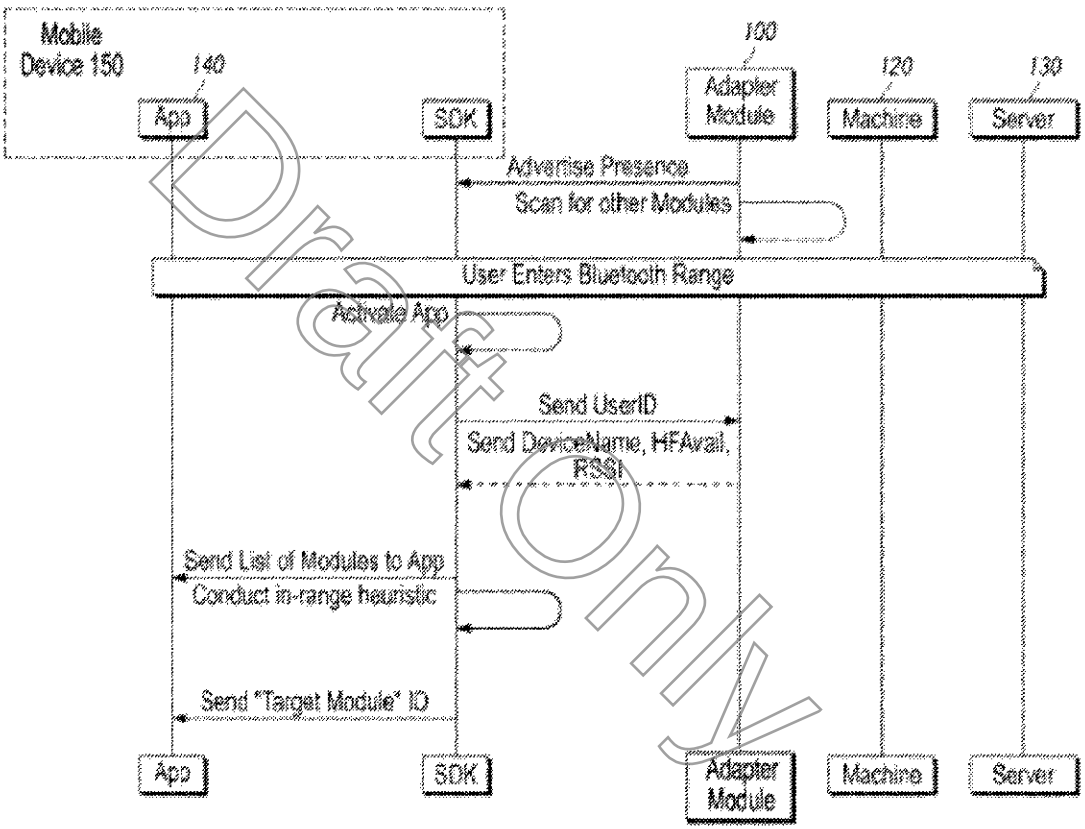


Figure 8A

Draft Only

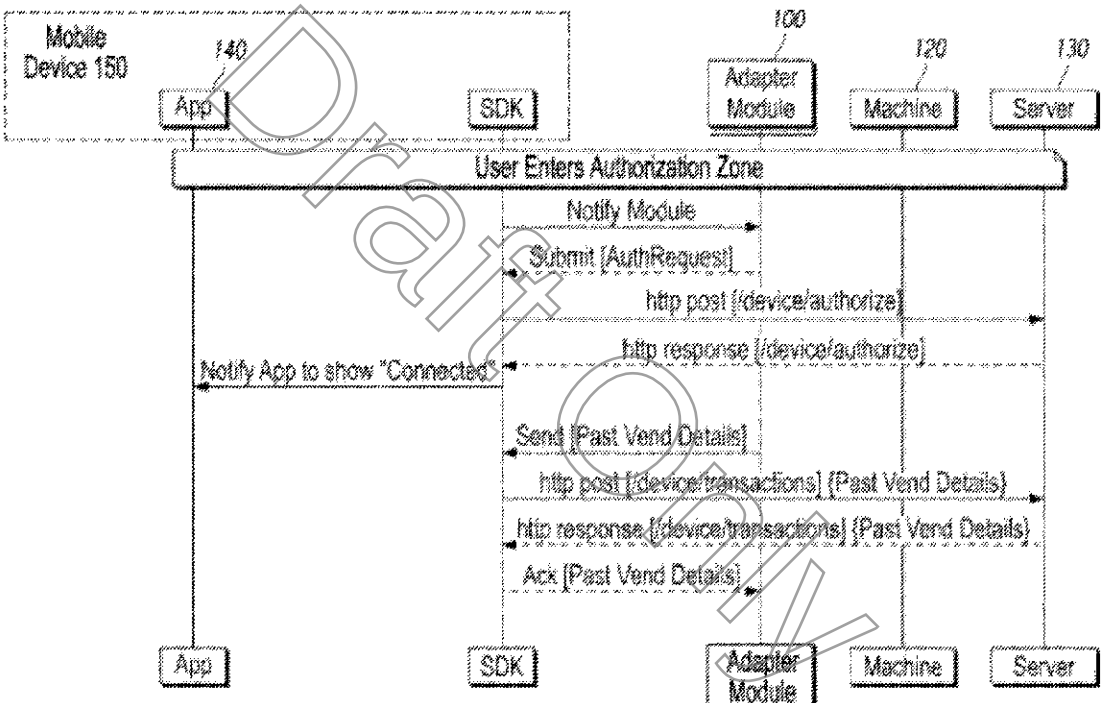


Figure 8B

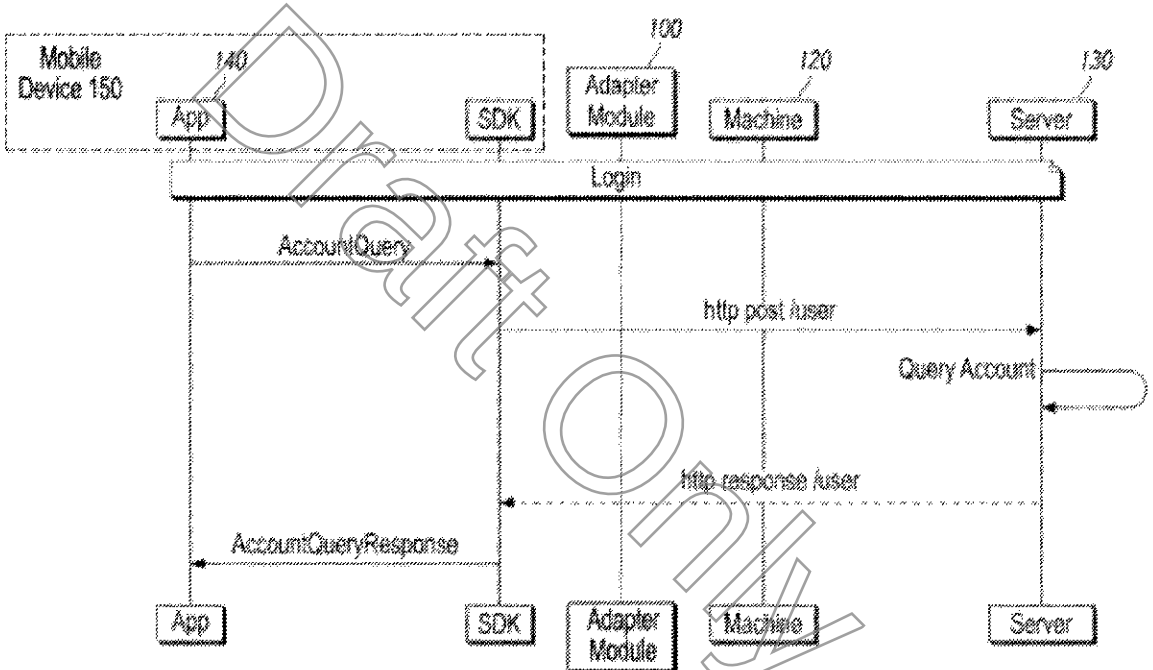
Draft Only

Figure 8C

Draft Only

Figure 8D

Draft Only



Draft Only

Figure 8E

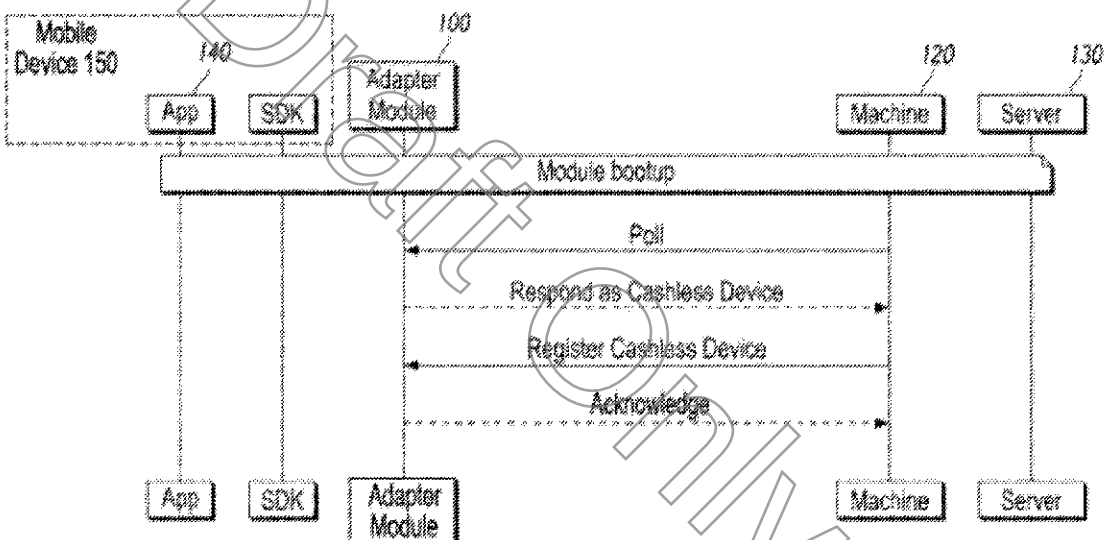
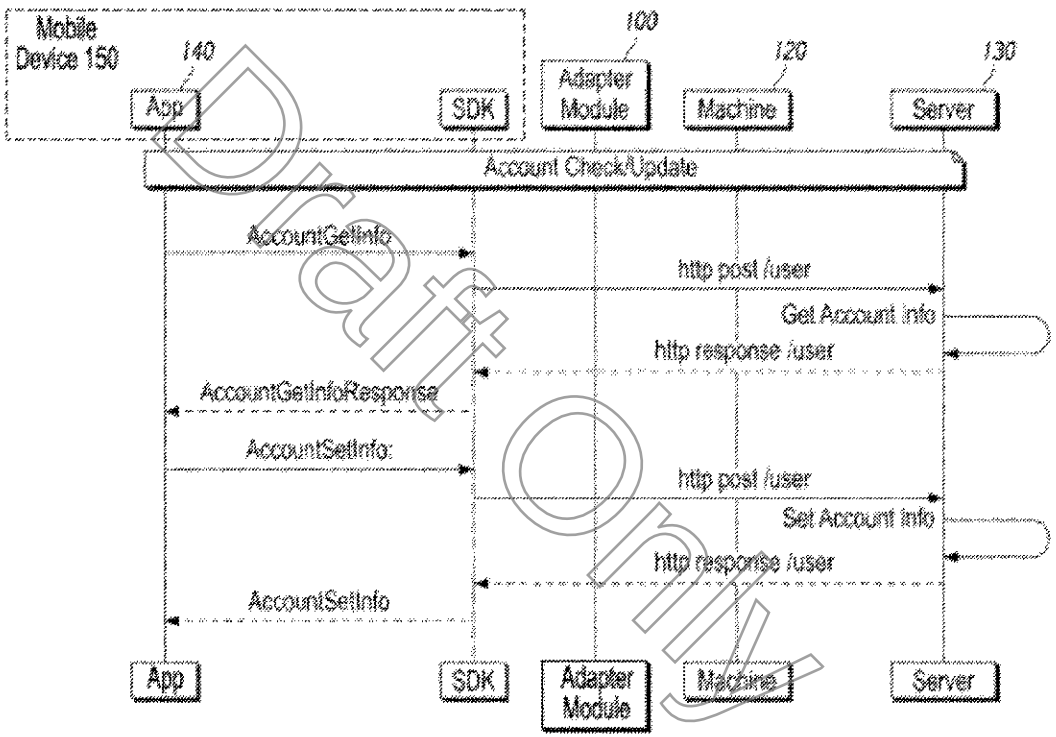


Figure 8F

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1430 of 1551



Draft Only

Figure 8G

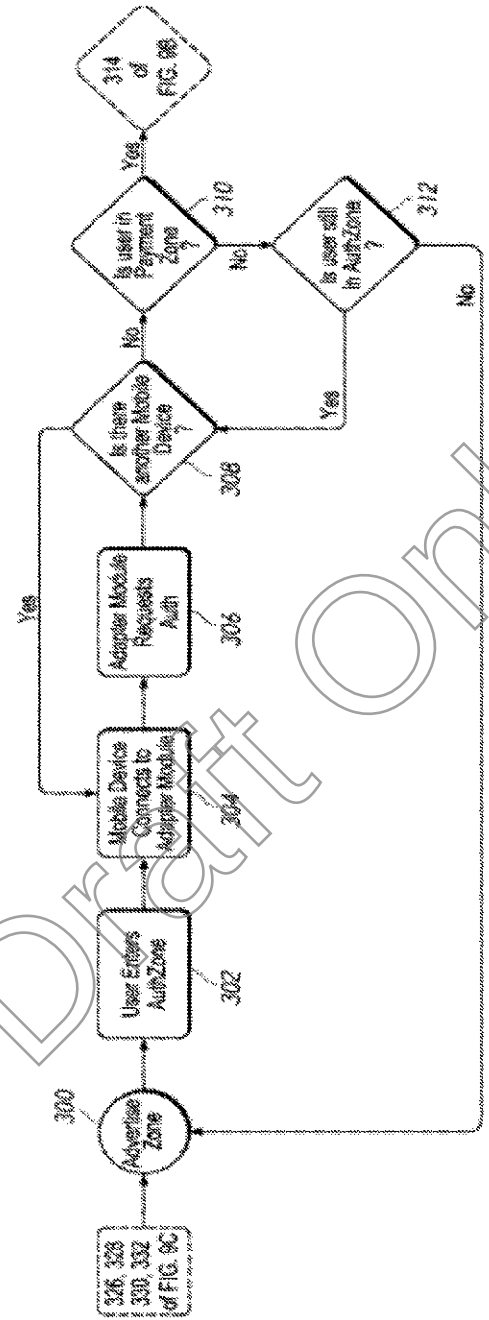


Figure 9A

Draft Only

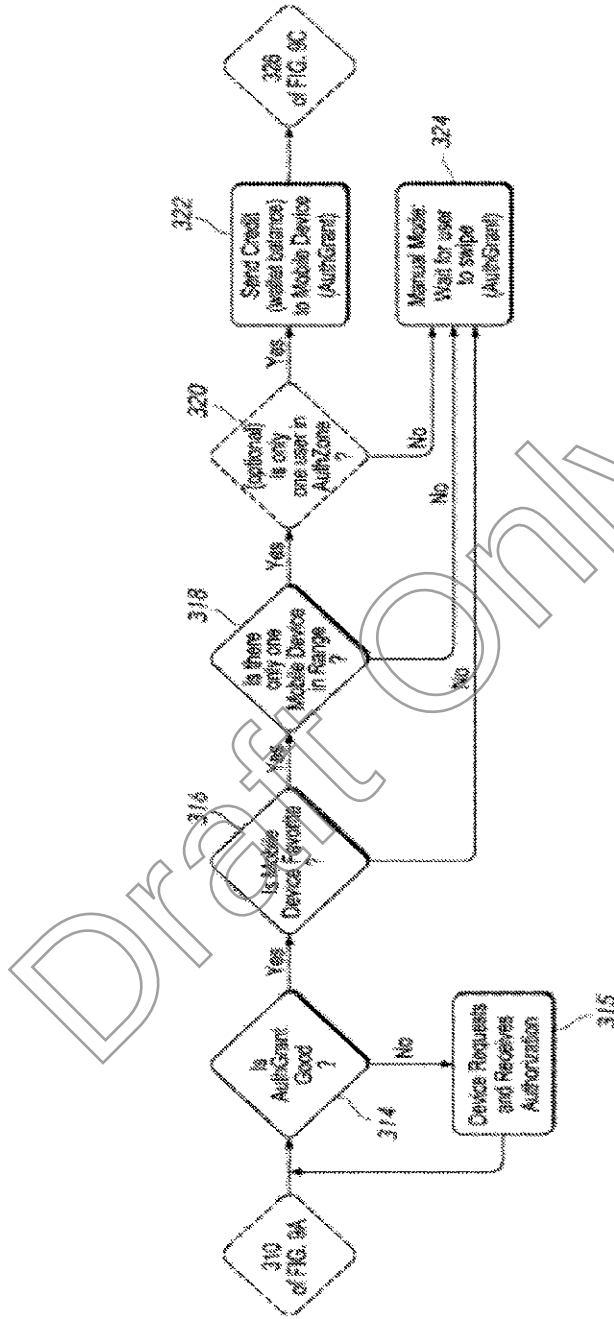
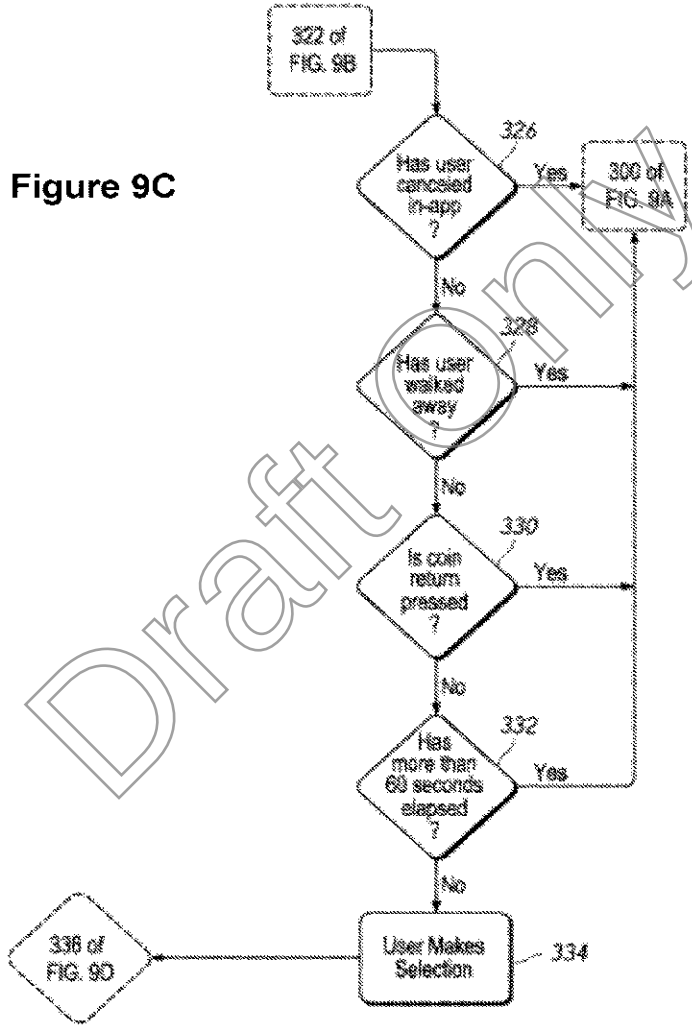


Figure 9B

Draft Only

Figure 9C



Draft Only

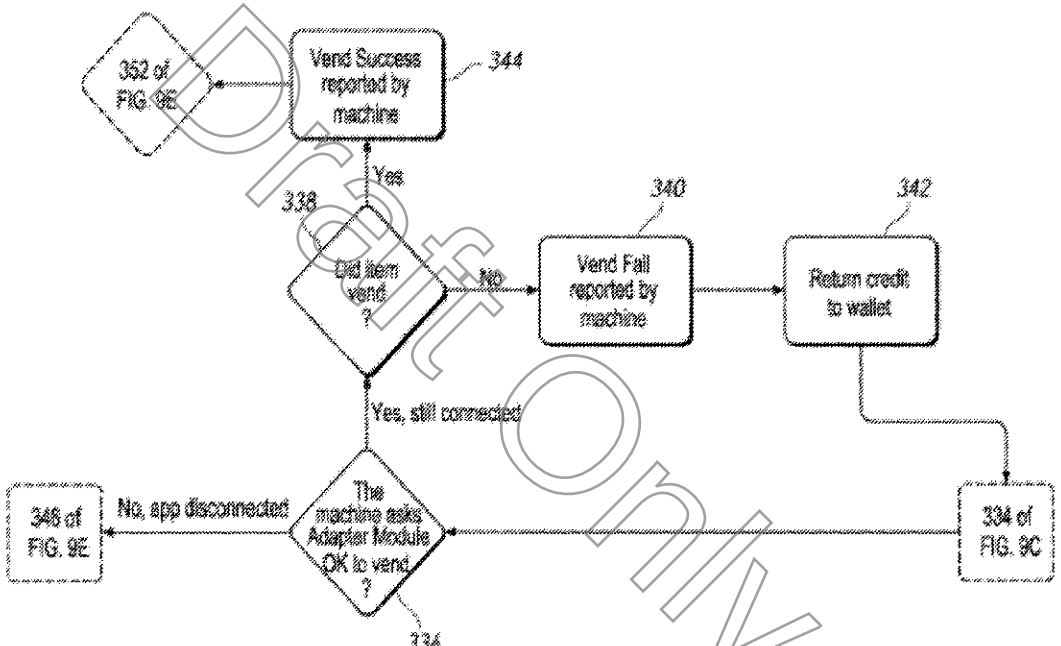


Figure 9D

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1435 of 1551

Figure 9E

Draft Only

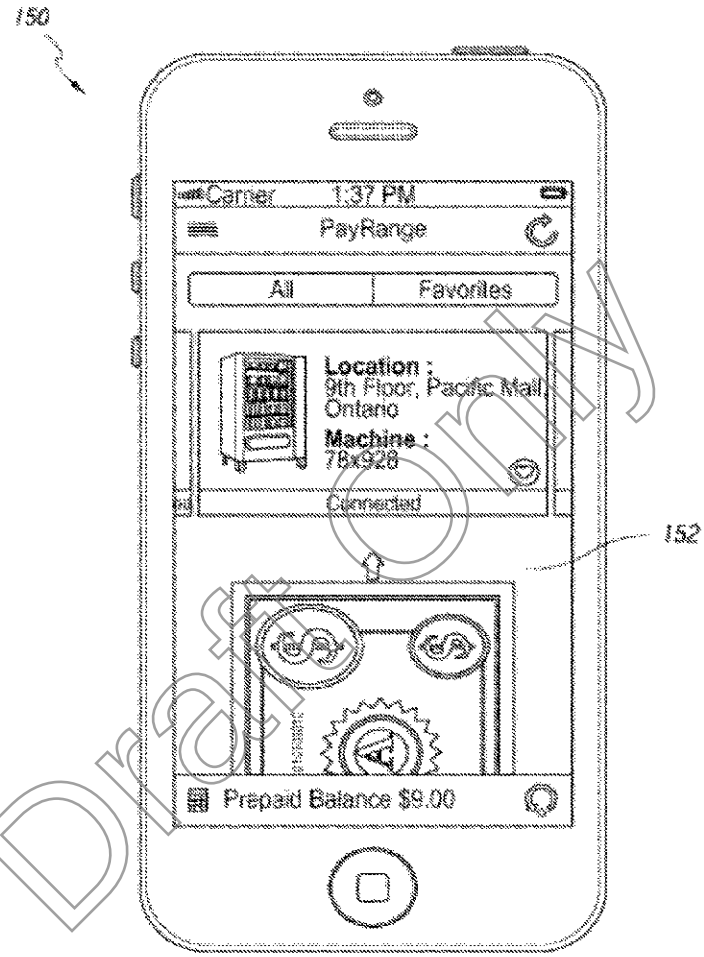


Figure 10A

Draft Only

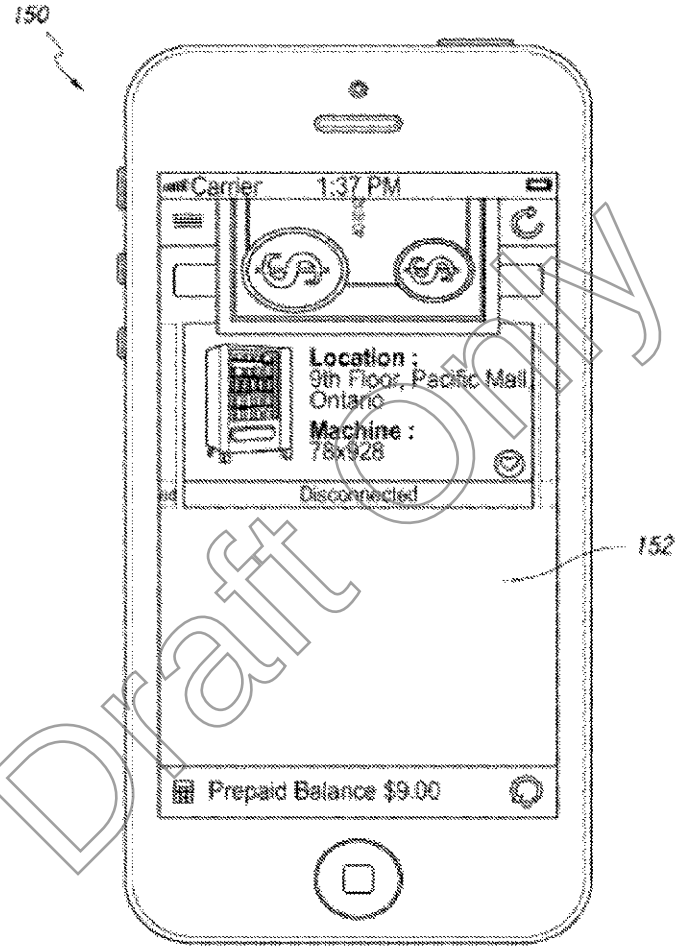


Figure 10B

Draft Only

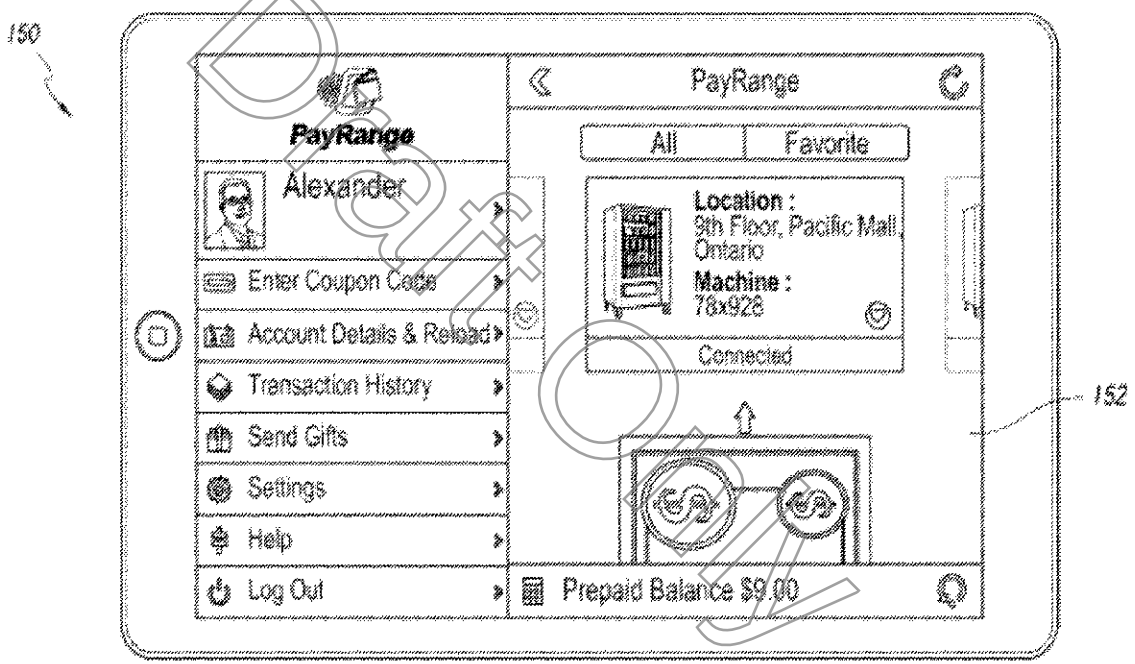


Figure 10C

Draft Copy

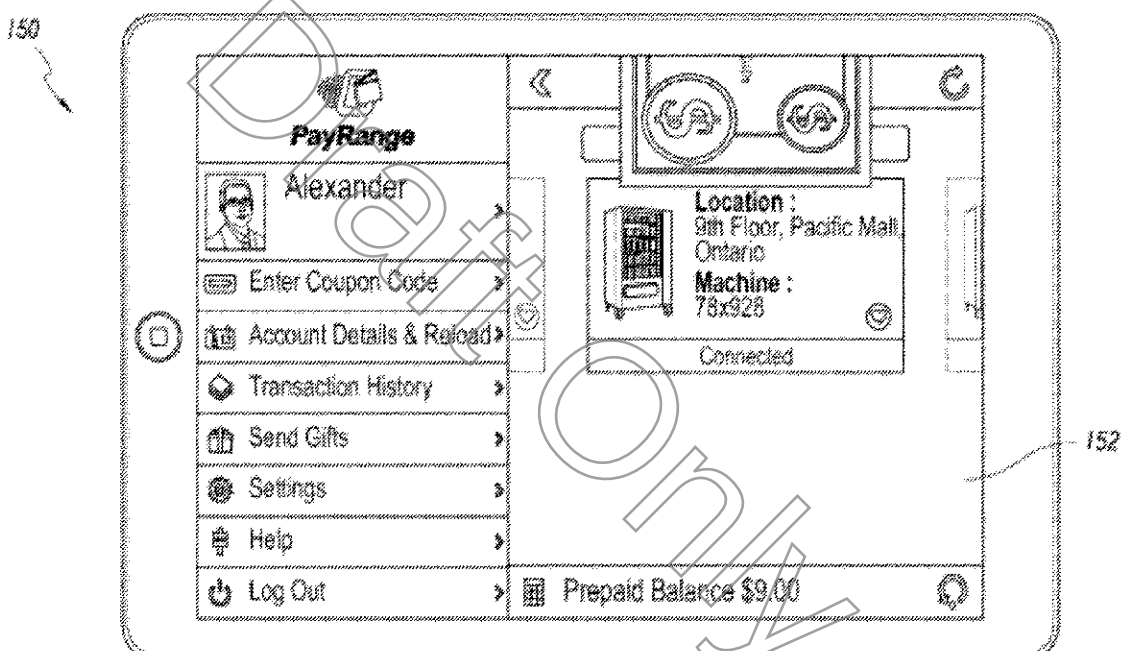


Figure 10D

Draft Only

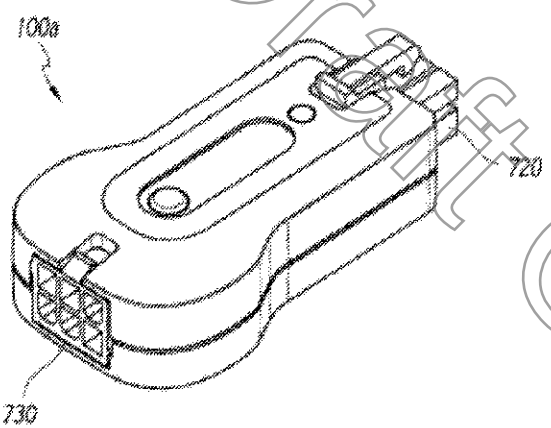


Figure 11

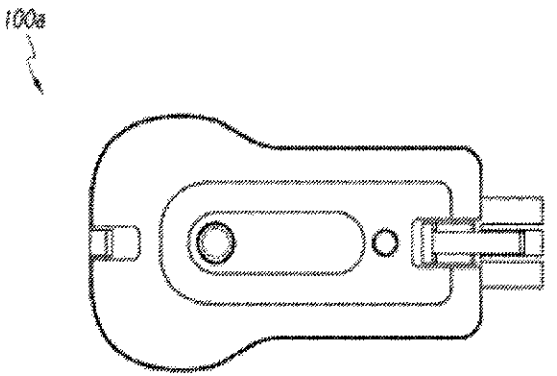


Figure 12

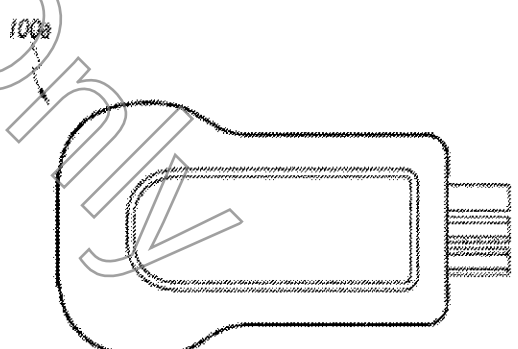


Figure 13

Draft Only

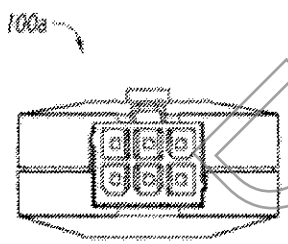


Figure 15

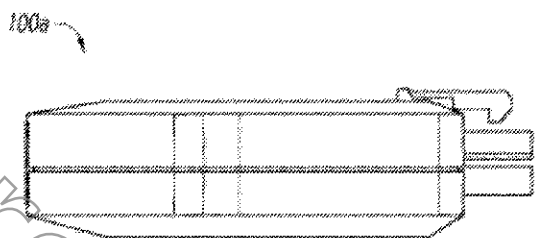


Figure 14

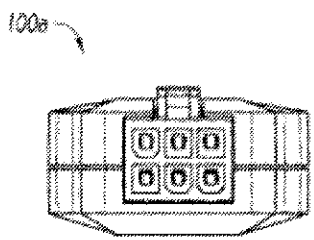


Figure 16

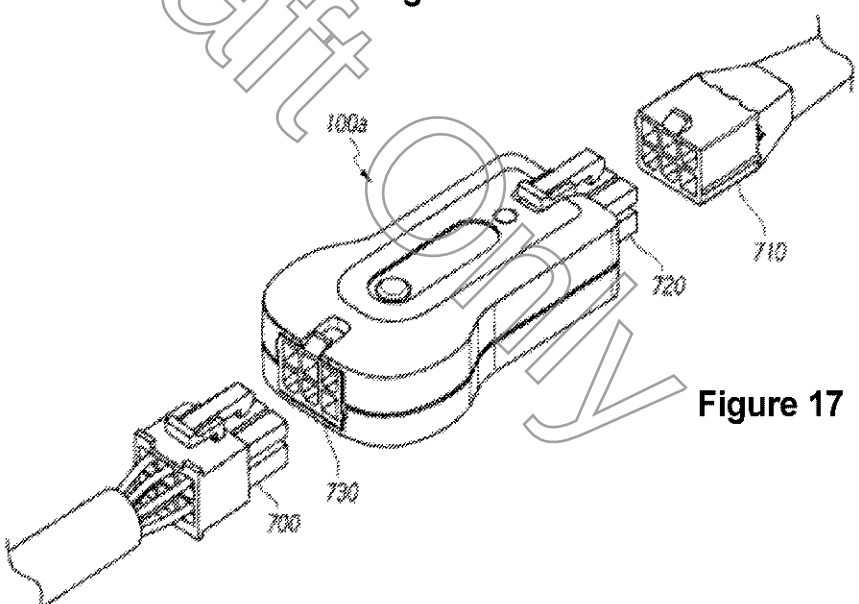


Figure 17

Draft Only

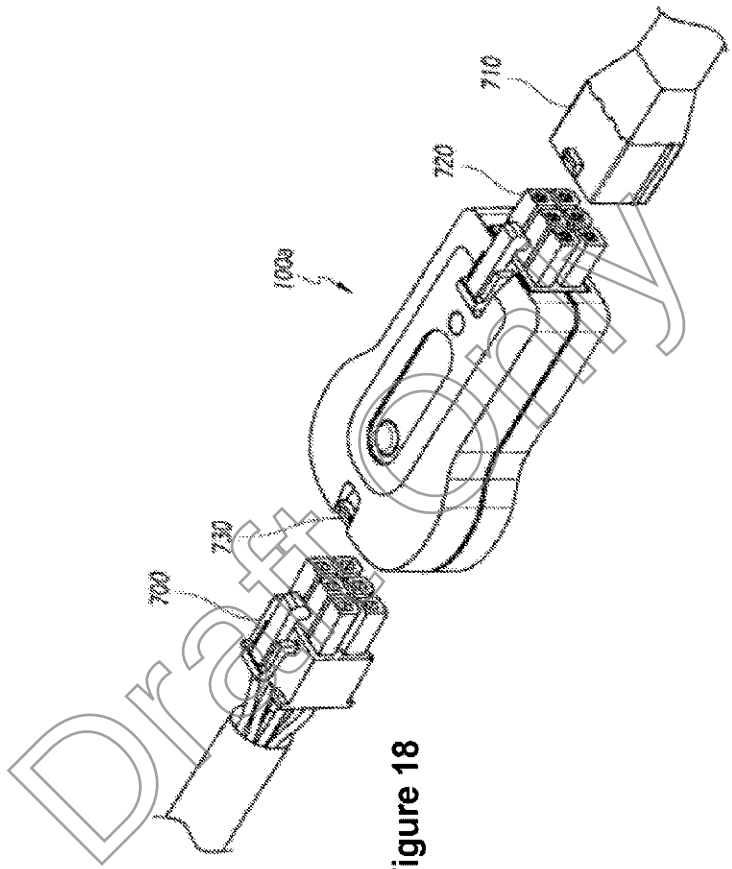


Figure 18

Draft Only

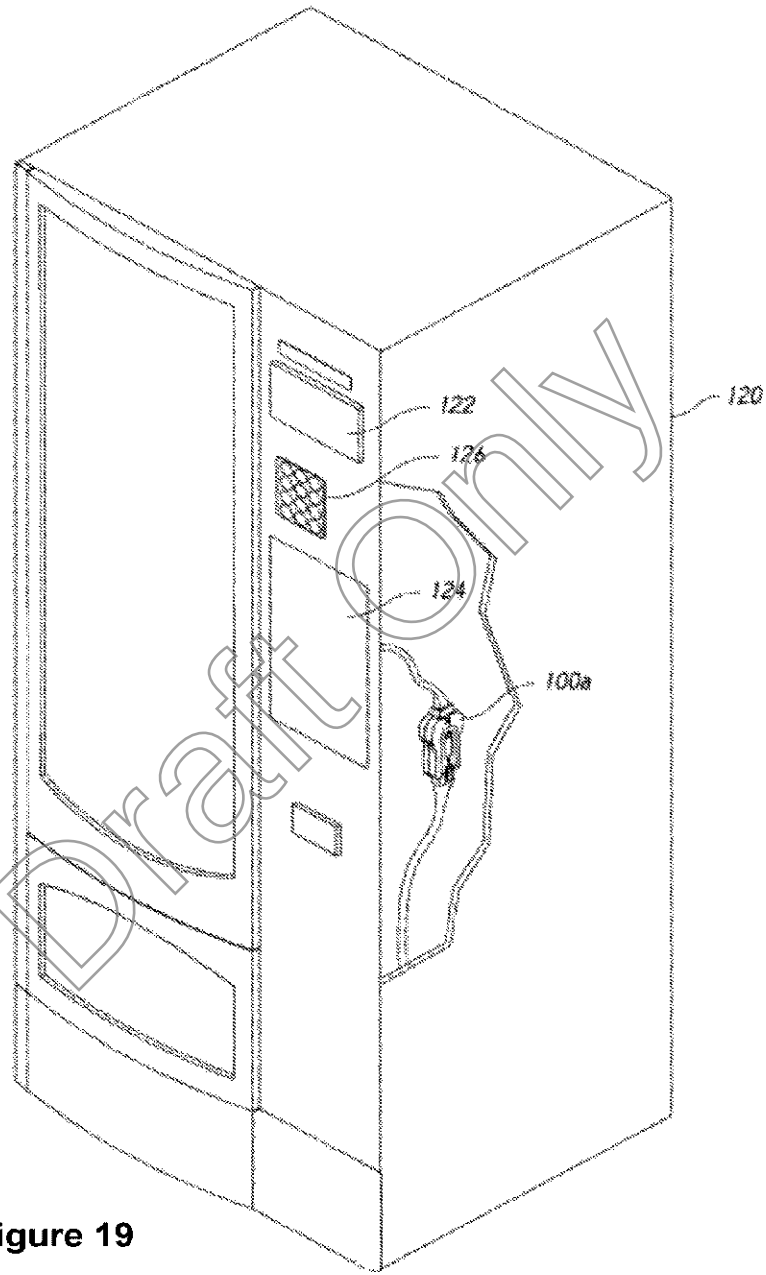
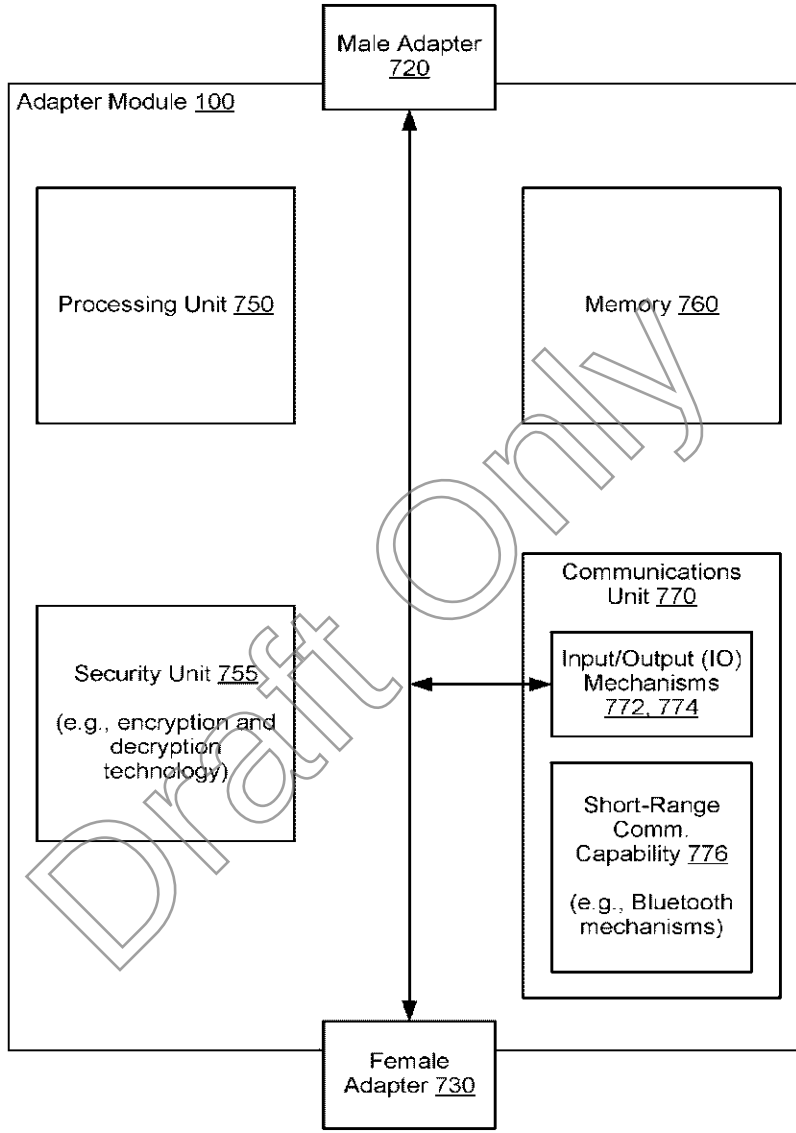


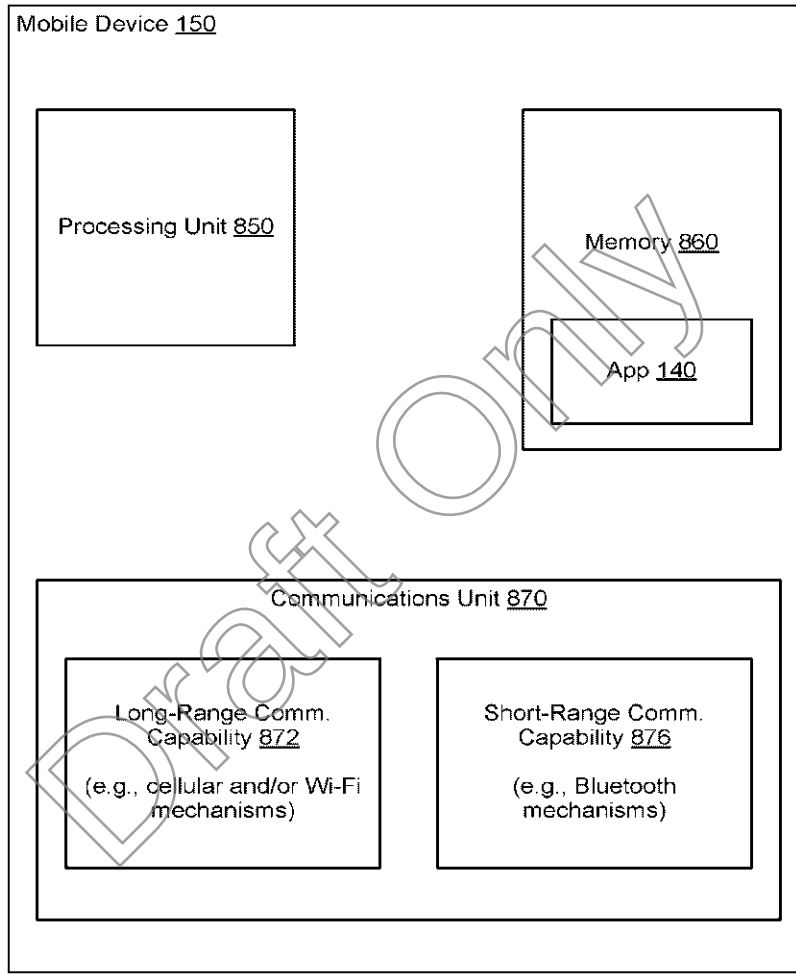
Figure 19

Draft Only



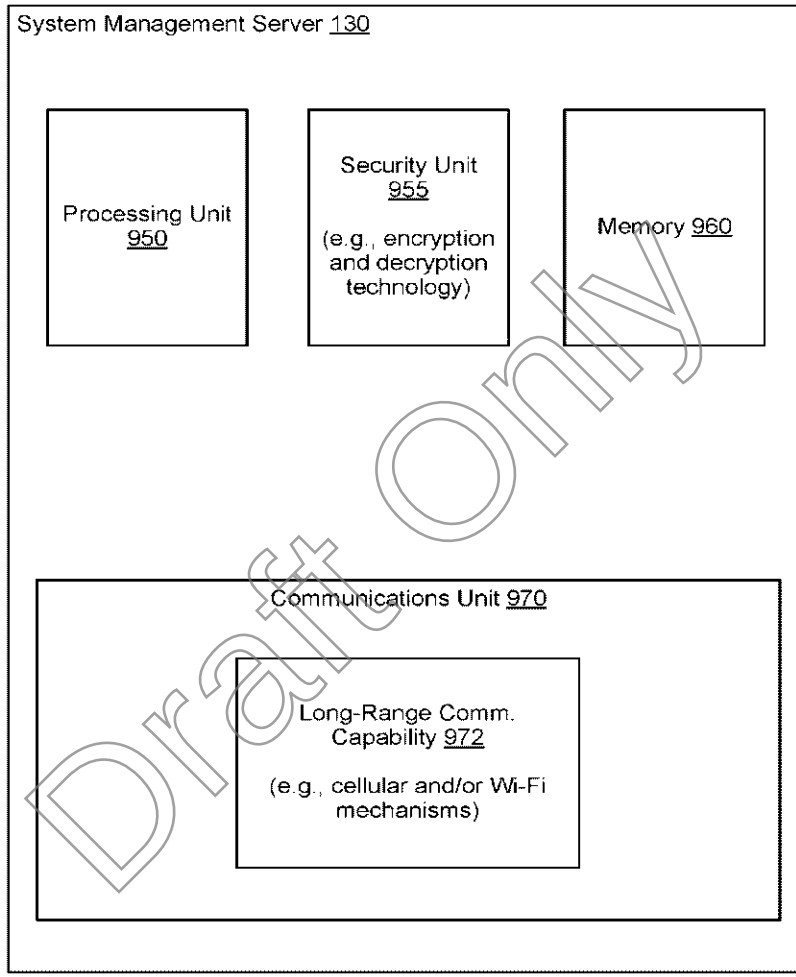
Draft Only

Figure 20



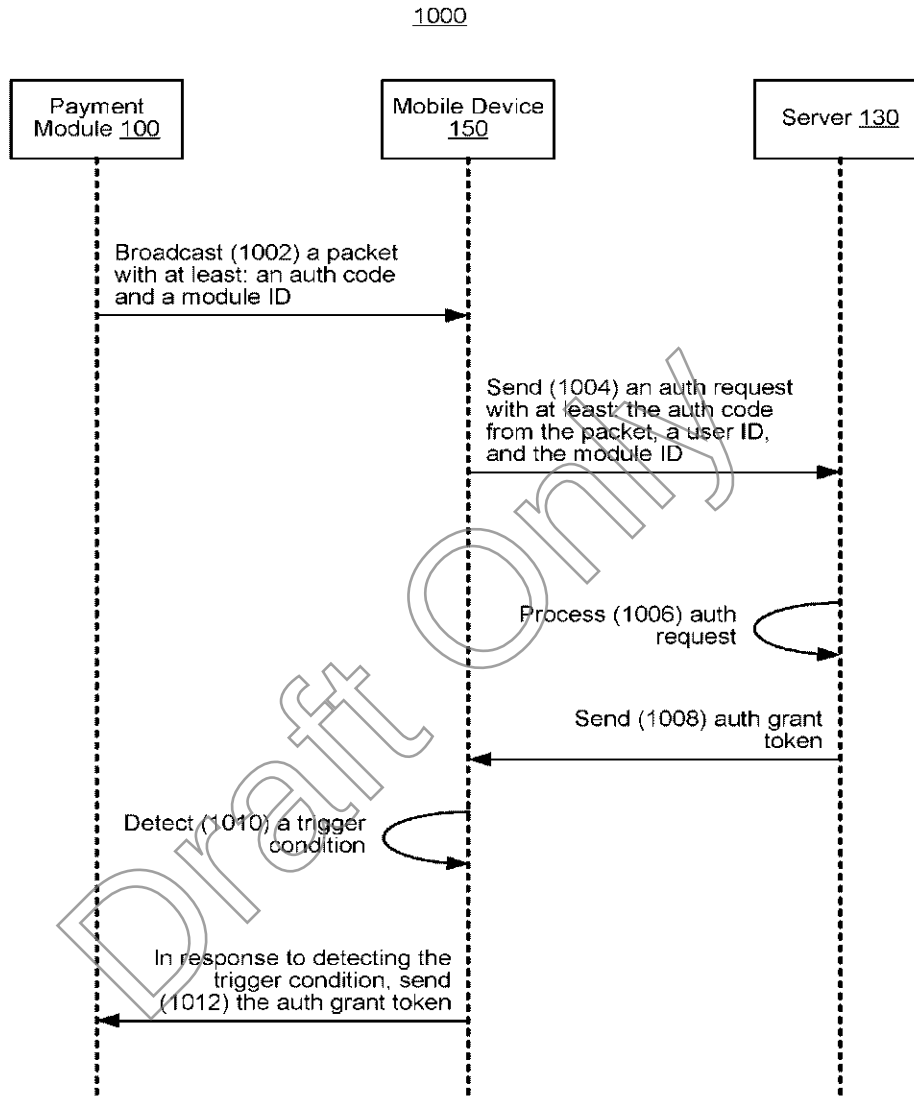
Draft Only

Figure 21



Draft Only

Figure 22



Draft Only

Figure 23

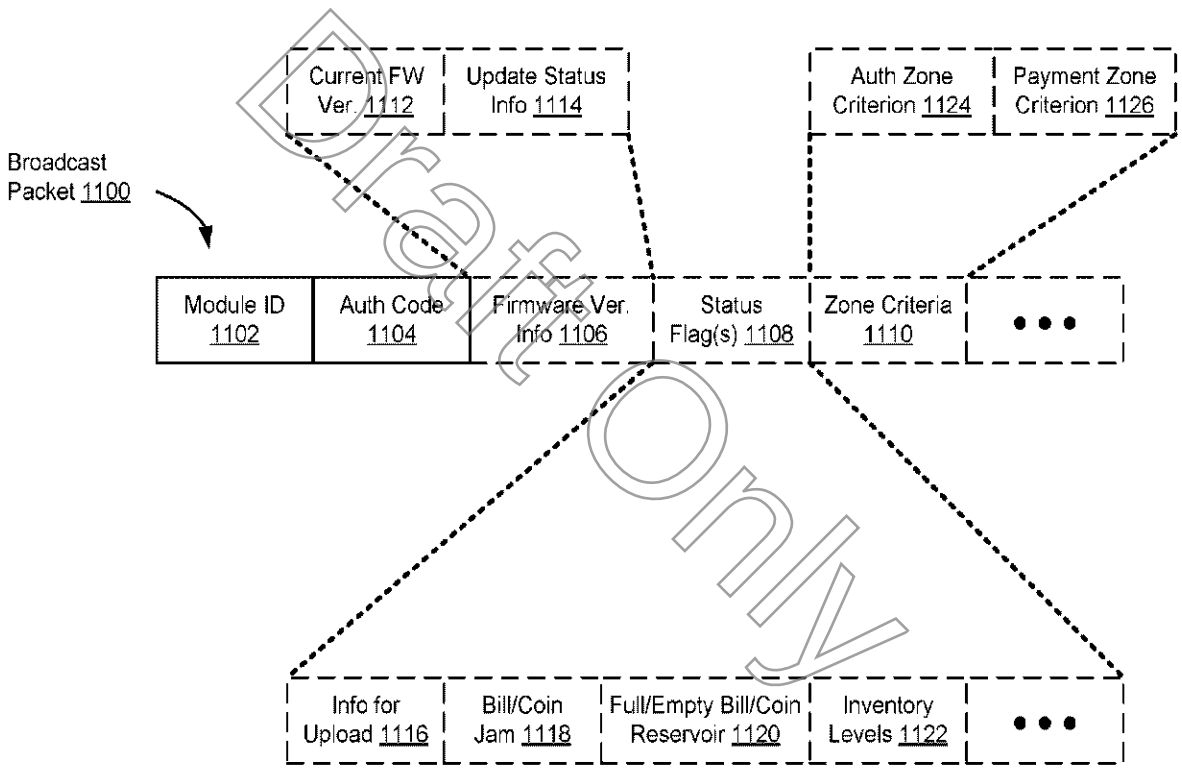


Figure 24A

Draft Only

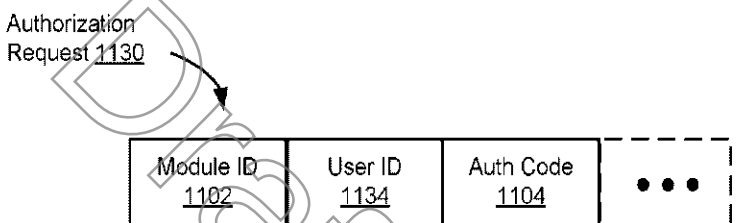


Figure 24B

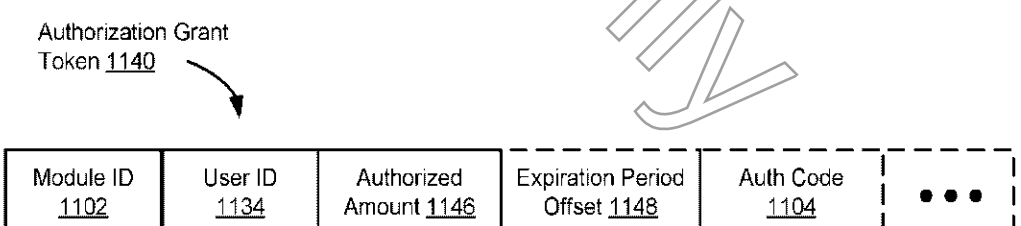
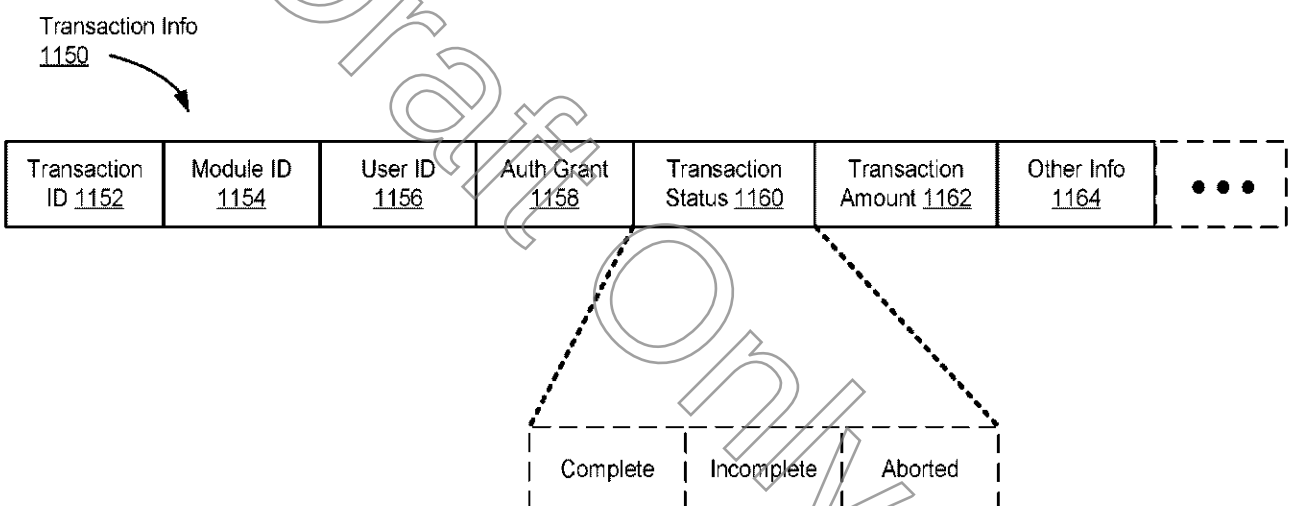


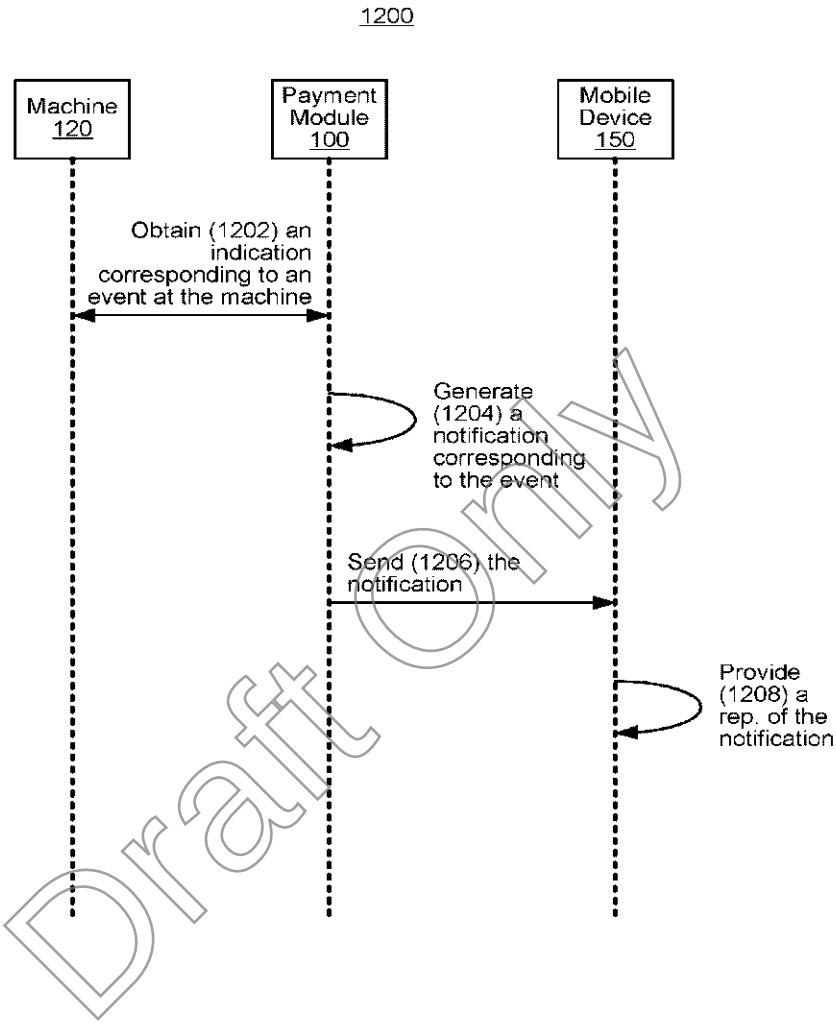
Figure 24C

Draft Only



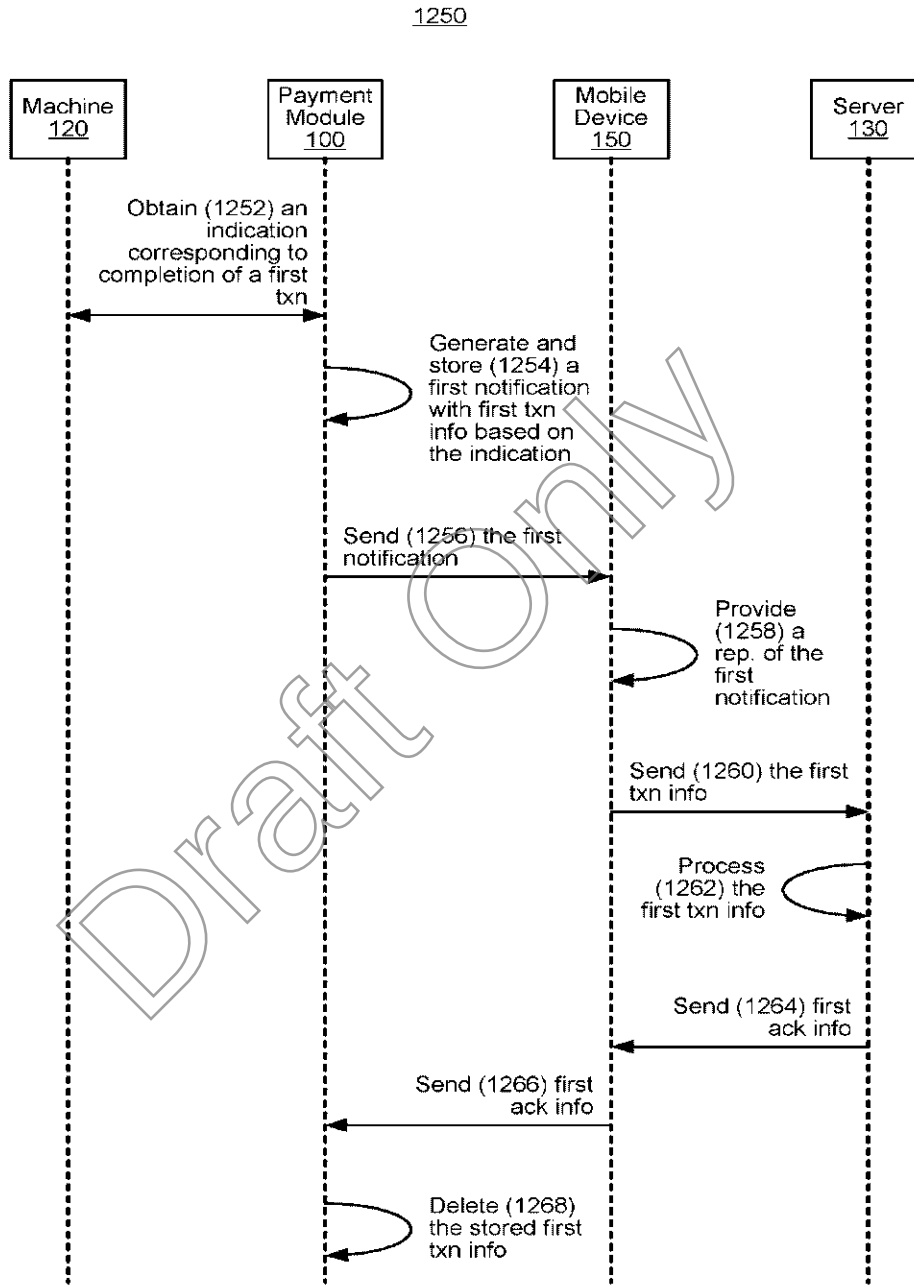
Draft Only

Figure 24D



Draft Only

Figure 25A



Draft Only

Figure 25B

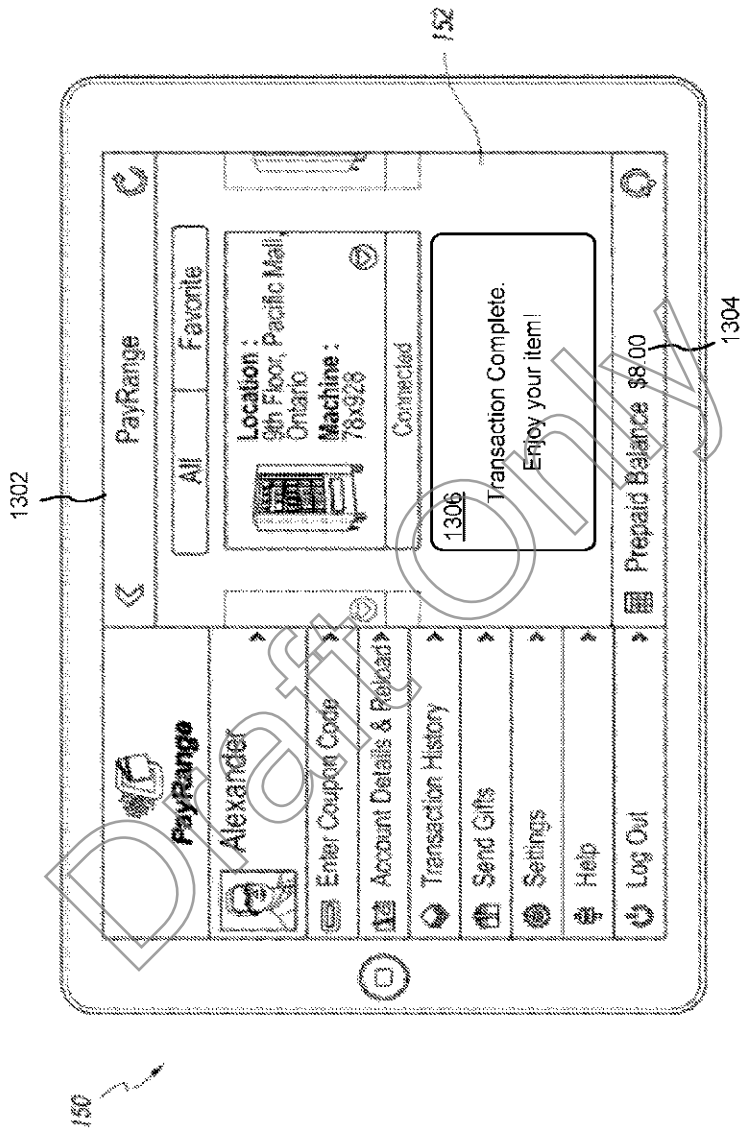


Figure 26A

Draft Only

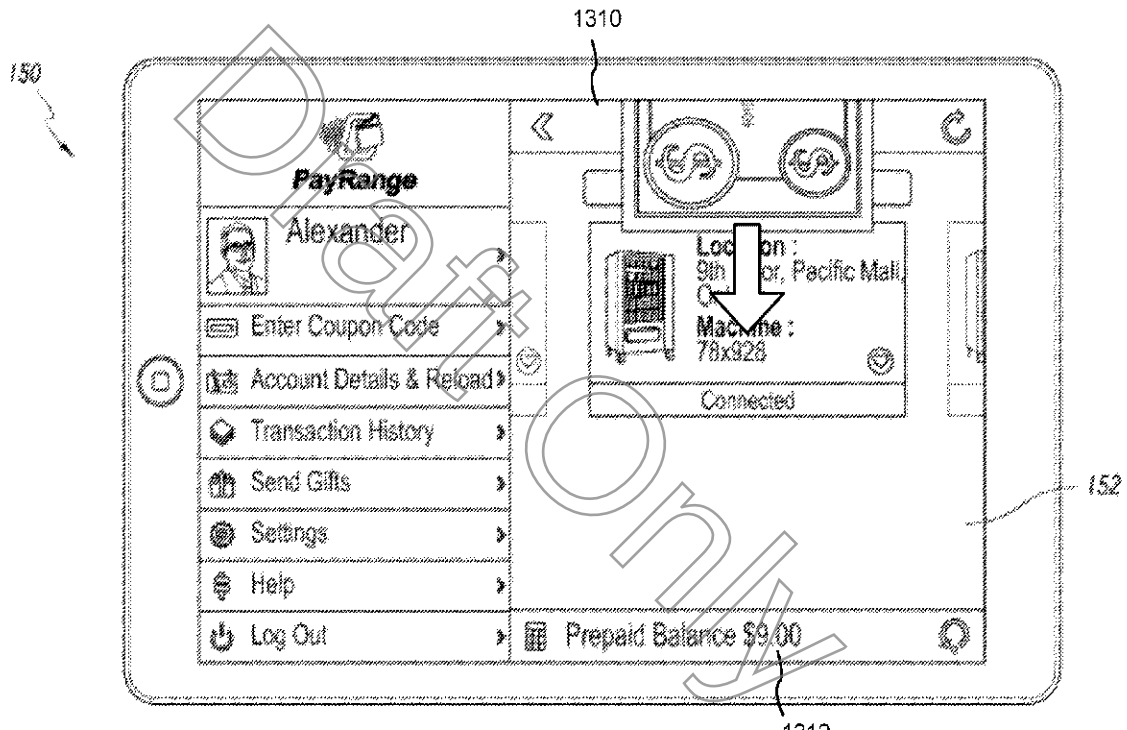


Figure 26B

Draft Only

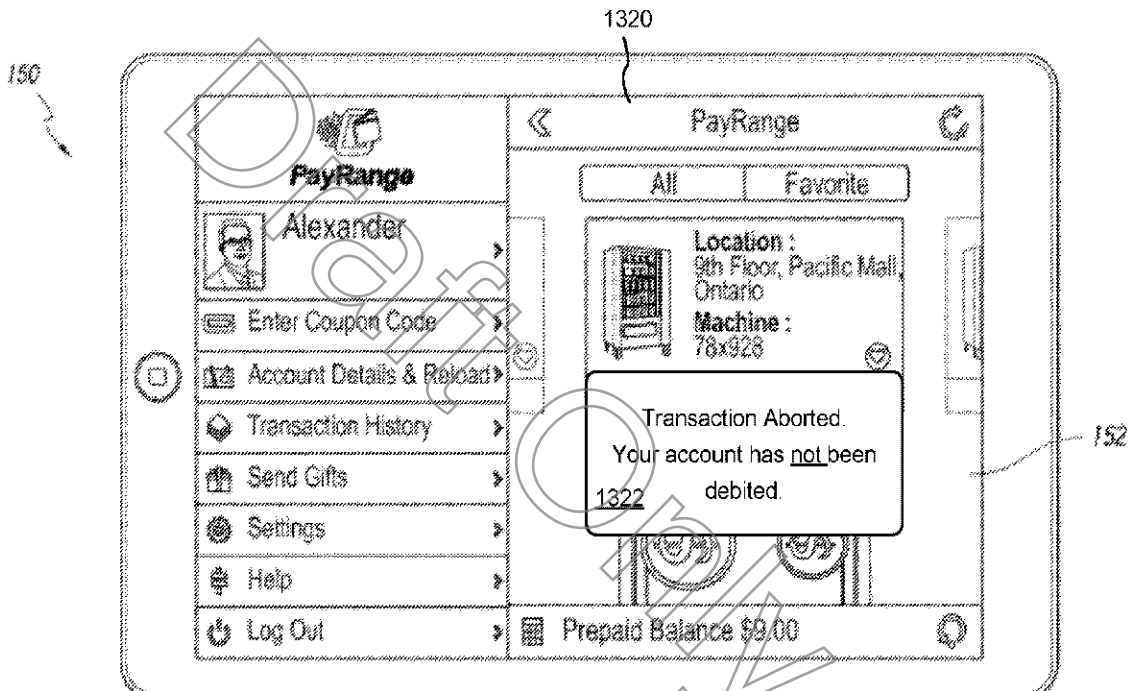


Figure 26C

Patent Owner
CSC ServiceWorks - Ex. 1002
Page 1456 of 1551

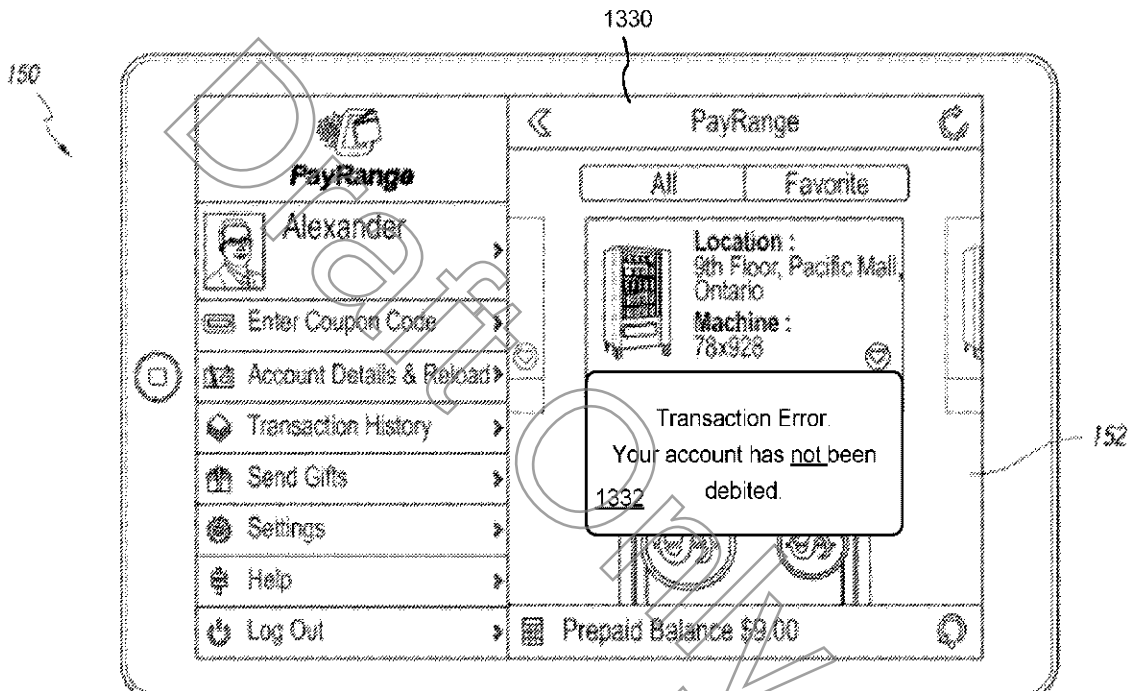


Figure 26D

Draft Only

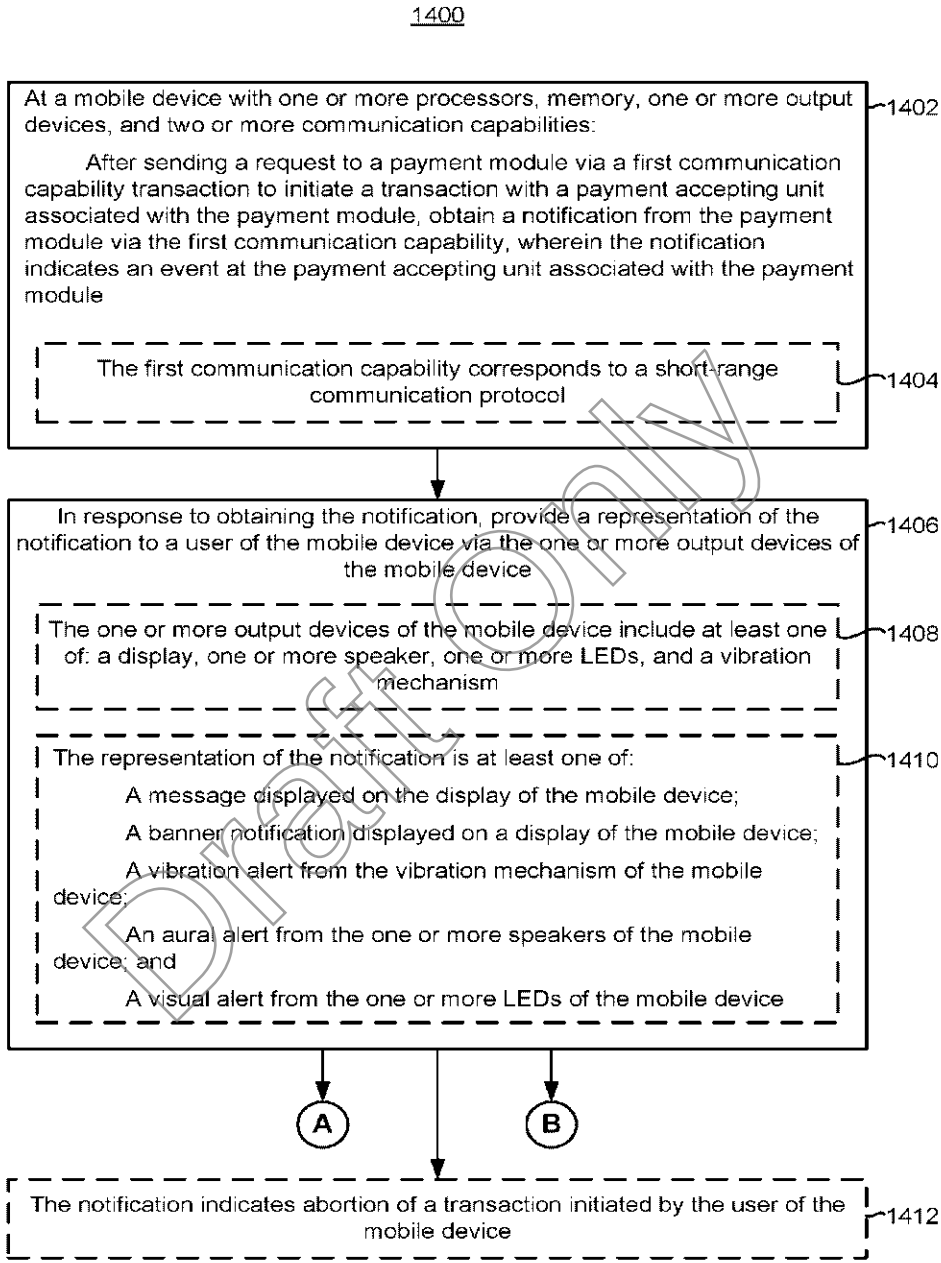
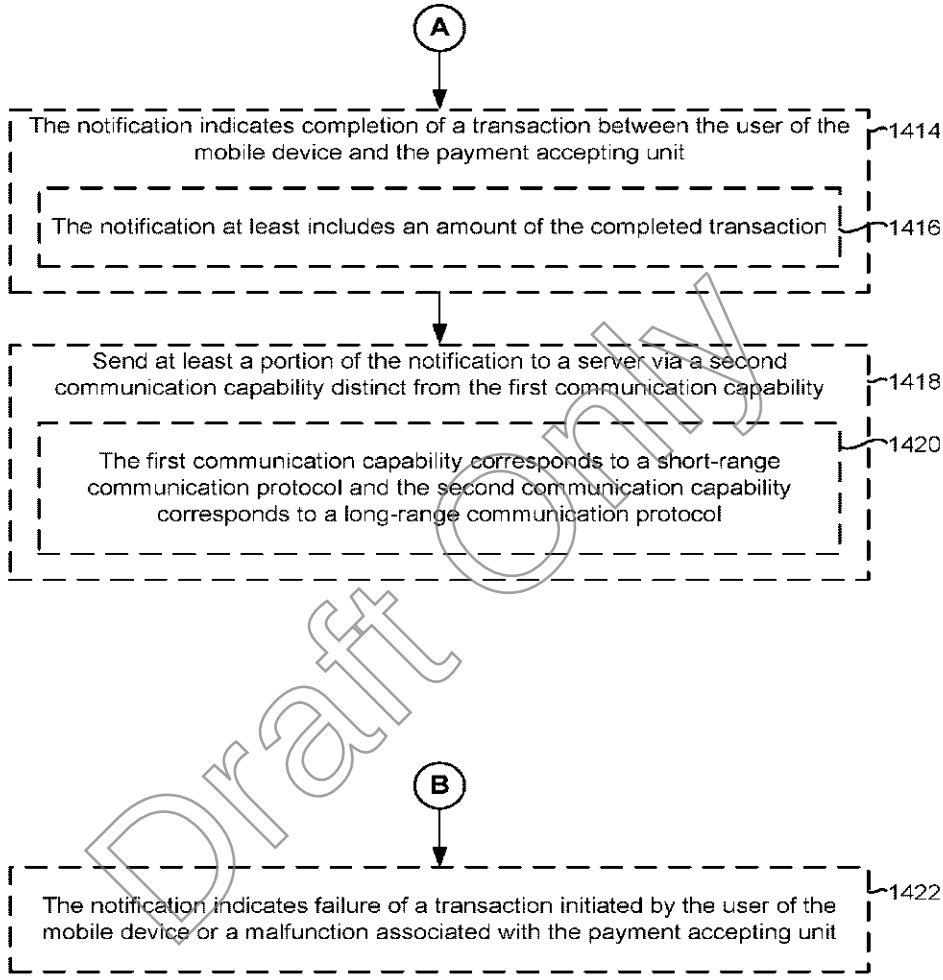


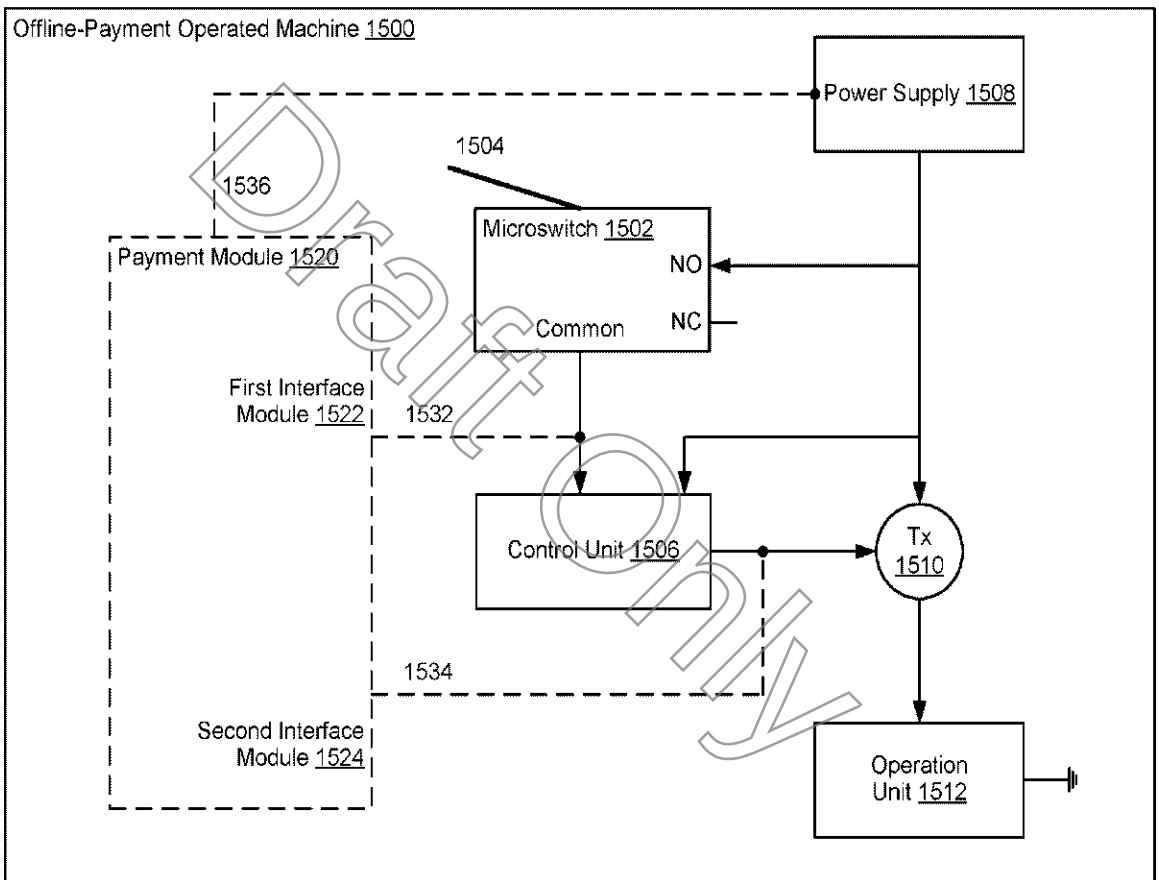
Figure 27A

Draft Only



Draft Only

Figure 27B



Draft Only

Figure 28A

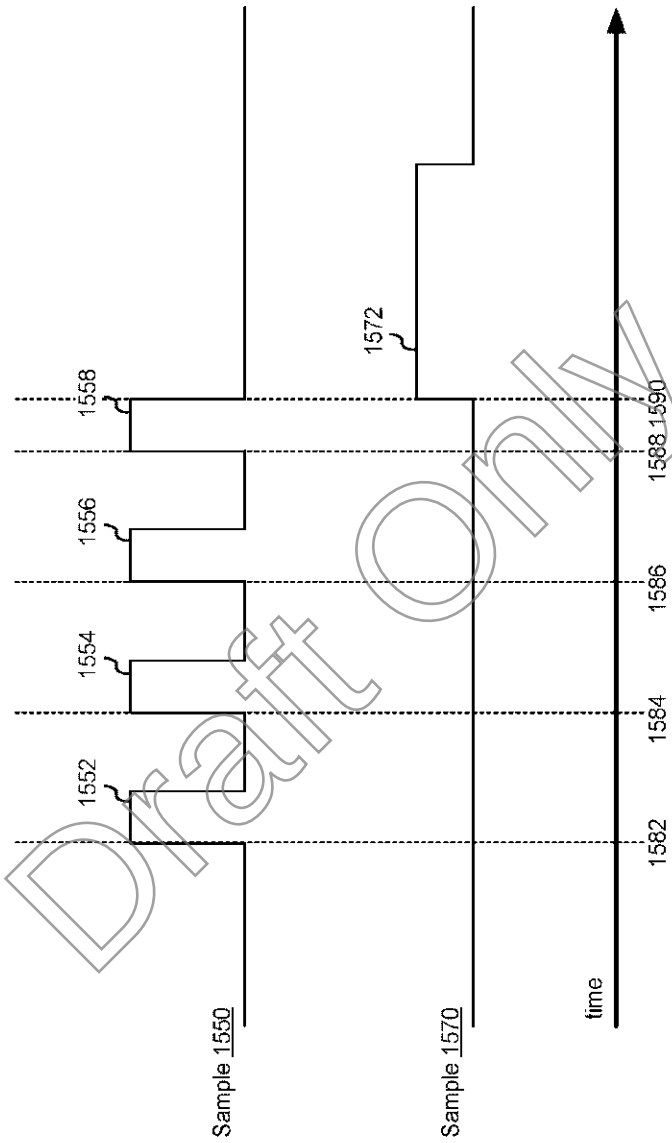


Figure 28B

Draft Only

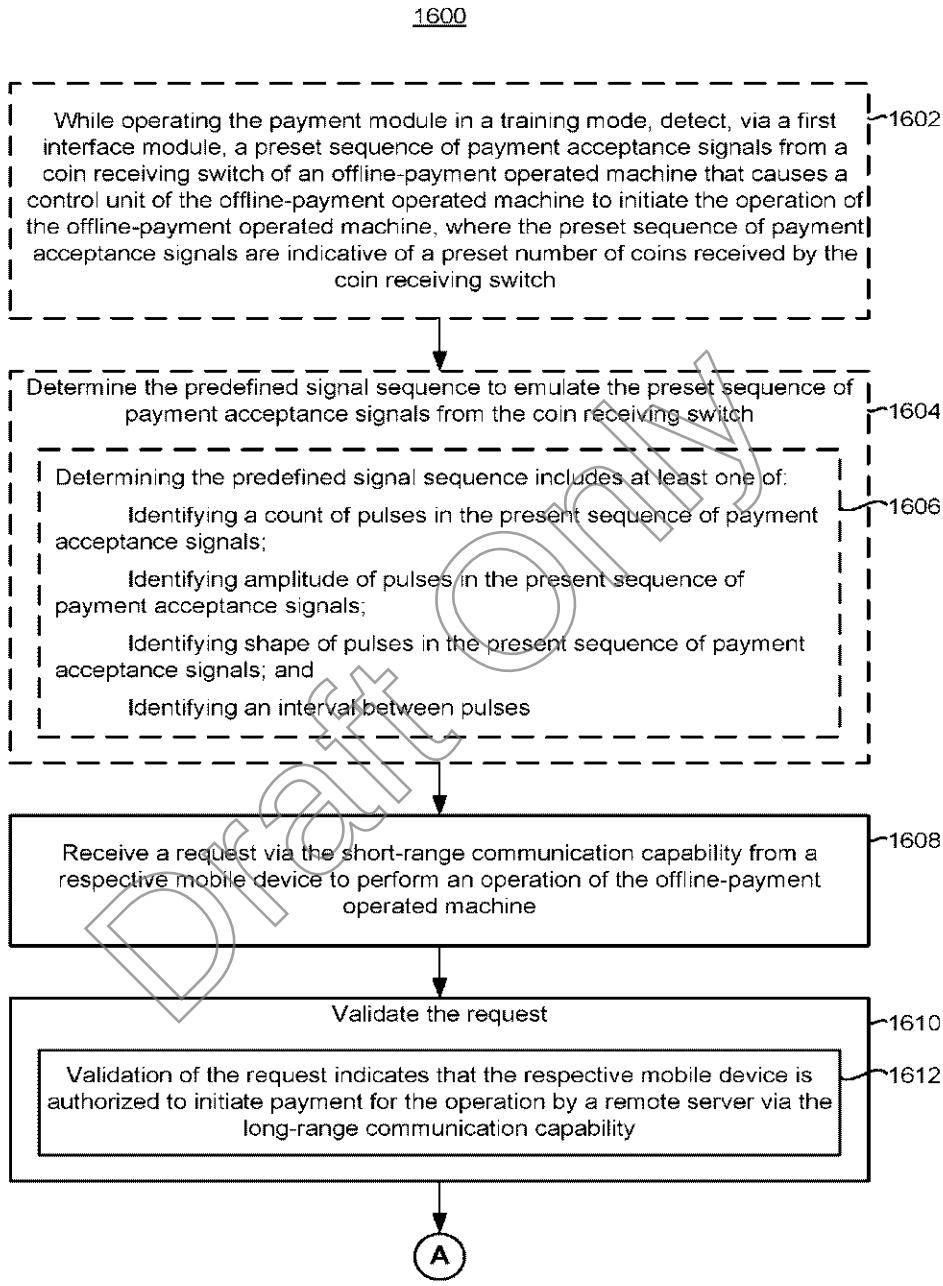
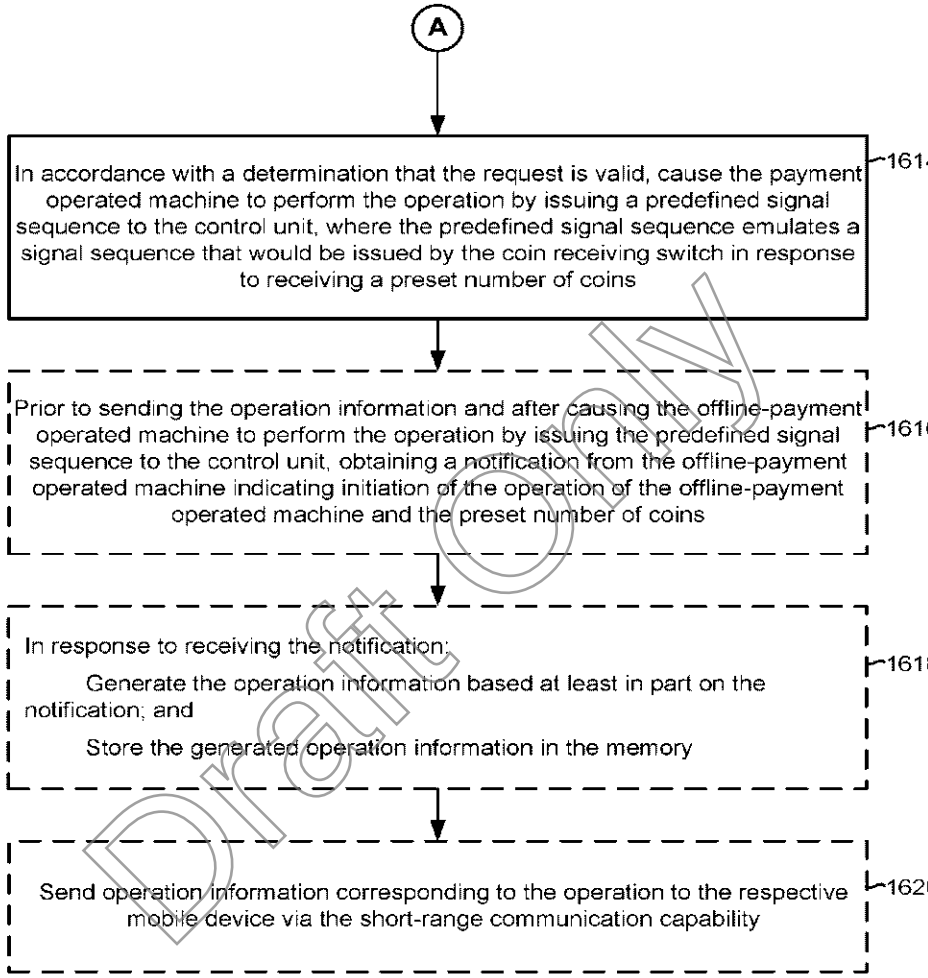


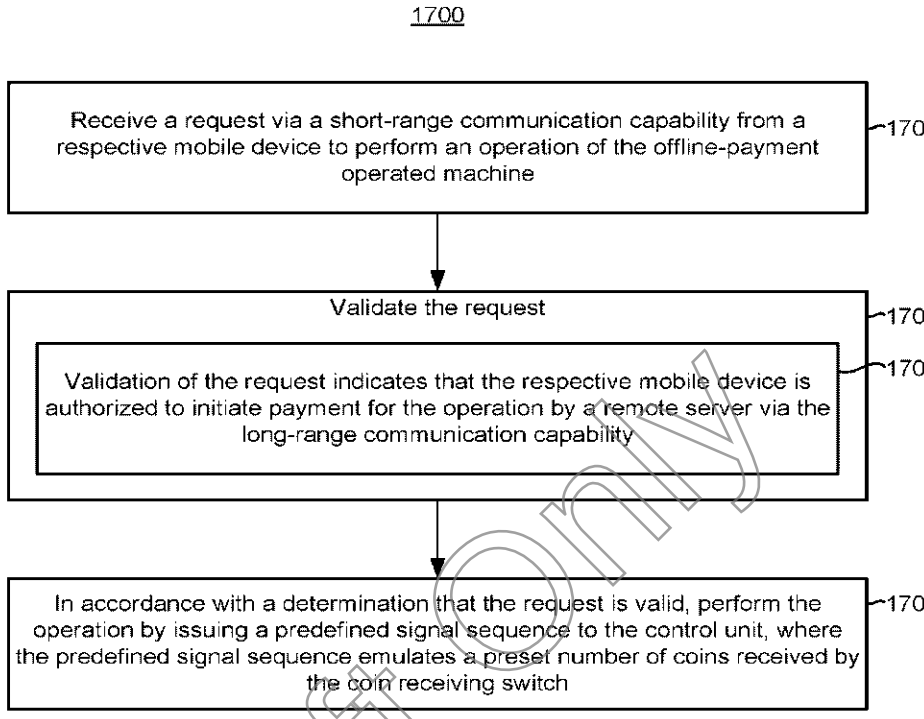
Figure 29A

Draft Only



Draft Only

Figure 29B



Draft Only

Figure 30

CLAIMS

1. A method of presenting representations of payment accepting unit events, comprising:

at a mobile device with one or more processors, memory, one or more output devices including a display, and one or more radio transceivers:

identifying one or more payment accepting units in proximity to the mobile device that are available to accept payment from a mobile payment application executing on the mobile device, the identifying based at least in part on an identifier corresponding to the one or more payment accepting units, wherein the one or more payment accepting units are payment operated machines that accept payment for dispensing of products and/or services;

displaying a user interface of the mobile payment application on the display of the mobile device, the user interface being configured to display a visual indication of the one or more payment accepting units and accept user input to (i) receive selection by a user of the mobile device of an available payment accepting unit of the one or more payment accepting units and (ii) trigger payment by the mobile payment application for a transaction initiated by the user of the mobile device with the available payment accepting unit of the one or more payment accepting units;

establishing via the one or more radio transceivers a wireless communication path including the mobile device and the available payment accepting unit of the one or more payment accepting units;

after establishing the wireless communication path, enabling user interaction with the user interface of the mobile payment application to complete the transaction;

exchanging information with the available payment accepting unit via the one or more radio transceivers, in conjunction with the transaction; and

after exchanging the information, displaying, on the display, an updated user interface of the mobile payment application to the user of the mobile device.

2. The method of claim 1, wherein the updated user interface of the mobile payment application includes at least one of:

a message displayed on the display of the mobile device;

a banner notification displayed on a display of the mobile device; and/or

a visual alert from one or more LEDs of the mobile device.

Draft Only

3. The method of claim 1, wherein the information indicates completion of the transaction between the user of the mobile device and the available payment accepting unit.

4. The method of claim 3, wherein the mobile device includes a long-range transceiver and the information at least includes an amount of the completed transaction, and the method further comprises:

sending at least the amount of the completed transaction to a server via the long-range transceiver.

5. The method of claim 1, wherein the information indicates abortion of the transaction initiated by the user of the mobile device.

6. The method of claim 1, wherein the information indicates failure of the transaction initiated by the user of the mobile device or a malfunction associated with the available payment accepting unit.

7. The method of claim 1, wherein the mobile device includes an accelerometer and the method further comprises:

based on data from the accelerometer, determining whether the user is walking away from the available payment accepting unit; and

in accordance with a determination that the user is walking away from the available payment accepting unit, canceling the wireless communication path.

8. The method of claim 1, wherein the information reflects availability of the available payment accepting unit to conduct a transaction.

9. The method of claim 1, further comprising:

in addition to exchanging the information, receiving, via the one or more radio transceivers, a coupon that is targeted to the user of the mobile device based on the transaction.

10. The method of claim 1, wherein the user interface of the mobile payment application, after establishing the wireless communication path, indicates that the wireless communication path has been established with the available payment accepting unit.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1466 of 1551

11. The method of claim 1, wherein the user interface of the mobile payment application, after establishing the wireless communication path, includes:

a visual representation of the available payment accepting unit;

an indication of a prepared balance; and

an affordance that when slid, indicates the initiation of the transaction;

wherein the affordance is slid in response to receiving a user input of swipe on the affordance displayed on the display of the mobile device.

12. The method of claim 1, wherein the payment operated machines include a payment activated washer, a payment activated dryer, a vending machine, a parking meter, a toll booth, an arcade game, a kiosk, a photo booth, or a ticket dispensing machine.

13. A mobile device, comprising:

one or more radio transceivers;

one or more output devices including a display;

one or more processors; and

memory storing one or more programs to be executed by the one or more processors, the one or more programs comprising instructions for:

identifying one or more payment accepting units in proximity to the mobile device that are available to accept payment from a mobile payment application executing on the mobile device, the identifying based at least in part on an identifier corresponding to the one or more payment accepting units, wherein the one or more payment accepting units are payment operated machines that accept payment for dispensing of products and/or services;

displaying a user interface of the mobile payment application on the display of the mobile device, the user interface being configured to display a visual indication of the one or more payment accepting units and accept user input to (i) receive selection by a user of the mobile device of an available payment accepting unit of the one or more payment accepting units and (ii) trigger payment by the mobile payment application for a transaction initiated by the user of the mobile device with the available payment accepting unit of the one or more payment accepting units;

Draft Only

establishing via the one or more radio transceivers a wireless communication path including the mobile device and the available payment accepting unit of the one or more payment accepting units;

after establishing the wireless communication path, enabling user interaction with the user interface of the mobile payment application to complete the transaction;

exchanging information with the available payment accepting unit via the one or more radio transceivers, in conjunction with the transaction; and

after exchanging the information, displaying, on the display, an updated user interface of the mobile payment application to the user of the mobile device.

14. The mobile device of claim 13, wherein identifying the one or more payment accepting units includes identifying a payment activated washer, a payment activated dryer, a vending machine, a parking meter, a toll booth, an arcade game, a kiosk, a photo booth, or a ticket dispensing machine.

15. A non-transitory computer readable storage medium storing one or more programs, the one or more programs comprising instructions, which, when executed by a mobile device with one or more processors, one or more output devices including a display, and one or more radio transceivers, cause the mobile device to perform operations comprising:

identifying one or more payment accepting units in proximity to the mobile device that are available to accept payment from a mobile payment application executing on the mobile device, the identifying based at least in part on an identifier corresponding to the one or more payment accepting units, wherein the one or more payment accepting units are payment operated machines that accept payment for dispensing of products and/or services;

displaying a user interface of the mobile payment application on the display of the mobile device, the user interface being configured to display a visual indication of the one or more payment accepting units and accept user input to (i) receive selection by a user of the mobile device of an available payment accepting unit of the one or more payment accepting units and (ii) trigger payment by the mobile payment application for a transaction initiated by the user of the mobile device with the available payment accepting unit of the one or more payment accepting units;

Draft Only

establishing via the one or more radio transceivers a wireless communication path including the mobile device and the available payment accepting unit of the one or more payment accepting units;

after establishing the wireless communication path, enabling user interaction with the user interface of the mobile payment application to complete the transaction;

exchanging information with the available payment accepting unit via the one or more radio transceivers, in conjunction with the transaction; and

after exchanging the information, displaying, on the display, an updated user interface of the mobile payment application to the user of the mobile device.

16. The non-transitory computer readable storage medium of claim 15, wherein the updated user interface of the mobile payment application includes at least one of:

a message displayed on the display of the mobile device;

a banner notification displayed on a display of the mobile device; and/or

a visual alert from one or more LEDs of the mobile device.

17. The non-transitory computer readable storage medium of claim 15, wherein:

the information indicates completion of the transaction between the user of the mobile device and the available payment accepting unit;

the information at least includes an amount of the completed transaction; and

the instructions further cause the mobile device to send at least the amount of the completed transaction to a server.

18. The non-transitory computer readable storage medium of claim 15, wherein the information indicates abortion of the transaction initiated by the user of the mobile device.

19. The non-transitory computer readable storage medium of claim 15, wherein the information indicates failure of the transaction initiated by the user of the mobile device or a malfunction associated with the available payment accepting unit.

20. The non-transitory computer readable storage medium of claim 15, wherein identifying the one or more payment accepting units includes identifying a payment activated washer, a

Draft Only

payment activated dryer, a vending machine, a parking meter, a toll booth, an arcade game, a kiosk, a photo booth, or a ticket dispensing machine.

Draft Only

Application Data Sheet 37 CFR 1.76

The Application Data Sheet is part of the provisional or non-provisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.

Inventor Information

of inventors: 1

1. Dr. Paresh K. Patel

Residence Information
US Residency
Portland, OR
UNITED STATES

Mailing Address
9600 NE Cascades Pkwy, Suite 280
Portland, OR 97220
UNITED STATES

Application Information

Customer number	24341 -
Correspondence address	---
Title of invention	METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS
Attorney docket number	104402-5065-US
Entity status	Small
Application type	Nonprovisional Application under 35 USC 111(a)

Draft Only

Subject matter	Utility
Total number of drawing sheets	45
Suggested figure for publication	...
Filing by reference	No
Publication request	Normal eighteen-month publication

Representative Information

of representatives: 1

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).

Customer number 24341

Domestic Benefit/National Stage Information

of benefit claims: 8

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c), 386(c), or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior app status	Pending
Application number	---
Continuity type	**Continuation of**
Prior app number	**17147305**
Filing Date	01/12/2021

Prior app status	Patented
Application number	**17147305**
Continuity type	**Continuation of**

Draft Only

Prior app number	15603400
Filing Date	05/23/2017
Patent number	10891614
Issue date	01/12/2021

Prior app status	Patented
Application number	15603400
Continuity type	Continuation of
Prior app number	14456199
Filing Date	08/12/2014
Patent number	9659296
Issue date	05/23/2017

Prior app status	Patented
Application number	14456199
Continuity type	Continuation in part of
Prior app number	14456683
Filing Date	08/11/2014
Patent number	9256873
Issue date	02/09/2016

Prior app status	Patented
Application number	14456683
Continuity type	Continuation of
Prior app number	14335762
Filing Date	07/18/2014
Patent number	9547859
Issue date	01/17/2017

Prior app status	Patented
Application number	14335762
Continuity type	Continuation of
Prior app number	14214644
Filing Date	03/14/2014
Patent number	8856045
Issue date	10/07/2014

Draft Only

Prior app status	Expired
Application number	**14214644**
Continuity type	**Claims benefit of provisional**
Prior app number	**61917936**
Filing Date	12/18/2013

Prior app status	Patented
Application number	**14214644**
Continuity type	**Continuation in part of**
Prior app number	**29477025**
Filing Date	12/18/2013
Patent number	D755183
Issue date	05/03/2016

Foreign Priority Information

of foreign priority claims: 0

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the Application Data Sheet constitutes the claim for priority as required by 35 U.S.C. 119 (b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Data was not provided for this section.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

Checking this box will cause the application to be examined under the first inventor to file provisions of the AIA.

This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013. NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Draft Only

Authorization or Opt-Out of Authorization to Permit Access

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE:
This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. **Priority Document Exchange (PDX)**
Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h) (1).

B. **Search Results from U.S. Application to EPO**
Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with the search results from the instant application.

NOTE:
Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1475 of 1551

Applicant Information

of applicants: 1

The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46.

1. **PAYRANGE INC.**
   9600 NE Cascades Pkwy, Suite 280
   Portland, OR 97220
   UNITED STATES

   Phone: ---
   Fax: ---
   Email: ---

Applicant: Organization
Applicant type: Assignee

Assignee Information including Non-Applicant Assignee Information

of assignees: 0

An assignee-applicant identified in the "Applicant" section will appear on the patent application as an applicant.

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Data was not provided for this section.

Signature

NOTE:

This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet must be signed by a patent practitioner if one or more of the applicants is a juristic entity (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, all joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of all joint inventor-applicants.

See CFR 1.4(d) for the manner of making signatures and certifications.

Signature	First name	Last name	Registration #	Date
/Benjamin Pezzner/	Benjamin	Pezzner	70711	03/14/2022

Draft Only

ABSTRACT

A mobile device presents representations of payment accepting unit events on a display, by identifying a payment accepting unit that is available to accept payment from a mobile payment application executing on the mobile device, displaying a visual indication of the payment accepting unit and accepting user input to receive selection of the payment accepting unit and trigger payment, establishing a wireless communication path including the mobile device and the payment accepting unit, enabling user interaction with the user interface to complete the transaction, exchanging information with the available payment accepting unit via the one or more radio transceivers in conjunction with the transaction, and displaying an updated user interface of the mobile payment application.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1477 of 1551

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

PRIORITY

[0001] The present application is:

- a continuation of U.S. Patent Application No. 17/147,305, filed January 12, 2021,
- which is a continuation of U.S. Patent Application No. 15/603,400, filed May 23, 2017 and issued as U.S. Patent No. 10,891,614 on January 12, 2021,
- which is a continuation of U.S. Patent Application No. 14/458,199, filed August 12, 2014 and issued as U.S. Patent No. 9,659,296 on May 23, 2017,
- which is a continuation-in-part of U.S. Patent Application Number 14/456,683, filed August 11, 2014 and issued as U.S. Patent No. 9,256,873 on February 9, 2016,
- which is a continuation of U.S. Patent Application Number 14/335,762, filed July 18, 2014 and issued as U.S. Patent No. 9,547,859 on January 17, 2017,
- which is a continuation of U.S. Patent Application Number 14/214,644, filed March 14, 2014 and issued as U.S. Patent No. 8,856,045 on October 7, 2014,
- which claims priority to U.S. Provisional Patent Application Number 61/917,936, filed December 18, 2013.
- U.S. Patent Application Number 14/214,644, filed March 14, 2014, is also a continuation-in-part of U.S. Design Patent Application Number 29/477,025, filed December 18, 2013 and issued as U.S. Design Patent No. D755,183 on May 3, 2016.

The present application is based on and claims priority to these applications, the disclosures of which are hereby incorporated by reference in their entirety.

Draft Only

TECHNICAL FIELD

[0002] The present application relates to the field of payment processing systems, and in particular, to a mobile-device-to-machine payment processing system over a non-persistent network connection.

CSC ServiceWorks - Ex. 1002
Page 1478 of 1551

BACKGROUND

[0003] Vending machines (or "automatic retailing" machines), in the broadest sense, have been around for thousands of years. The first simple mechanical coin operated vending machines were introduced in the 1880s. Modern vending machines stock many different types of products including, but not limited to drinks (e.g., water, juice, coffee, and soda) and edible food products/items (e.g., snacks, candy, fruit, and frozen meals), as well as a wide variety of non-food items. In this fast paced world, vending machines are ubiquitous.

[0004] Vending machines are one type of "payment accepting unit" (payment accepting units are also referred to herein generically as "machines"). A payment accepting unit (or machine) is equipment that requires payment for the dispensing of products and/or services. In addition to vending machines, payment accepting units can also be other machines that require payment for the dispensing of a product and/or services including, but not limited to parking meters, toll booths, laundromat washers and dryers, arcade games, kiosks, photo booths, toll booths, transit ticket dispensing machines, and other known or yet to be discovered payment accepting units.

[0005] In using a payment accepting unit, a user will (1) approach the payment accepting unit, (2) determine from the face of the payment accepting unit the product (or service) he/she desires, (3) insert payment (e.g., coins, bills, or payment cards), and (4) input his/her selection into the payment accepting unit using a user interface (e.g., a series of buttons, a key pad, touch screen, or other input mechanism using, for example, the column and row at which a product is located). Based on the user's inputted selection, technology within the payment accepting unit provides the desired product (or service) to the user.

[0006] As the number of people with Internet-connected mobile devices proliferates, so does the variety of uses for such devices. Mobile payment is a logical extension. There is a large development effort around bringing mobile payment to the retail sector in an effort to not only provide options to the user, but also increased convenience.

SUMMARY

[0007] Disclosed herein is a payment processing system or, more specifically, a mobile-device-to-machine payment processing system over a non-persistent network connection with

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1479 of 1551

hands-free mode and manual mode (sometimes also herein called "swipe" or "swipe-to-pay" mode).

[0008] In some implementations, a method of presenting representations of payment accepting unit events is performed at a device (e.g., the mobile device 150, Figures 5 and 21) with one or more processors, memory, one or more output devices, and two or more communication capabilities. After sending a request to a payment module (e.g., the adapter module 100, Figures 5 and 20), via a first communication capability (e.g., a short-range communication technology/protocol such as BLE), to initiate a transaction with a payment accepting unit (e.g., the payment accepting unit 120, Figures 5 and 19) (sometimes also herein called "machine 120") associated with the payment module, the method includes obtaining a notification from the payment module via the first communication capability, where the notification indicates an event at the payment accepting unit associated with the payment module. In response to obtaining the notification, the method includes providing a representation of the notification to a user of the mobile device via the one or more output devices of the mobile device (e.g., a message displayed on a display of the mobile device, a vibration produced by a vibration mechanism of the mobile device, an aural alert produced by a speaker of the mobile device, and/or the like).

[0009] In some implementations, a method of retrofitting an offline-payment operated machine to accept electronic payments is performed at a payment module (e.g., the adapter module 100, Figures 5 and 20) with one or more processors, memory, a short-range communication capability (e.g., a short-range communication technology/protocol such as BLE), and a first interface module configured to couple the payment module with a control unit of an offline-payment operated machine (e.g., the payment accepting unit 120, Figures 5 and 19) (sometimes also herein called "machine 120"). The method includes receiving a transaction request via the short-range communication capability from a respective mobile device to perform a transaction with the offline-payment operated machine. The method includes validating the transaction request, where validation of the transaction request indicates that the respective mobile device is authorized to initiate payment for the transaction by a remote server (e.g., the server 130, Figures 5 and 22) via the long-range communication capability (e.g., the long-range communication technology/protocol such as GSM, CDMA, or Wi-Fi). In accordance with a determination that the transaction request is valid, the method includes causing the offline-

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1480 of 1551

payment operated machine to perform the requested transaction by issuing a signal to perform the transaction to the control unit of the offline-payment operated machine via the first interface module.

[0010] In some implementations, a device (e.g., the machine 120, (Figures 5 and 19), the adapter module 100 (Figures 5 and 20), the mobile device 150 (Figures 5 and 21), the server 130 (Figures 5 and 22), or a combination thereof) includes one or more processors and memory storing one or more programs for execution by the one or more processors, the one or more programs include instructions for performing, or controlling performance of, the operations of any of the methods described herein. In some implementations, a non-transitory computer readable storage medium storing one or more programs, the one or more programs comprising instructions, which, when executed by a device (e.g., the machine 120, (Figures 5 and 19), the adapter module 100 (Figures 5 and 20), the mobile device 150 (Figures 5 and 21), the server 130 (Figures 5 and 22), or a combination thereof) with one or more processors, cause the computer system to perform, or control performance of, the operations of any of the methods described herein. In some implementations, a device (e.g., the machine 120, (Figures 5 and 19), the adapter module 100 (Figures 5 and 20), the mobile device 150 (Figures 5 and 21), the server 130 (Figures 5 and 22), or a combination thereof) includes means for performing, or controlling performance of, the operations of any of the methods described herein.

[0011] The subject matter described herein is particularly pointed out and distinctly claimed in the concluding portion of this specification. Objectives, features, combinations, and advantages described and implied herein will be more readily understood upon consideration of the following detailed description of the invention, taken in conjunction with the accompanying drawings.

Draft Only

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] Figure 1 is a schematic diagram that shows three zones: a "communication zone" (e.g., Bluetooth range), an "authorization zone," and a "payment zone" in accordance with some implementations.

[0013] Figure 2 is a schematic diagram that shows the three zones of Figure 1 with multiple users therein in accordance with some implementations.

CSC ServiceWorks - Ex. 1002
Page 1481 of 1551

[0014] Figure 3 is a table that illustrates the hands-free credit or alert user principle in accordance with some implementations.

[0015] Figure 4 is a flow chart showing the logging received signal strength indicator (RSSI) information in accordance with some implementations.

[0016] Figure 5 is a block schematic that shows elements of the payment processing system including, but not limited to, the adapter module, the machine, the mobile device, and servers, as well as communications therebetween in accordance with some implementations.

[0017] Figure 6 is a block schematic that shows three areas of encryption used (each is bi-directional) between the adapter module, the machine, the mobile device, and/or servers in accordance with some implementations.

[0018] Figure 7 is a block diagram that shows communications, messaging, vending sequence, and purchase flow between the adapter module, the mobile device, and a system management server in accordance with some implementations.

[0019] Figure 8A is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) when the user enters the "communication zone" (e.g., Bluetooth range) in accordance with some implementations.

[0020] Figure 8B is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) when the user enters the "authorization zone" in accordance with some implementations.

[0021] Figure 8C is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) when the user enters the "payment zone" and, in particular, detailing a hands-free mode embodiment and a swipe mode embodiment in accordance with some implementations.

[0022] Figure 8D is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1482 of 1551

sequence, and purchase flow) in a vending transaction including a loop for multiple transactions in accordance with some implementations.

[0023] Figure 8E is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) in the login mode in accordance with some implementations.

[0024] Figure 8F is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) during boot-up of the adapter module in accordance with some implementations.

[0025] Figure 8G is a schematic process flow diagram that shows additional elements and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) during an account check/update process in accordance with some implementations.

[0026] Figures 9A-9E are flow charts that show example steps and features of the payment processing system (e.g., communications, messaging, vending sequence, and purchase flow) in accordance with some implementations.

[0027] Figures 10A-10D show a mobile device with a graphical representation of a mobile application shown thereon, the mobile application being used as part of the mobile-device-to-machine payment processing system in accordance with some implementations.

[0028] Figure 11 is a perspective view of the in-line dongle adapter module in accordance with some implementations.

[0029] Figure 12 is a front plan view of the in-line dongle adapter module of Figure 11 in accordance with some implementations.

[0030] Figure 13 is a back plan view of the in-line dongle adapter module of Figure 11 in accordance with some implementations.

[0031] Figure 14 is a side view of the in-line dongle adapter module of Figure 11 in accordance with some implementations.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1483 of 1551

[0032] Figure 15 is a first end view of a connector receptacle of the in-line dongle adapter module of Figure 11 in accordance with some implementations.

[0033] Figure 16 is a second end view of a connector receptacle of the in-line dongle adapter module of Figure 11 in accordance with some implementations.

[0034] Figure 17 is a perspective view taken from the first end of the in-line dongle adapter module of Figure 11, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for illustrative purposes in accordance with some implementations.

[0035] Figure 18 is a perspective view taken from the second end of the in-line dongle adapter module of Figure 11, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for illustrative purposes in accordance with some implementations.

[0036] Figure 19 is a perspective view of the in-line dongle adapter module of Figure 11 within a vending machine in accordance with some implementations.

[0037] Figure 20 is a block diagram of an adapter module in accordance with some implementations.

[0038] Figure 21 is a block diagram of a mobile device in accordance with some implementations.

[0039] Figure 22 is a block diagram of a server in accordance with some implementations.

[0040] Figure 23 is a schematic flow diagram of a process for authenticating a user to perform a transaction in the payment processing system in accordance with some implementations.

[0041] Figure 24A is a block diagram of a packet of information broadcast by the payment module (sometimes also herein called the "adapter module") in accordance with some implementations.

[0042] Figure 24B is a block diagram of an authorization request in accordance with some implementations.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1484 of 1551

[0043] Figure 24C is a block diagram of an authorization grant token in accordance with some implementations.

[0044] Figure 24D is a block diagram of transaction information generated by the payment module in accordance with some implementations.

[0045] Figure 25A illustrates a schematic flow diagram of a process for providing a representation of a machine event at a mobile device in accordance with some implementations

[0046] Figure 25B is a schematic flow diagram of a process for processing acknowledgment information in the payment processing system in accordance with some implementations.

[0047] Figures 26A-26D illustrate example user interfaces for providing a representation of a machine event at a mobile device in accordance with some implementations.

[0048] Figures 27A-27B illustrate a flowchart diagram of a method of presenting representations of payment accepting unit events in accordance with some implementations.

[0049] Figure 28A illustrates a block diagram of an offline-payment operated machine in accordance with some implementations.

[0050] Figure 28B illustrates signals sampled by the payment module in accordance with some implementations.

[0051] Figures 29A-29B illustrate a flowchart diagram of a method 1600 of retrofitting an offline-payment operated machine to accept electronic payments in accordance with some implementations.

[0052] Figure 30 illustrates a flowchart diagram of a method of enabling a payment operated machine to accept electronic payments in accordance with some implementations.

[0053] Like reference numerals refer to corresponding parts throughout the several views of the drawings.

DETAILED DESCRIPTION

[0054] Disclosed herein is a payment processing system or, more specifically, a mobile-device-to-machine payment processing system for processing transactions over a non-persistent

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1485 of 1551

network connection. The mobile-device-to-machine payment processing system disclosed herein focuses on the unattended retail space (e.g., a payment accepting unit 120, sometimes also herein called a "machine 120"). More specifically, the mobile-device-to-machine payment processing system disclosed herein allows a user (having a mobile device 150 with a mobile application 140 thereon) to make a cashless purchase from a payment accepting unit 120 (having an adapter module 100 associated therewith).

[0055] The mobile-device-to-machine payment processing system described herein can be implemented with one or more of the following features: easy installation feature, a non-persistent network connection feature; a manual (swipe to pay) mode feature; a hands-free mode feature; and a multiple vending transactions (multi-vend) feature.

[0056] Easy Installation: Installation is very easy, requires no tools, requires no configuration, and takes as little as 30 seconds. This is accomplished by using an adapter module 100 (sometimes also herein called "payment module 100") such as an in-line dongle (a hardware device with software thereon) design for in-line insertion within a multi-drop bus (MDB) of a payment accepting unit 120 (e.g., a vending machine) (sometimes also herein called 'the machine 120"). Installation is as simple as "powering down" (turning off) the machine 120, identifying the "wire" that connects with a payment receiving mechanism (e.g., the coin mechanism), disconnecting the wire (so that there are two loose ends, such as a male connection end or adapter of an MDB and a female connection end or adapter of an MDB), plugging (inserting) the adapter module 100 in serial ("in-line") with the wire (e.g., connecting the MDB female adapter to a male adapter of the adapter module 100 and connecting the MDB male adapter to a female adapter of the adapter module 100), tucking the wire and the installed adapter module 100 back into position, and "powering up" (turning on) the machine 120. Most vending machines made since 1995 have this industry standard MDB technology that would allow this easy 30-second installation. On machines without MDB technology, the adapter module 100 can be configured or designed to work with other serial protocols or activate a switch. In essence the adapter module 100 simulates establishing payment on payment accepting unit 120 in much the same manner as other alternative forms of payment (e.g., cash).

[0057] Non-persistent Network Connection: Although payment accepting units (or "machines") that accept only cash (e.g., paper currency and coins) may not require a connection

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1486 of 1551

(persistent or non-persistent) to a network, traditional payment accepting units that accept cashless payments (e.g., credit cards, debit cards, and alternative mobile device payment methods using, for example, smart phones) require a persistent connection to a network (wired or wireless) to facilitate the cashless payments. In other words, without a persistent (ongoing or accessible on demand) network connection, traditional payment accepting units cannot accept cashless payments. Most traditional payment accepting units that accept cashless payments include the technology to accomplish this persistent network connection that allows them to connect to a remote server. If the network connection to a traditional machine is temporarily interrupted, cashless payments will be temporarily unavailable. If the machine is located in a location where no network connection is available, cashless payments is not possible. In addition to using a mobile device 150 as an intermediary between the payment accepting units 120 and the server 130, the mobile-device-to-machine payment processing system described herein minimizes (i.e., the manual mode) or eliminates (i.e., the hands-free mode) user interaction with the mobile device 150. Further, in some implementations, the mobile-device-to-machine payment processing system described herein facilitates the acceptance of cashless payments without requiring any network connection near the payment accepting unit 120. In some implementations, when the mobile-device-to-machine payment processing system described herein is located in a remote location where network connection is unavailable, the mobile-device-to-machine payment processing system, therefore, can still accept cashless payments.

[0058] Manual (Swipe-to-Pay) Mode: Using a "swipe-to-pay" feature (or just "swipe") refers to a user's action implemented on his/her mobile device 150 where he/she quickly brushes his/her finger (or other pre-determined interaction) on the mobile device's touch screen 152 (Figures 10A-10D) or other input devices associated with the mobile device 150. From the user's perspective, when the user is within range, a pre-installed mobile application 140 automatically connects to the payment accepting unit 120 (e.g., a vending machine). The mobile application 140 might display (on the touch screen 152) a prepaid balance that the user "swipes" to transfer payment to the payment accepting unit 120. The user could observe the transferred funds on the touch screen 152 of the mobile device 150 and/or on the display 122, 124 (Figure 19) of the payment accepting unit 120. The transaction is completed just as if cash was inserted in the machine 120 with the user inputting his selection on the payment accepting unit 120 and the payment accepting unit 120 dispensing the product or service. After the selection is made, the

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1487 of 1551

change is returned to the mobile device 150 and this may be shown on the touch screen 152 of the mobile device 150.

[0059] Hands-Free Mode: A "hands-free pay" feature (or just "hands-free") would most likely be used with "favorite" payment accepting units 120 (e.g., a frequently used vending machine at a user's work or school). From the user's perspective, he/she would approach the favorite payment accepting unit 120 and notice that the display 122, 124 (Figure 19) of the payment accepting unit 120 shows funds available, he/she would select the product or service using the payment accepting unit's input mechanisms (e.g., buttons 126 or a touch screen display 124 shown in Figure 19), and he/she would retrieve dispensed services or products. It would be that simple. More specifically, when the user is within range, a pre-installed mobile application 140 automatically connects to the payment accepting unit 120 (e.g., a vending machine). The user may leave the mobile device 150 in a pocket, purse, briefcase, backpack, or other carrier. As the user approaches the payment accepting unit 120 and is in approximately "arm's-length" distance (e.g., 3 to 5 feet) of the payment accepting unit 120, the user could observe the transferred funds on the display 122, 124 (Figure 19) of the payment accepting unit 120. The transaction is completed just as if cash was inserted into the payment accepting unit 120 with the user inputting his/her selection on the payment accepting unit 120 and the payment accepting unit 120 dispensing the product or service. After the selection is made, the change is returned to the mobile device 150. Figure 3 details when the hands-free mode would be available.

[0060] Multiple Vending Transactions (Multi-Vend): Both the manual and hands-free modes could be used multiple times in sequence (implemented, for example, as a loop) so that a user may make multiple purchases. After making his/her first selection and receiving his product (or service), the user would observe that additional funds were available on the display 122, 124 (Figure 19) on the payment accepting unit 120. He/she could make another selection (or multiple selections) and receive additional product(s) (or service(s)). More specifically, the display 122, 124 (Figure 19) may reset as if the transaction is complete, but then, because the user is still standing in range, the mobile application 140 would send another credit to the payment accepting unit 120, allowing for a second purchase. When the user walks away, the system clears (e.g., returns unused funds to the application 140 on the mobile device 150).

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1488 of 1551

[0061] The features described above, alone or in combination with other features described herein will revolutionize the hundred billion dollar automated retail industry. The hardware is very low cost and there are no reoccurring fees because no cellular connection is required on the machine 120. Using the mobile-device-to-machine payment processing system described herein, operators of machines 120 can increase frequency of visits by purchasers and items sold with each visit.

[0062] The mobile-device-to-machine payment processing system described herein may be implemented as an apparatus, system, and/or method for enabling payments to a machine 120 via a mobile device 150. The mobile-device-to-machine payment processing system may be better understood with reference to the drawings, but the shown mobile-device-to-machine payment processing system is not intended to be of a limiting nature.

DEFINITIONS

[0063] Before describing the mobile-device-to-machine payment processing system and the figures, some of the terminology should be clarified. Please note that the terms and phrases may have additional definitions and/or examples throughout the specification. Where otherwise not specifically defined, words, phrases, and acronyms are given their ordinary meaning in the art. The following paragraphs provide some of the definitions for terms and phrases used herein.

[0064] Adapter Module 100: As shown in Figures 1 and 2, the adapter module 100 (sometimes also herein called the "payment module 100") is a physical device that is installed in a machine 120 (a payment accepting unit 120). The shown adapter module 100 is an in-line dongle (a hardware device with software thereon) device that may be inserted in-line within a multi-drop bus (MDB) of a machine 120. The adapter module 100 bridges the communication between the machine 120 and a mobile device 150. Although described as a unique component, it should be noted that the adapter module 100 could be implemented as a plurality of devices or integrated into other devices (e.g., components of a machine 120). In its unique component form, the adapter module 100 can be easily inserted into a machine 120 so that the machine 120 is able to perform new features with the assistance of the adapter module 100. Figure 20 shows components associated with the adapter module 100. As shown in Figure 20, the communications unit 770 of the adapter module 100 includes short-range communication capability 776 (e.g., Bluetooth mechanisms).The shown example may be divided into multiple

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1489 of 1551

distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g., a computer or a payment accepting unit) as long as the components are associated with each other.

[0065] Mobile Device 150 and Application 140 (also referred to as a "mobile application," "mobile app," or "app"): In general, a mobile device 150 may be a user's personal mobile device 150. The mobile device 150 (with a mobile application 140 thereon) acts as a communication bridge between the adapter module 100 (associated with a payment accepting unit 120) and the server 130. The mobile device 150 and the application 140, however, are not "trusted" in that the communications (transmissions) it passes are encrypted. Encrypted (secured) communications are undecipherable (unencryptable, unreadable, and/or unusable) by the mobile device 150. This keeps the communications passed between the adapter module 100 and the server 130 secured and safe from hacking. Mobile devices include, but are not limited to smart phones, tablet or laptop computers, or personal digital assistants (PDAs), smart cards, or other technology (e.g., a hardware-software combination) known or yet to be discovered that has structure and/or capabilities similar to the mobile devices described herein. The mobile device 150 preferably has an application (e.g., the application 140) running on it. The term "app" is used broadly to include any software program(s) capable of implementing the features described herein. Figures 10A-10D show user interfaces for the application 140 displayed by the mobile device 150. It should be noted that the phrase "mobile device" can be assumed to include the relevant app unless specifically stated otherwise. Similarly, it should be noted that an "app" can be assumed to be running on an associated mobile device unless specifically stated otherwise. Figure 21 shows components associated with the mobile device 150. The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g., the cell phone itself) as long as the components are associated with each other.

[0066] Payment accepting unit 120 (or Machine 120): A payment accepting unit 120 (or the machine 120) is equipment that requires payment for the dispensing of an product and/or service. Payment accepting units 120 may be vending machines, parking meters, toll booths, laundromat washers and dryers, arcade games, kiosks, photo booths, toll booths, transit ticket dispensing machines, and other known or yet to be discovered payment accepting units 120. Some payment accepting units 120 can accept cashless payments (payments other than cash

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1490 of 1551

(paper currency and coins)) by accepting payment from, for example, credit cards, debit cards, and mobile devices.

[0067] Network Connections: For purposes of this discussion, a persistent network connection is a wired or wireless communications connection that is ongoing (e.g., a dedicated connection, a dedicated online connection, and/or a hardwired connection) or accessible on demand (e.g., the ability for the machine to make a temporary connection to a server or the ability for the user to contact a server from his mobile device). Typically the persistent network connection has been conducted over "long-range communication technology" or "long-range communication protocol" (e.g., hardwired, telephone network technology, cellular technology (e.g., GSM, CDMA, or the like), Wi-Fi technology, wide area network (WAN), local area network (LAN), or any wired or wireless communication technology over the Internet that is known or yet to be discovered). Traditionally, machines that accept payment other than cash require a persistent (ongoing or accessible on demand) connection to a network to facilitate payment. This is true for machines that accept, for example, credit cards and debit cards. The payment accepting units 120 described herein do not require a traditional persistent network connection. The user's mobile device 150 acts as a communication bridge between the adapter module 100 and the server 130. Communications between user mobile devices 150 and the servers (e.g., a system management server 130 and/or a funding source server 160) take place using long-range communication technology. Communications between user mobile devices 150 and the adapter module 100 of the payment accepting unit 120 take place using "short-range communication technology" or "short-range communication protocol" (e.g., Bluetooth (such as Bluetooth 4.0, Bluetooth Smart, Bluetooth Low Energy (BLE)), near-field communication (NFC), Ultra Wideband (UWB), radio frequency identification (RFID), infrared wireless, induction wireless, or any wired or wireless technology that could be used to communicate a small distance (approximately a hundred feet or closer) that is known or yet to be discovered). Therefore, neither the adapter module 100 nor the payment accepting unit 120 requires a traditional persistent long-range wireless network connection. The communications technology shown in the figures may be replaced with alternative like communications technology and, therefore, specific shown communications technologies are not meant to be limiting. For example, Wi-Fi technology could be replaced with another long-range communication technology.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1491 of 1551

[0068] Server: A server is the host processing server that may be operated by the company running the payment processing system. For each user, the server 130 preferably maintains at least one "virtual wallet" having at least one "balance" (which can be $0) of designated funds for which the server 130 keeps an accounting. The balance may represent, for example, "cash" or it may be a "promotional value" that represents funds that may be spent under certain circumstances. If these funds begin to be depleted, the user may be notified (e.g., via the application 140 on the mobile device 150) that additional funds need to be designated and/or transferred. Alternatively, funds from other sources (e.g., the funding source server 160) may be automatically transferred to restore a predetermined balance. The balance may also be increased based on a promotion (e.g., points earned or coupons). As shown in Figure 22, the server includes appropriate processors 950, memory 960 (which would keep an accounting of the user's balance in a manner similar to a gift card), and communication systems 970. As shown in Figure 22, the communications unit 970 of the server 130 includes long-range communication capability 972 (e.g., cellular technology and/or Wi-Fi mechanisms). The server 130 also includes a security unit 955 for encrypting and decrypting messages. The server 130 receives an authorization request (sometimes also herein called an "AuthRequest") from the adapter module 100 (via a mobile device 150) and, if funds are available, returns an authorization grant (sometimes also herein called an "AuthGrant" or an "authorization grant token") for funds. Figure 22 shows components associated with the server 130. The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g., a computer or a main frame) as long as the components are associated with each other.

[0069] Advertise Presence: Each adapter module 100 advertises its presence by broadcasting signals (advertising broadcast signals) to mobile devices in the zones 102, 104, 106. Each adapter module 100 can listen to other adapter modules' advertisements.

[0070] Received Signal Strength Indicator (RSSI): The adapter module 100 may have a self-calibrating signal strength to determine zone thresholds (e.g., a payment zone threshold and an authentication zone threshold). At the time the user selects an item (product or service) from the payment accepting unit 120, the Received Signal Strength Indicator (RSSI) is logged. At this moment, it is presumed the user is within "arm's-length" (which may be a predetermined length approximating the distance of a user standing in front of a machine for the purpose of making a

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1492 of 1551

purchase) from the payment accepting unit 120. A mathematical computation (i.e., In-Range Heuristics) is conducted to derive the optimal RSSI threshold at which point payment should be triggered by an application 140 on a mobile device 150. The threshold may be payment accepting unit specific and can vary over a period of time. This optimal zone threshold is preferably reported to the mobile device 150 during an initial handshake.

[0071] In-Range Heuristics: A mathematical computation that determines the RSSI threshold to determine when a user is in the authorization zone 104 and/or the payment zone 102. This computation can take into consideration numerous historical data points as well as transaction specific information such as which the mobile device 150 is being used, payment accepting unit type, among other factors. Preferably the RSSI is logged while the user is making his selection (this is the one time in the entire process that the user definitely will be "in range" (e.g., they will be arm's length from the machine 120 because they are physically interacting with the machine 120). The type of user mobile device 150, accelerometer data (e.g., is the user moving or stationary), and/or other information may also be logged while the user is making his selection. The adapter module 100 can give a reference RSSI for the payment zone 102 for the machine 120, and the application 140 can make a +/- adjustment based on the specific mobile device 150 on which it is installed. Over a period of time, the payment processing system continues to improve itself based on additional data points.

[0072] Authorization Request ("AuthRequest:): When a user enters the authorization zone 104, the mobile device 150 notifies the adapter module 100 and the adapter module 100 sends a secured authorization request (e.g., the encrypted authorization request) as a "message" (also referred to as a communication or transmissions) to the server 130 via the mobile device 150. Encryption may be performed by a security unit 755 (Figure 20) with security technology (e.g., encryption and decryption means) that may be associated with the processing unit 750 and/or the memory 760. Significantly, the AuthRequest is a request for authorization of funds, not a request for authorization of a transaction. The purpose of the funds is irrelevant to the server 130.

[0073] Authorization Grant Token ("AuthGrant"): This is a "message" (also referred to as a communication or transmissions) encrypted by the security unit 955 (Figure 22) with security technology (e.g., encryption and decryption means) of the server 130 with the unique

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1493 of 1551

private key corresponding to the adapter module 100. The secured authorization grant (e.g., the encrypted authorization grant) is passed from the server 130 to the adapter module 100 via the mobile device 150 in the form of a message. The mobile device 150, however, is not able to decrypt and/or read the message. The authorization grant is in response to the authorization request. The amount of the funds granted by the AuthGrant may be determined by factors including, but not limited to, the amount of funds available (or, if funds are not available, a mini-loan could be granted), a pre-authorized amount (e.g., set by the server, set by the user during set-up, set by the funding source, or a standard amount), limited by time (e.g., only a certain amount per hour, or a predetermined amount at specific times of the day), limited to the maximum amount of an item on the machine (or enough for two or three items in the machine), or one or more of these and other factors. Significantly, the AuthGrant makes the funds available, but does not authorize a transaction. The AuthGrant may have an associated expiration period in that it may expire if it is not used in a pre-determined time period. The length of time before the AuthGrant expires may be determined by factors including, but not limited to, the trustworthiness of the user (e.g., the user has a long history with the payment processing system or some known provider (e.g., credit card provider, bank, or credit union), the user has a good credit rating, or the user has a large wallet balance), a pre-authorized time period (e.g., set by the server, set by the user during set-up, set by the funding source, or a standard time period), limited by time (e.g., predetermined time periods at specific times of the day such as longer times during breakfast, lunch, and dinner), limited by the machine or the products or services sold in the machine, limited by the number of other users near the machine (e.g., if it is a crowded machine, the AuthGrant may expire faster), or one or more of these and other factors. The AuthGrant remains valid until it expires or some other event occurs to end its validity (e.g., the user cancels it). This means that under normal circumstances the mobile device 150 will hold the AuthGrant authorizing use of funds for a pre-determined time period that will allow the user sufficient time to make a purchase. The authorized amount may be considered to be the "wallet balance" that is held in a virtual "wallet."

[0074] Synchronization: Time may be synchronized to the adapter module 100 from the server 130. The server 130 sends time information with encrypted messages and the adapter module 100 uses the time encoded in the messages for synchronization.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1494 of 1551

[0075] The mobile-device-to-machine payment processing system and components thereof may have associated hardware, software, and/or firmware (a variation, subset, or hybrid of hardware and/or software). The term "hardware" includes at least one "processing unit," "processor," "computer," "programmable apparatus," and/or other known or yet to be discovered technology capable of executing instructions or steps (shown as the processing unit 750 in Figure 20, the processing unit 850 in Figure 21, and the processing unit 950 in Figure 22). The term "software" includes at least one "program," "subprogram," "series of instructions," or other known or yet to be discovered hardware instructions or hardware-readable program code. Software may be loaded onto hardware (or firmware) to produce a "machine," such that the software executes on the hardware to create structures for implementing the functions described herein. Further, the software may be loaded onto the hardware (or firmware) so as to direct the mobile-device-to-machine payment processing system (and components thereof) to function in a particular manner described herein or to perform a series of operational steps as described herein. "Hardware" such as the adapter module 100, the mobile device 150, and the payment accepting unit 120 may have software (e.g., programs and apps) loaded thereon. The phrase "loaded onto the hardware" also includes being loaded into memory (shown as the memory 760 in Figure 20, the memory 860 in Figure 21, and the memory 960 in Figure 22) associated with or accessible by the hardware. The term "memory" is defined to include any type of hardware (or other technology) -readable media (also referred to as computer-readable storage medium) including, but not limited to, attached storage media (e.g., hard disk drives, network disk drives, servers), internal storage media (e.g., RAM, ROM, EPROM, FLASH-EPROM, or any other memory chip or cartridge), removable storage media (e.g., CDs, DVDs, flash drives, memory cards, floppy disks, flexible disks), firmware, and/or other known or yet to be discovered storage media. Depending on its purpose, the memory may be transitory and/or non-transitory. Appropriate "messages," "communications," "signals," and/or "transmissions" (that includes various types of information and/or instructions including, but not limited to, data, commands, bits, symbols, voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, and/or any combination thereof) over appropriate "communication paths," "transmission paths," and other means for signal transmission including any type of connection between two elements on the payment processing system (e.g., the adapter module 100, the mobile device 150, the

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1495 of 1551

payment accepting unit 120, hardware systems and subsystems, and memory) would be used as appropriate to facilitate controls and communications.

[0076] It should be noted that the terms "programs" and "subprograms" are defined as a series of instructions that may be implemented as software (i.e. computer program instructions or computer-readable program code) that may be loaded onto a computer to produce a "machine," such that the instructions that execute on the computer create structures for implementing the functions described herein or shown in the figures. Further, these programs and subprograms may be loaded onto a computer so that they can direct the computer to function in a particular manner, such that the instructions produce an article of manufacture including instruction structures that implement the function specified in the flow chart block or blocks. The programs and subprograms may also be loaded onto a computer to cause a series of operational steps to be performed on or by the computer to produce a computer implemented process such that the instructions that execute on the computer provide steps for implementing the functions specified in the flow chart block or blocks. The phrase "loaded onto a computer" also includes being loaded into the memory of the computer or a memory associated with or accessible by the computer. Separate, albeit interacting, programs and subprograms may be associated with the adapter modules 100, the server 130, and the mobile device 150 (including the mobile application 140) and these programs and subprograms may be divided into smaller subprograms to perform specific functions.

[0077] The terms "messages," "communications," "signals," and/or "transmissions" include various types of information and/or instructions including, but not limited to, data, commands, bits, symbols, voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, and/or any combination thereof. Appropriate technology may be used to implement the "communications," "signals," and/or "transmissions" including, for example, transmitters, receivers, and transceivers. "Communications," "signals," and/or "transmissions" described herein would use appropriate technology for their intended purpose. For example, hard-wired communications (e.g., wired serial communications) would use technology appropriate for hard-wired communications, short-range communications (e.g., Bluetooth) would use technology appropriate for close communications, and long-range communications (e.g., GSM, CDMA, Wi-Fi, or the like) would use technology appropriate for remote communications over a distance. Appropriate security (e.g., SSL or TLS) for each type of communication is

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1496 of 1551

included herein. The security units 755 and 955 include technology for securing messages. The security technology may be, for example, encryption/decryption technology (e.g., software or hardware). Although encryption/decryption is discussed primarily as being performed using a unique private key, alternative strategies include, but are not limited to encryption/decryption performed using public/private keys (i.e., asymmetric cryptography), or other encryption/decryption strategies known or yet to be discovered. Appropriate input mechanisms and/or output mechanisms, even if not specifically described, are considered to be part of the technology described herein. The communications unit 770 (shown in Figure 20) of the adapter module 100 is shown as including appropriate input and output mechanisms 772, 774 that may be implemented in association (e.g., directly or indirectly in functional communication) with male and female adapters 720, 730 of the adapter module 100. The communications unit 870 (shown in Figure 21) of the mobile device 150 includes mechanisms for both long-range communications (shown as the long-range communication capability 872 such as cellular and/or Wi-Fi mechanisms) for communicating with the server 130 and short-range communications (shown as the short-range communication capability 876 such as Bluetooth mechanisms) for communicating with the adapter module 100.

[0078] When used in relation to "communications," "signals," and/or "transmissions," the terms "provide" and "providing" (and variations thereof) are meant to include standard means of provision including "transmit" and "transmitting," but can also be used for non-traditional provisions as long as the "communications," "signals," and/or "transmissions" are "received" (that can also mean obtained). The terms "transmit" and "transmitting" (and variations thereof) are meant to include standard means of transmission, but can also be used for non-traditional transmissions as long as the "communications," "signals," and/or "transmissions" are "sent." The terms "receive" and "receiving" (and variations thereof) are meant to include standard means of reception, but can also be used for non-traditional methods of obtaining as long as the "communications," "signals," and/or "transmissions" are "obtained."

[0079] The term "associated" is defined to mean integral or original, retrofitted, attached, connected (including functionally connected), positioned near, and/or accessible by. For example, if the user interface (e.g., a traditional display 122 (Figure 19), a touch screen display 124 (Figure 19), a key pad 126 (Figure 19), buttons 126 (Figure 19, shown as part of the key pad 126), a keyboard (not shown), and/or other input or output mechanism) is associated with a

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1497 of 1551

payment accepting unit 120, the user interface may be original to the payment accepting unit 120, retrofitted into the payment accepting unit 120, attached to the payment accepting unit 120, and/or a nearby the payment accepting unit 120. Similarly, adapter modules 100 may be associated with payment accepting units 120 in that the adapter modules 100 may be original to the payment accepting unit 120, retrofitted into the payment accepting unit 120, attached to the payment accepting unit 120, and/or a nearby the payment accepting unit 120.

SYSTEM OVERVIEW

[0080] Figures 5, 6, and 7 together show major components of the mobile-device-to-machine payment system and the interactions there-between.

[0081] As shown, the adapter module 100 functionally connected bi-directionally to the payment accepting unit 120 via a wired serial connection such that no security is necessary. The adapter module 100 is also functionally connected bi-directionally to the mobile device 150 (and its installed mobile application 140) via short-range communication technology (e.g., a Bluetooth connection). Because the mobile device 150 is not a "trusted" link (e.g., it could be hacked by a user), only secured communications (transmissions) are passed between the adapter module 100 and the mobile device 150. This keeps communications secured and safe from hacking. The mobile device 150 (and its installed mobile application 140) is also functionally connected bi-directionally to a system management server 130 and/or a funding source server 160 via long-range communication technology (e.g., Wi-Fi or Cellular connection) that preferably has appropriate security (e.g., SSL security). Security between the mobile device 150 and the system management server 130 has the advantage of protecting communications from the mobile device 150 to the system management server 130 that may include sensitive data and may not be encrypted. The system management server 130 and the funding source server 160 may be connected via a wired Internet connection with SSL security. The system management server 130 may be connected via a wired Internet connection with SSL security to an operators' server 170. Although not necessary to implement a purchase transaction, for other purposes (e.g., inventory), the operators' server 170 may be connected to the payment accepting unit 120 using a handheld computer sync or a cellular connection.

[0082] Also, a unique private key may be used to securely transmit encrypted messages between the adapter module 100 and the system management server 130 (although the encrypted

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1498 of 1551

transmissions would most likely be routed through the mobile device 150). The server 130 stores a private key for each adapter module 100, and this key is only known to the adapter module 100 and the server 130. No intermediary is privy to this key (especially not the mobile device 150). When the adapter module 100 and the server 130 communicate messages (e.g., AuthRequest and AuthGrant), the security unit 755 of the adapter module 100 encrypts the message with its private key and passes the message to the mobile device 150. The mobile device 150 (which preferably cannot decrypt the message) passes the encrypted message to the server 130. The server 130 is able to decrypt the message using the security unit 955 of the adapter module 100 and the unique private key. The security unit 955 of the server 130 uses this same unique private key to encrypt messages to the adapter module 100 and sends the message to the mobile device 150 to relay to the adapter module 100 that is able to decrypt the message using the security unit 755 of the adapter module 100 and the unique private key.

[0083] Figure 7 shows specific communications and messaging with a vending sequence (the numbers to the left of the communications and messaging) between the adapter module 100, the mobile device 150, and the system management server 130. These communications are discussed in more detail in the discussion pertaining to the schematic flow diagrams (Figures 8A-8G) and the flow charts (Figures 9A-9E).

[0084] It should be noted that Figures 5, 6, and 7 are examples, and are meant to help in the understanding of the mobile-device-to-machine payment system. For example, the shown long-range communications technology may be replaced with alternative long-range communications technology known or yet to be discovered, the shown short-range communication technology may be replaced with alternative short-range communication technology known or yet to be discovered, and the shown security may be replaced with alternative security known or yet to be discovered. The shown connections are meant to be examples, and there may be intermediaries that are not shown. The shown components have been simplified in that, for example, only one mobile device 150 (or machine 120, adapter module 100, or server 130) is shown where many may be included. Finally, the order of the steps may be changed and some steps may be eliminated.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1499 of 1551

ADAPTER MODULE

[0085] Figures 11-18 show views of adapter module 100a (referred to generally as adapter module 100). Adapter module 100 is a relatively low cost hardware component that is pre-configured to work with the industry standard multi-drop bus (MDB). On machines without MDB technology, the adapter module 100 can be configured or designed to work with other serial protocols or activate a switch. In essence the adapter module 100 simulates establishing payment on payment accepting unit 120 in much the same manner as other alternative forms of payment (e.g., cash).

[0086] The shown adapter modules 100 are preferably designed to be used as an in-line dongle for in-line insertion within, for example, a MDB of a machine 120. The wire used in MDB technology uses male and female connection ends or adapters to allow the attachment of peripherals. In the case of a vending machine, the wire with the connection ends or adapters would be present to allow the attachment of a payment receiving mechanism (e.g., a coin mechanism). The MDB male and female adapters 700, 710 may be separated (as shown in Figures 17-18). The adapter module 100a in Figures 11 and 17-18 has a male adapter 720 and a female adapter 730. The adapter module 100a may be plugged (inserted) in serial ("in-line") with the wire. For example, the MDB female adapter 710 may be connected to the male adapter 720 of the adapter module 100 and the MDB male adapter 700 may be connected to the female adapter 730 of the adapter module 100. The resulting in-line configuration is shown in Figure 19. It should be noted that the adapter modules 100 are designed to allow pass-through communications so that if the mobile-device-to-machine payment processing system is not enabled (e.g., for a particular purchase or simply turned off) the MDB functions as though the adapter module 100 is not there and the machine 120 can function normally.

Draft Only

HANDS-FREE MODE

[0087] Summarily, if it is available, a hands-free mode, from the user's perspective, would allow the user to approach a favorite payment accepting unit 120 and notice that the display (e.g., the displays 122 or 124 shown in Figure 19) associated with the payment accepting unit 120 shows funds available (e.g., the wallet balance), he would select the product or service using input mechanisms (e.g., buttons 126 or a touch screen display 124 shown in Figure 19)

CSC ServiceWorks - Ex. 1002
Page 1500 of 1551

associated with the payment accepting unit 120, and he would retrieve his dispensed services or products.

[0088] During an initial handshake with the mobile device 150 (when the user is within range), the adapter module 100 reports to the mobile device 150 whether or not hands-free mode is available. If it is available, the installed mobile application 140 automatically connects to the payment accepting unit 120 without the user having to interact with the mobile device 150. The user observes that funds are available on the display 122, 124 of the payment accepting unit 120 and completes the purchase transaction as if cash was inserted in the machine 120 by inputting his selection on the payment accepting unit 120. The payment accepting unit 120 dispenses the product or service. After the selection is made, the change is returned to the mobile device 150.

[0089] Whether hands-free payment is available is determined by factors including, but not limited to whether if other mobile devices 150 are in range, if other adapter modules 100 are in range, if there are any alerts, if the payment trigger threshold is having wide variances and so deemed unstable, or if the payment accepting unit operator (e.g., a vending machine operator) has opted to disable hands-free mode for the payment accepting unit 120. In the latter instance, operators can disable via a maintenance mobile device 150, as well as through the operators' server 170 and/or the system management server 130.

[0090] Figure 3 is a table that shows considerations, conditions, or factors that may be used to determine whether the hands-free pay feature is available. Starting at the "Favorite?" column, this indicates whether the payment accepting unit 120 is a favorite machine. Preferably the hands-free pay feature is only available for use with "favorite" payment accepting units 120 (e.g., a vending machine at work or school). The "Alert" column has to do with whether there is some reason (e.g., there are too many users in range) that the hands-free pay feature should not work and, if there is such a reason, the user will be notified (alerted) and may be able to use the manual mode to resolve the alert and/or complete the transaction. Figure 3 shows situations in which a user is or is not able to make hands-free purchases from a machine 120 using a mobile application 140 on his mobile device 150. It should be noted that the shown interface is an example. For example, some of the features could be automated or pre-selected. (It should be noted that the left hand column, the "Tab" column, relates to whether the selected tab on the mobile application 140 is "all" or "favorite." Figures 10A-10D all show these tabs. Unlike the

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1501 of 1551

other columns in Figure 3, this column has more to do with the functionality and view of the application 140 than specifically with the hands-free feature. The tabs would allow a user to select whether he wanted to be alerted when he was in range of all payment accepting units 120 or just "favorite" payment accepting units 120 and the application 140 would show the appropriate view.)

[0091] Balance Display: An optional feature of the mobile-device-to-machine payment system that is particularly helpful in the hands-free mode (although it may be available in the manual mode and/or in a multiple-vend scenarios) is when the user's mobile device 150 sends "credit" to the payment accepting unit 120 (either via hands-free payment or through a manual swipe), the wallet balance is sent to the payment accepting unit 120 that is then displayed to the user on a display 122, 124 of the machine 120. This is particularly beneficial during hands-free mode when the user does not retrieve the mobile device 150 and, therefore, may not know the balance. Also, in a multiple-vend scenario the user would not have to calculate a remaining balance.

[0092] An example of a hands-free, multiple-vend scenario where a balance is displayed by the payment accepting unit 120, follows: The user has $5.00 in his/her virtual wallet as that is the amount that has been authorized (the AuthGrant being stored on the mobile device 150). The user walks up to the payment accepting unit 120 and $5.00 is displayed on the display 122, 124 of the payment accepting unit 120 since hands-free mode was enabled and credit was sent (e.g., via the short-range communication capability) to the payment accepting unit 120. The user makes a selection of $1.50 by interacting (e.g., pressing buttons) with the machine 120. The item (product or service) is dispensed and the "change" is "returned" (e.g., via the short-range communication capability) to the virtual wallet. But since the user is still standing in the payment zone 102, the remaining wallet balance of $3.50 is sent to the payment accepting unit 120 and displayed so that the user can now see that he/she has a $3.50 balance. (It should be noted that the authorized funds may remain on the machine 120 and not be transferred back to the mobile device 150 between transactions.) The user decides to purchase a $1.50 item, and the transaction is completed as usual (e.g., by interacting with the machine 120). Now the user is still standing in the payment zone 102 and he/she sees the wallet balance of $2.00 on the display 122, 124 of the payment accepting unit 120. The user decides that he/she does not wish to purchase anything else and simply walks away. As he/she walks out of the payment zone 102, the credit is cleared from

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1502 of 1551

the machine 120, but he/she is left with the knowledge that his wallet balance is $2.00 even though he/she never touched the mobile device 150. Communications between the payment accepting unit 120 and the adapter module 100 (via the mobile device 150) handle the accounting incidental to the transaction. The remaining balance ($2.00) is technically stored on the server 130, and may be reflected on the application 140 on the mobile device 150.

MULTIPLE DISTINCT ZONES

[0093] As shown in Figures 1-2, the functions performed by the adapter module 100 can be divided into distinct zones: a first "communication zone" (e.g., "Bluetooth range" 106), a second "authorization zone" 104, and a third "payment zone" 102. The payment zone 102 is smaller than or equal to (overlapping completely) the authorization zone 104. Put another way, the payment zone 102 is within or coextensive with the authorization zone 104. The payment zone 102 is a subset of the authorization zone 104 with a ratio of the payment zone 102 to the authorization zone 104 ranging from 0.01:1 to 1:1. It is not necessarily a fixed ratio and can vary between different payment accepting units 120, different mobile devices 150, different users, and over time. While the zones 102, 104, 106 are depicted as having a uniform shape, the zones may not necessarily be uniform (or constant over time) in that the shape can vary. For example, the shape of the Bluetooth range 106 may vary depending on environmental conditions such as obstacles in the room and payment accepting unit 120 door/wall materials.

[0094] Bluetooth Range 106 (sometimes also herein called the "communication zone"): The outermost range is the Bluetooth range 106 (shown in Figures 1-2). This is the area in which the adapter module 100 is able to broadcast its presence. In most situations, the Bluetooth range 106 is a passive range in that no actual data is exchanged between the mobile device 150 and the adapter module 100. While in the Bluetooth range 106, the mobile device 150 monitors the RSSI (Received Signal Strength Indicator).

[0095] Authorization Zone 104: The middle region is the authorization zone 104 (shown in Figures 1-2). This is a computed area based on the RSSI. As mentioned, the mobile device 150 monitors the RSSI while it is in the Bluetooth range 106. When the RSSI reaches a certain predetermined threshold based on In-Range Heuristics, the mobile device 150 can be considered to be in the authorization zone 104. In the authorization zone 104 the mobile device 150 establishes a connection to the adapter module 100 (e.g., a Bluetooth connection (Figure 5) with

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1503 of 1551

SSL protection (Figure 6)) and informs the adapter module 100 of its presence. After a successful handshake with the adapter module 100, the mobile device 150 registers the adapter module 100 and the adapter module 100 requests an authorization to the server 130 via the mobile devices' network connection (e.g., a Wi-Fi or cellular connection (Figure 5) with SSL protection (Figure 6)). It is important to note the mobile device 150 and the adapter module 100 have a non-exclusive relationship at this point. The adapter module 100 may collect registrations for all mobile devices 150 that are within the authorization zone 104.

[0096] An authorization occurs in preparation for when the user enters the payment zone 102 (shown in Figures 1-2). An authorization expires in a set period of time (for example, five minutes), so if the mobile device 150 is still in the authorization zone 104 at the time of expiration, the adapter module 100 submits for and receives another authorization. This will continue for a set number of times (for example, the limit may be three times to limit cases of numerous authorizations for a mobile device that may remain in the authorization zone 104 for an extended period of time without completing a transaction). Should authorization fail (for instance if the limit had been reached) prior to the user entering the payment zone 102, the adapter module 100 will request authorization when the mobile device 150 enters the payment zone 102 (which adds a few seconds to the experience).

[0097] Payment Zone 102: As a user enters the payment zone 102, the mobile device 150 establishes exclusive control of the adapter module 100. Once established, any other user in the payment zone 102 is put into a "waiting" status.

[0098] In the payment zone 102, the payment can be triggered automatically if the payment processing system has and is in hands-free mode. In such instances, the mobile device 150 is running the application 140 in background mode and will send credit to the payment accepting unit 120 without any explicit user interaction. The user completes the transaction on the payment accepting unit 120 in much the same manner as if cash had been inserted into the payment accepting unit 120 to establish credit. After the user completes the transaction (that may include one or more purchases), details of the transaction are preferably returned to the mobile device 150 and server 130 in separate messages. The message to the server 130 is preferably encrypted with the adapter module's 100 private key (Figure 6) to ensure data integrity. As shown in Figure 7, the "private key" coded message (Encrypted VendDetails) is preferably sent

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1504 of 1551

via the mobile device 150. The message to the mobile device 150 may be sent solely for the purpose of closing the transaction. The transaction history and balance are updated server-side via the encrypted message sent to the server 130.

[0099] The other mode of operation is manual mode. In manual mode, the user launches the mobile device 150 and is able to swipe to send payment to the payment accepting unit 120. The user can also swipe back to cancel the payment. Like in hands-free mode, the purchase transaction is completed on the payment accepting unit 120 in the same manner as if cash were inserted into the payment accepting unit 120. The mobile device 150 is only used to send payment. Selection is made directly on the payment accepting unit 120.

[00100] Self-Calibrating Zone Threshold: A key, but optional feature, of the payment processing system is a self-calibrating payment zone RSSI threshold. Because RSSI can vary machine to machine, environment to environment, and device to device, having a fixed threshold at which payment is triggered can be problematic. The approach suggested herein is the creation of a self-calibrating threshold. When the user is interacting with the payment accepting unit 120 (such as when he makes his selection on the payment accepting unit 120), the payment accepting unit 120 notifies the adapter module 100 and the adapter module 100 logs the conditions such as RSSI, type of user mobile device 150, accelerometer data, and other information. It is at this point that it can be ascertained safely that the user is within arm's-length from the payment accepting unit 120 (by necessity the user is arm's-length because he is making some physical interaction with the payment accepting unit 120). This is the only point in the entire transaction in which it can be certain that the user is within arm's-length from the payment accepting unit 120.

Draft Only

[00101] Figure 4 shows a simplified set of steps involved when users enter the payment zone 102. Specifically, Figure 4 shows that credit is established 200 (this may have been done in the authorization zone 104, but if not it would be handled in the payment zone 102), that the user makes a selection using the machine 202, that the machine notifies the adapter module of the selection 204, that the adapter module (optionally) logs the RSSI 206, and that the purchase process(es) continues 208. Using the historically logged RSSI data, the adapter module 100 calculates one of several "average" RSSI using various mathematical models. This "average" could be a traditional average, a moving average, a weighted average, a median, or other similar

CSC ServiceWorks - Ex. 1002
Page 1505 of 1551

summary function. The adapter module 100 could pre-process the historical data before running the function, such as to eliminate top and bottom data points, suspect data points, etc.

[00102] Optionally, during the handshake between the mobile device 150 and the adapter module 100, the information transmitted to the adapter module 100 may include, for example, the model of the mobile device 150. Using the received information pertaining to the mobile device models, the adapter module 100 can create multiple payment thresholds, one for each mobile device model. This allows for variances that may be inherent in different types of Bluetooth radios. An alternative to this method is for the adapter module 100 to broadcast a baseline payment zone threshold, and the mobile device 150 can use an offset from this baseline based on its specific model type. The payment zone thresholds (or baseline offsets) can be unique to specific types of mobile devices (e.g., by manufacturer, operating system, or component parts), models of mobile devices, or individual mobile devices (unique to each user).

[00103] In a typical scenario in which the payment zone threshold has been calibrated, the adapter module 100 advertises its presence along with the threshold at which it considers any mobile device 150 to be in the authorization zone 104. This is a one-way communication from adapter module 100 to mobile device 150. Once the mobile device 150 enters the authorization zone 104, there is a handshake that is established between the adapter module 100 and the mobile device 150. During this handshake, the mobile device 150 can share its model information with the adapter module 100, and the adapter module 100 can return the payment zone 102 threshold for that specific model.

[00104] Optionally, in addition to calibrating the payment zone threshold, the adapter module 100 can apply the self-calibrating model to the authorization zone 104 to calibrate the authorization zone threshold. As with the payment zone thresholds, the authorization zone thresholds can be unique to specific types of mobile devices, models of mobile devices, or individual mobile devices. In this scenario, the adapter module 100 would broadcast multiple thresholds by device type and the mobile device 150 would determine which threshold to apply (or alternatively broadcast a baseline and the mobile device 150 uses an offset based on its device model). Even in this scenario, the authorization zone 104 is a one-way communication.

[00105] Optionally, along with the threshold that is calculated (in the payment and/or the authorization zone(s)), a safety margin can be added to minimize scenarios in which a user is

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1506 of 1551

within range, but the mobile-device-to-machine payment processing system does not recognize it because the threshold may not have been reached. For example, if the calculated RSSI for an iPhone™ 5 on machine 4567 is -68 db, the mobile-device-to-machine payment processing system may add a safety margin of -5 db, and establish the threshold at -73 db. So when a user's phone is communicating with the adapter module 100 at an RSSI of -73 db or better, the mobile-device-to-machine payment processing system will allow the mobile device 150 to credit the payment accepting unit 120. The safety margin can be set on the server 130 and downloaded to the adapter module 100, or set on the mobile device 150, or set on the adapter module 100 itself.

[00106] Optionally, in the payment zone threshold, the mobile device 150 can use other data to determine when to cancel the exclusive control of the payment accepting unit 120, to identify when the user is moving out of the payment zone 102. External data could include accelerometer data from the mobile device 150. Using that data, the mobile device 150 can determine whether the user is standing relatively still in front of the payment accepting unit 120, or if the user is in motion – effectively walking away from the payment accepting unit 120.

SIGNAL UNAVAILABILITY ADAPTATION

[00107] The mobile-device-to-machine payment processing system described herein uses a mobile device's 150 short-range communication technology (e.g., Bluetooth mechanisms) (shown as short-range communication capability 876 in Figure 21) and a mobile device's 150 long-range communications technology (e.g., cellular and/or Wi-Fi mechanisms) (shown as long-range communication capability 872 in Figure 21). The short-range communication capability 876 communicates with the adapter module's 100 short-range communication technology (e.g., Bluetooth mechanisms) (shown as short-range communication capability 776 in Figure 20). The long-range communication capability 872 communicates with the server's 130 long-range communications technology (e.g., cellular and/or Wi-Fi mechanisms) (shown as long-range communication capability 972 in Figure 22). The mobile device 150 (with a mobile application 140 thereon) acts as a communication bridge between the adapter module 100 (associated with a payment accepting unit 120) and the server 130. This process is described herein and works properly if there is cellular or Wi-Fi coverage within the payment zone 102.

[00108] One option if there is no cellular or Wi-Fi coverage within the payment zone 102 is to determine whether there is cellular or Wi-Fi coverage within the authorization zone 104 or

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1507 of 1551

the Bluetooth range 106. If there is, then the sizes of the zones 102, 104, 106 could be adapted and the timing could be adapted. For example, if the mobile devices 150 detected problems with the cellular or Wi-Fi coverage within the payment zone 102, the user could carry his mobile device 150 into the other zones (or the mobile device 150 could use short-range communication technology to communicate with other mobile devices 150 within the authorization zone 104 or the Bluetooth range 106) to determine whether the zones have cellular or Wi-Fi coverage. If they do have coverage, communication between the mobile device 150 and the server 130 can be advanced (conducted earlier when the mobile device 150 is further from the machine 120) or delayed (conducted later when the mobile device 150 is further from the machine 120). This can be thought of as changing the size or shapes of the zones 102, 104, 106. The timing would also have to be adjusted so that the authorization of funds (AuthGrant) does not expire before the user has a chance to make a purchase. It also means that balance updates to the server 130 may happen after the user has moved away from the machine 120 and has cellular or Wi-Fi coverage again.

[00109] Another option if there is no cellular or Wi-Fi coverage within any of the zones 102, 104, 106 is for the user to obtain authorization while outside of the zones in a place with cellular or Wi-Fi coverage. This may occur, for example, if a user knows that he will be going to a place with a payment accepting unit 120 equipped with an adapter module 100 (perhaps to a favorite payment accepting unit 120) that does not have (or rarely has) cellular or Wi-Fi coverage. A user may also use the mobile application 140 to query payment accepting units 120 in a given range (e.g., within 50 miles) or at a given location (e.g., at a campground or in a particular remote city) to determine whether there is cellular or Wi-Fi coverage within the zones 102, 104, 106. The user can then obtain pre-authorization from the server 130 using the mobile application 140. Again, the timing would also have to be adjusted so that the authorization of funds (AuthGrant) does not expire before the user has a chance to make a purchase. It also means that balance updates to the server 130 may happen after the user has moved away from the machine 120 and has cellular or Wi-Fi coverage again. A mobile-device-to-machine payment system having the ability to implement this option would be able to accept cashless payments without requiring any network connection near the payment accepting unit 120. In some implementations, the mobile-device-to-machine payment processing systems described herein is

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1508 of 1551

located in a remote location where no signal is available, therefore, can accept cashless payments.

[00110] As an example of a situation in which there might be no cellular or Wi-Fi coverage within any of the zones 102, 104, 106 of a particular payment accepting unit 120, the user (a teenager) may be traveling to a remote location to attend summer camp where there is no cellular or Wi-Fi coverage. The camp may have several payment accepting units 120 (e.g., a machine that creates a dedicated "hot spot" that requires payment for use, vending machines, or machines for renting equipment such as bikes, kayaks, or basketballs). The camp facility might notify parents that the mobile-device-to-machine payment system is available. The parents, while at home, could obtain authorization for a particular amount (that could be doled out a certain amount per day or limited to type of machine or location) to be authorized and "loaded" into the user's mobile device 150 and specify that the authorization will not expire for a certain period or until a certain date. Thereafter, while at camp, the user could use the mobile application 140 on his mobile device 150 in a manner similar to those discussed elsewhere herein. Short-range communications may be used for communications between the adapter modules 100 (associated with the machines 120) and users' mobile devices 150.

[00111] One subtle but powerful component of the payment processing system described herein is that it requires a long-range communication capability (e.g., an Internet or cellular network connection) only in the authorization zone 104 and only for the time period required to send the AuthRequest and receive the AuthGrant. Once a valid AuthGrant is received by the mobile device 150, the long-range communication capability (e.g., an Internet or cellular network connection) is not required by either the mobile device 150 or the adapter module 100 in the payment zone 102 as long as the AuthGrant is valid (unexpired). This mechanism allows the system to seamlessly handle authenticated transactions in (temporary) offline mode, with the deferred acknowledgement and transaction messages performing the bookkeeping and cleanup when network connection is regained. The alternatives described above provide a unique way to artificially extend the authorization zone to include any location where the mobile device 150 can communicate with the server 130.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1509 of 1551

MULTIPLE USER RESOLUTION

[00112] As shown in Figure 2, in one practical scenario, multiple users are in the zones 102, 104, 106. As shown in Figure 2, users 1, 2, and 3 are in the payment zone 102 near the machine 120; users 5 and 6 are shown as positioned between the authorization zone 104 and the Bluetooth range 106; users 4 and 7 are in the Bluetooth range 106, user 10 is positioned on the edge of the Bluetooth range 106; and users 8 and 9 are positioned outside of Bluetooth range 106. In some implementations, the mobile-device-to-machine payment processing system manages and resolves issues pertaining to multiple users.

[00113] Users 4 and 7 are within the Bluetooth range 106 and the user 10 is either entering or leaving the Bluetooth range 106. Within the Bluetooth range 106 the users' mobile devices 150 are able to see the adapter module's 100 advertisement. In this zone, the mobile device 150 preferably does not initiate a connection. The adapter module 100 is preferably unaware of the users in the Bluetooth range 106. All the adapter module 100 is doing is advertising its presence to any multitude of users that may be in Bluetooth range 106.

[00114] The adapter module 100 begins to log users as the users (and their respective mobile devices 150) enter the authorization zone 104 (shown in Figure 2 as users 5 and 6). At this point, there is a non-exclusive connection initiated by the mobile device 150 to the adapter module 100. It does a handshake (e.g., to exchange information needed to obtain authorization and, optionally, to log information needed for a self-calibrating authorization zone threshold) and the mobile device 150 contacts the server 130 for an authorization (e.g., sending an AuthRequest and receiving an AuthGrant). The adapter module 100 registers all mobile devices 150 that have requested and received AuthGrants. The adapter module 100 continues communicating with any other mobile device 150 that enters the authorization zone 104. After initial contact, the adapter module 100 may provide the mobile device 150 with a deferral delay of when to check back in with the adapter module 100 allowing opportunity for other mobile devices 150 to communicate with the adapter module 100.

[00115] If there is only one user in the payment zone 102, a purchase transaction may be performed. If there are multiple users in the payment zone 102, the mobile-device-to-machine payment system must handle the situation.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1510 of 1551

[00116] One optional solution for handling the situation of the multiple users in the payment zone 102 is queuing users in the payment zone 102. Once any mobile device 150 enters the payment zone 102, it establishes exclusivity to a particular mobile device 150 (e.g., in a first-come-first-serve manner). Technically, however, the adapter module 100 is not establishing an exclusive connection to the mobile device 150. The adapter module 100 can still perform a round-robin poll and communicate with and advertise to other mobile devices 150. Instead, the adapter module 100 establishes a queue prioritized by RSSI and time (e.g., who was first and whether the authorization has expired) and it notifies (e.g., alerts) other mobile devices 150 to wait. The earliest valid (unexpired) authorization takes precedence when there is any tie in the RSSI. Otherwise, for example, the strongest average RSSI takes priority. Preferably the queue is not a static measure of the RSSI but an averaged measure over the period of time in the queue. This compensates for a scenario in which a user may be walking around in the queue and then shows up at the payment accepting unit 120 just as the previous user is finishing. If another user was also in the payment zone 102 and stood there the entire time, but may have newer authorization, he could win out.

[00117] Anytime that the adapter module 100 cannot determine exactly which user is in the payment zone 102 in front of the payment accepting unit 120, the adapter module 100 will disable hands-free payment. The mobile device 150 will send an alert to the user and he can use swipe to pay (manual mode). All users in payment zone 102 will show "Connected" and the first to swipe payment to the payment accepting unit 120 then locks out other users.

Draft Only

MULTIPLE MODULE RESOLUTION

[00118] In the scenario where there are multiple modules present, determining which payment accepting unit 120 a user is in front of can be a challenge. In some implementations, the mobile-device-to-machine payment processing system described herein allows adapter modules 100 to communicate to other adapter modules 100 in range via Bluetooth. Each user receives authorization grants for specific payment accepting units 120. This means if there are multiple adapter modules 100 within the same authorization zone 104, there will be multiple authorization grants for the user. When the user enters the payment zone 102, it can be difficult to differentiate which payment accepting unit 120 the user is in front of if the payment zones 102 overlap.

CSC ServiceWorks - Ex. 1002
Page 1511 of 1551

[00119] To solve this problem, when the user enters the payment zone 102, the adapter modules 100 communicate with each other to determine the RSSI for the particular user (based on the signal from his mobile device 150) to triangulate which adapter module 100 (and the associated payment accepting unit 120) is closer to the user. Optionally, the inter-module communications can restrict the user to establishing an exclusive connection with only one payment accepting unit 120.

[00120] Optionally, when the user connects to a payment accepting unit 120, the mobile device 150 can send a communication to the payment accepting unit 120 for momentary display to the user on the display 122, 124 of the payment accepting unit 120. For example, the mobile device 150 can send a communication (e.g., "connected" or "Fred's Mobile Device Connected") to the payment accepting unit's display 122, 124 for a predetermined period of time (e.g., 1-3 seconds) so when the user is in payment zone 102, it is clear which payment accepting unit 120 the user is connected to prior to making a purchase (either in hands-free or manual mode).

[00121] In addition, when the user is in manual mode, the mobile device 150 can display (e.g., on the touch screen 152 as shown in Figures 10A-10D) a visual indication of the payment accepting unit 120 (e.g., a picture and/or a payment accepting unit ID of the payment accepting unit 120) for visual confirmation. If the user is in manual mode, the user can manually change the payment accepting unit 120.

Draft Only

DESCRIPTIVE SCENARIO

[00122] Figure 7, Figures 8A-8G, and 9A-9E (as well as other figures) can be used to understand a detailed scenario of the mobile-device-to-machine payment processing system described herein. A flow of communications and steps are loosely described below with reference to these (and other figures). It should be noted that alternative scenarios could include, for example, a modified order of the steps performed.

[00123] Prior to vending transactions, a user downloads a mobile application 140 onto his mobile device 150, creates an account, and configures a funding source via, for example, a funding source server 160. A funding source may be, for example, a debit card, a credit card, campus cards, rewards points, bank accounts, payment services (e.g., PayPal™) or other payment option or combination of payment options known or yet to be discovered. The funding

CSC ServiceWorks - Ex. 1002
Page 1512 of 1551

sources may be traditional and/or nontraditional payment sources that are integrated into the ecosystem described herein and then used indirectly as a source of funds. Funds from the funding source are preferably held on the server 130 such that when an AuthRequest is received by the server 130, the server 130 can send an AuthGrant authorizing funds for a purchase.

[00124] The user can specify one or more "favorite" adapter module(s) 100 (that has a one-to-one relationship to the payment accepting unit 120) that he may visit regularly, such as a vending machine at school or work. Favorite adapter modules 100 appear on a pre-filtered list and allow for additional rich features such as hands-free payment.

[00125] The payment accepting unit 120 may be equipped with an adapter module 100 that is constantly advertising its availability via Bluetooth (or other "signals," "communications," and/or "transmissions"). This ongoing advertising and scanning for adapter modules is shown in Figure 8A. As shown, the mobile device 150 is continuously scanning for any adapter module 100 within Bluetooth (or other "signal," "communication," and/or "transmission") range. When the user is within range of that adapter module 100, the mobile device 150 tracks and monitors the signal strength until a predetermined "authorization zone" threshold is achieved.

[00126] Figures 8B and 9A generally show that when the authorization zone threshold is reached, the mobile device 150 enters the authorization zone (block 302) and registers the adapter module 100. The mobile device 150 connects to the server 130 (block 304). The application 140 on the mobile device 150 creates a request for authorization (AuthRequest) and passes the AuthRequest to the server 130 using appropriate communication technology (e.g., GSM, CDMA, Wi-Fi, or the like) (block 306). The server 130 responds with an authorization grant (AuthGrant) encrypted with the specific adapter module's private key (block 306). This authorization token may minimally include the User identifier (ID), Apparatus ID (for the adapter module 100), authorization amount, and expiration time. The mobile device 150 receives the AuthGrant from the server 130, and retains it until the mobile device 150 is ready to issue payment to an adapter module 100. The mobile device 150 collects all pending AuthGrants that may be one or more depending on how many adapter modules 100 are in-range. Unused AuthGrants that expire are purged from the mobile device 150 and the server 130. It is important to note that the mobile device 150 is unable to read the AuthGrant because it is encrypted with the adapter module's unique private key that is only known to server 130 and adapter module

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1513 of 1551

100. This provides a preferred key element of security in the system as the adapter module 100 only trusts AuthGrants that are issued by the server 130, and the AuthGrants cannot be read or modified by the mobile device 150 or any other party in between the server and the adapter module 100. Additional mobile devices 150 may enter the authorization zone 104 (block 308).

[00127] As the user approaches a specific adapter module 100, the user enters the payment zone 102 and an event threshold is triggered based on heuristics performed by the mobile device 150. Blocks 310 and 312 show the loop steps of waiting for a mobile device 150 from the authorization zone 104 to enter the payment zone 102. If the user leaves the authorization zone 104 without entering the payment zone 102, the adapter module 100 returns to advertising its presence (block 300).

[00128] Figures 8C and 9B generally show the user entering the payment zone. The mobile device 150 verifies that it has an unexpired and valid AuthGrant. If the AuthGrant is not good, it may be requested again, repeating the Authorization Request process (block 315). If the AuthGrant is good, the mobile device 150 sends the valid AuthGrant (including the wallet balance (block 322)) to the adapter module 100 to initiate a transaction. The mobile device 150 may issue the AuthGrant automatically without specific user interaction if the hands-free mode is supported (and the device is a favorite (block 318), there is only one device in the payment zone 102 (block 318), and (optionally) there is only one user in the authorization zone 104 (block 320). If any of these factors are not present, the mobile device 150 will prompt and/or wait for the user to begin the transaction manually (block 324).

[00129] Figures 8D, 9C, and 9D generally show the transaction process. As shown in Figure 9C, the adapter module 100 runs through a series of questions to determine if there are any issues that would prevent vending including: has the user canceled in-app? (block 326), has the user walked away? (block 328), is the coin return pressed? (block 330), has more than a predetermined period of time elapsed? (block 332). If the answer to any of these questions is "yes," the transaction does not proceed. If the answers to all of these questions is "no," the user makes a selection (block 334) on the payment accepting unit 120 in the same or similar manner as compared to if cash or credit were presented to the payment accepting unit 120. If the machine 120 is able to vend (block 336), it attempts to release the product. If the vend fails (block 338) it is reported by the machine (block 340) and a credit is returned to the virtual wallet (block 342).

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1514 of 1551

If the vend is successful (block 338) it is reported by the machine (block 344). Put another way, after the transaction is complete, the adapter module 100 returns to the mobile device 150 the details of the transaction as well as an encrypted packet containing the vend details to be sent to the server 130 via the mobile device 150. Optionally, the adapter module 100 can pass additional information not directly related to the transaction such as payment accepting unit health, sales data, error codes, etc.

[00130] Figures 8D and 9E generally show the multi-vend function. If the machine has enabled multi-vend capabilities (block 350) and the multi-vend limit has not been reached, the process returns to the question of whether the user is in the payment zone (block 310 of Figure 9A). If the machine does not have enabled multi-vend capabilities (block 350) or the multi-vend limit has been reached, the wallet is decremented by the vend amount(s) and "change" is returned to the virtual wallet (block 354) and the process ends (block 356).

[00131] Figure 8E is a schematic flow diagram of an example login process. Figure 8F is a schematic flow diagram of an example boot-up process. Figure 8G is a schematic flow diagram of an example account check/update process.

[00132] Several of the figures are flow charts (e.g., Figures 9A-9E) illustrating methods and systems. It will be understood that each block of these flow charts, components of all or some of the blocks of these flow charts, and/or combinations of blocks in these flow charts, may be implemented by software (e.g., coding, software, computer program instructions, software programs, subprograms, or other series of computer-executable or processor-executable instructions), by hardware (e.g., processors, memory), by firmware, and/or a combination of these forms. As an example, in the case of software, computer program instructions (computer-readable program code) may be loaded onto a computer to produce a machine, such that the instructions that execute on the computer create structures for implementing the functions specified in the flow chart block or blocks. These computer program instructions may also be stored in a memory that can direct a computer to function in a particular manner, such that the instructions stored in the memory produce an article of manufacture including instruction structures that implement the function specified in the flow chart block or blocks. The computer program instructions may also be loaded onto a computer to cause a series of operational steps to be performed on or by the computer to produce a computer implemented process such that the

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1515 of 1551

instructions that execute on the computer provide steps for implementing the functions specified in the flow chart block or blocks. Accordingly, blocks of the flow charts support combinations of steps, structures, and/or modules for performing the specified functions. It will also be understood that each block of the flow charts, and combinations of blocks in the flow charts, may be divided and/or joined with other blocks of the flow charts without affecting the scope of the invention. This may result, for example, in computer-readable program code being stored in whole on a single memory, or various components of computer-readable program code being stored on more than one memory.

ADDITIONAL IMPLEMENTATIONS

[00133] Figure 23 illustrates a schematic flow diagram of a process 1000 of authenticating a user to perform a transaction in the payment processing system in accordance with some implementations. In some implementations, the payment processing system includes one or more payment modules 100 (e.g., each associated with a respective payment accepting unit 120 such an automatic retailing machine for dispensing goods and/or services), one or more mobile devices 150 (e.g., each executing the application 140 for the payment processing system either as a foreground or background process), and the server 130. The server 130 manages the payment processing system and, in some cases, is associated with an entity that supplies, operates, and/or manufactures the one or more payment modules 100. For brevity, the process 1000 will be described with respect to a respective payment module 100 and a respective mobile device 150 in the payment processing system.

[00134] The payment module 100 broadcasts (1002), via a short-range communication capability (e.g., BLE), a packet of information (sometimes also herein called "advertised information"). The packet of information at least includes an authorization code and an identifier associated with the payment module 100 (module ID). In some implementations, the packet of information further includes a firmware version of the payment module 100 and one or more status flags corresponding to one or more states of the payment module 100 and/or the payment accepting unit 120. The information included in the packet broadcast by the payment module 100 is further discussed below with reference to Figure 24A.

[00135] In some implementations, the payment module 100 sends out a unique authorization code every X seconds (e.g., 100 ms, 200 ms, 500 ms, etc.). In some

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1516 of 1551

implementations, the unique authorization codes are randomly or pseudo-randomly generated numbers. In some implementations, the payment module 100 stores broadcasted authorization codes until a received authorization grant token matches one of the stored authorization codes. In some implementations, the payment module 100 stores broadcasted authorization codes for a predetermined amount of time (e.g., Y minutes) after which time an authorization code expires and is deleted. In some implementations, the authorization code is encrypted with a shared secret key known by the server 130 but unique to the payment module 100. In some implementations, the payment module 100 initializes a random number and then the authorization codes are sequential counts from this random number. In such implementations, the payment module 100 stores the earliest valid (unexpired) counter without a need to store every valid authorization code. In some implementations, the authentication code included in the broadcast packet of information is a hash value of the randomly or pseudo-randomly generated number or the sequential number.

[00136] The mobile device 150 receives the broadcasted packet of information, and the mobile device 150 sends (1004), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), an authorization request to the server 130. For example, an application 140 that is associated with the payment processing system is executing as a foreground or background process on the mobile device 150. In this example, the application 140 receives the broadcasted packet of information when the mobile device 150 is within the communication zone of the payment module 100 (i.e., BLE range) and either automatically sends the authorization request to the server 130 or sends the authorization request to the server 130 when the mobile device 150 is within the authorization zone of the payment module 100. In some implementations, the broadcasted packet of information includes a baseline authorization zone threshold (i.e., an authorization zone criterion) indicating a baseline RSSI that the mobile device 150 (or the application 140) is required to observe before being within the authorization zone of the payment module 100. In some implementations, the mobile device 150 (or the application 140) offsets the baseline authorization zone threshold based on the strength and/or reception of the short-range communication capability (e.g., BLE radio/transceiver) of the mobile device 150. In some implementations, the authorization request at least includes the authorization code which was included in the broadcasted packet of information, an identifier associated with the user of the mobile device 150 or the user account under which the user of the mobile device 150 is

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1517 of 1551

logged into the application 140 (user ID), and the identifier associated with the payment module 100 (module ID). In some implementations, the authentication code included in authorization request is the hash value in cleartext. The authorization request is further discussed below with reference to Figure 24B.

[00137] After receiving the authorization request, the server 130 processes (1006) the authorization request. In some implementations, the server 130 decrypts the authorization code included in the authorization request with the shared secret key corresponding to the payment module 100. In some implementations, the server 130 determines whether the user associated with the user ID in the authorization request has sufficient funds in his/her account for the payment processing system to perform a transaction at the machine 120 that is associated with the payment module 100 corresponding to the module ID in the authorization request.

[00138] The server 130 sends (1008), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), an authorization grant token to the mobile device 150. In some implementations, the server 130 does not send the authorization grant token if the authorization code in the authorization request cannot be decrypted with the shared secret key corresponding to the payment module 100 (e.g., the authorization code is corrupted or hacked). In some implementations, the server 130 does not send the authorization grant token if the user associated with the user ID in the authorization request does not have sufficient funds in his/her account. In some implementations, in addition to the authorization grant token, the server 130 sends a message directly to the mobile device 150 which is not encrypted with the shared secret key corresponding to the payment module 100. After receiving the message, the mobile device 150 displays an appropriate message to the user such as insufficient balance or declined authorization. In some implementations, the server 130 sends an authorization grant token for an amount equal to zero, in which case, the payment module 100 interprets this as a declined or failed authorization which can result for any number of reasons including, but not limited to, insufficient balance or credit.

[00139] The mobile device 150 receives the authorization grant token, and, subsequently, the mobile device 150 detects (1010) a trigger condition. In some implementations, the mobile device 150 (or the application 140) detects the trigger condition via the hand-free mode (e.g., upon entrance into the payment zone of the payment module 100) or manual mode (e.g.,

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1518 of 1551

interacting with the user interface of the application 140 to initiate a transaction with the payment accepting unit associated with the payment module 100).

[00140] In some implementations, unused authorization grants (e.g., if there was no trigger condition or it expired) are canceled by the mobile device 150 by sending a cancellation message to the server 130 corresponding to the unused authorization grant. In some implementations, the server 130 denies or limits the number of authorization grants sent to the mobile device 150 until it has received transaction information or cancellation of authorization outstanding authorization grants sent to the mobile device 150.

[00141] In response to detecting the trigger condition, the mobile device 150 sends (1012), via a short-range communication capability (e.g., BLE), the authorization grant token to the payment module 100. Subsequently, the machine 120 displays credit to the user (e.g., via one of the displays 122 or 124 shown in Figure 19) and the user interacts with the input mechanisms of the machine 120 (e.g., via the buttons 126 or a touch screen display 124 shown in Figure 19) to purchase products and/or services.

[00142] Figure 24A illustrates a block diagram of a packet 1100 of information broadcast by the payment module 100 (e.g., in step 1002 of the process 1000 in Figure 23) in accordance with some implementations. In some implementations, the packet 1100 at least includes: module ID 1102 and authorization code 1104. In some implementations, the packet 110 additional includes: a firmware version 1106 and one or more status flags 1108.

[00143] In some implementations, the module ID 1102 is a unique identifier corresponding to the payment module 100 (sometimes also herein called the "adapter module 100") that broadcast the packet 1100.

[00144] In some implementations, the authorization code 1104 is a hash value in cleartext. In some implementations, the payment module 100 randomly or pseudo-randomly generates a number or determines a sequential number (*See* step 1002 of process 1000 in Figure 23) and performs a predetermined hash function (e.g., SHA-256) on the number to produce the hash value as the authorization code 1104. In some implementations, the authorization code 1104 is a unique code that is encrypted with a secret encryption key corresponding to the payment module 100. The secret encryption key is shared with the server 130, which enables the server 130 to decrypt the authorization code 1104 and encrypt the authorization grant token but not the mobile

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1519 of 1551

device 150. In some implementations, the encryption between server 130 and payment module 100 is accomplished by two pairs of public/private keys.

[00145] In some implementations, the firmware version information 1106 identifies a current firmware version 1112 of the payment module 100. In some implementations, the firmware version information 1106 also includes update status information 1114 indicating one or more packets received by the payment module 100 to update the firmware or one or more packets needed by the payment module 100 to update the firmware. In some implementations, the one or more status flags 1108 indicate a state of the payment module 100 and/or the payment accepting unit 120 associated with the payment module 100. In some implementations, the one or more status flags 1108 indicate a state of the payment module 100 such upload information indicator 1116 indicating that that the payment module 100 has information to be uploaded to the server 130 (e.g., transaction information for one or more interrupted transactions). In some implementations, upload information indicator 1116 triggers the mobile device 150 to connect to payment module 100 immediately (e.g., if it has interrupted transaction information to be uploaded to the server 130). In some implementations, the one or more status flags 1108 indicate a state of the payment accepting unit 120 including one or more of an error indicator 1118 (e.g., indicating that a bill and/or coin acceptor of the payment accepting unit 120 is experiencing a jam, error code, or malfunction), a currency level indicator 1120 (e.g., indicating that the level of the bill and/or coin acceptor reservoir of the payment accepting unit 120 is full or empty), and/or inventory level(s) indicator 1122 (e.g., indicating that one or more products of the payment accepting unit 120. In some implementations, the one or more status flags 1108 are error codes issued by payment accepting unit 120 over the MDB.

[00146] In some implementations, the zone criteria information 1110 specifies an authorization zone criterion 1124 (e.g., a baseline authorization zone threshold indicating a baseline RSSI that the mobile device 150 (or the application 140) is required to observe before being within the authorization zone of the payment module 100) and/or a payment zone criterion 1126 (e.g., a baseline payment zone threshold indicating a baseline RSSI that the mobile device 150 (or the application 140) is required to observe before being within the payment zone of the payment module 100). In some implementations, the baseline authorization zone threshold and the baseline payment zone threshold are default values determined by the server 130 or stored as variables by the application 140, in which case the authorization zone criterion 1124 and

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1520 of 1551

payment zone criterion 1126 are offsets to compensate for the strength and/or reception of the short-range communication capability (e.g., BLE radio/transceiver) of the payment module 100. Alternatively, zone criteria information 1110 includes a spread between the baseline authorization zone threshold and the baseline payment zone threshold. Thus, the mobile device 150 (or the application 140) determines the baseline authorization zone threshold and the baseline payment zone threshold based on the spread value and a default value for either the baseline authorization zone threshold or the baseline payment zone threshold. For example, the spread indicates -10 db and the default baseline payment zone threshold is -90 db; thus, the baseline authorization zone threshold is -80 db. Continuing with this example, after determining the baseline authorization zone threshold and the baseline payment zone threshold, the mobile device 150 (or the application 140) may further adjust the authorization zone threshold and/or the payment zone threshold based on the strength and/or reception of its short-range communication capability (i.e., BLE radio/transceiver).

[00147] Figure 24B is a block diagram of an authorization request 1130 sent by the mobile device 150 to the server 130 (e.g., in step 1004 of the process 1000 in Figure 23) in accordance with some implementations. In some implementations, the authorization request 1130 at least includes: a module ID 1102, a user ID 1134, and an authorization code 1104.

[00148] In some implementations, the module ID 1102 is a unique identifier corresponding to the payment module 100 that broadcast the 1100 that included the authorization code 1104.

[00149] In some implementations, the user ID 1134 is an identifier associated with the user of the mobile device 150 sending the authorization request 1130 to the server 130. In some implementations, the user ID 1134 is associated with the user account under which the user of the mobile device 150 is logged into the application 140.

[00150] In some implementations, the authorization code 1130 includes the authorization code 1104 included in the packet 1100 of information that was broadcast by the payment module 100.

[00151] Figure 24C is a block diagram of an authorization grant token 1140 sent by the server 130 to the mobile device 150 (e.g., in step 1008 of the process 1000 in Figure 23) in accordance with some implementations. In some implementations, in accordance with a

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1521 of 1551

determination that the authorization code 1136 included in the authorization request 1130 from the mobile device 150 is valid and that the user associated with the mobile device 150 has sufficient funds in his/her account for the payment processing system, the server 130 generates the authorization grant token 1140. In some implementations, the authorization grant token 1140 at least includes: a module ID 1102, a user ID 1134, an authorized amount 1146, (optionally) an expiration period offset 1148, and (optionally) the authorization code 1104.

[00152] In some implementations, the module ID 1102 is a unique identifier corresponding to the payment module 100 that broadcast the packet 1100 that included the authorization code 1104.

[00153] In some implementations, the user ID 1134 is an identifier associated with the user of the mobile device 150 that sent the authorization request 1130 to the server 130.

[00154] In some implementations, the authorized amount 1146 indicates a maximum amount for which the user of the mobile device 150 is authorized for a transaction using the authorization grant token 1140. For example, the authorized amount 1146 is predefined by the user of the mobile device 150 or by the server 130 based on a daily limit or based on the user's total account balance or based on a risk profile of the user correspond to the user ID 1134.

[00155] In some implementations, the expiration period 1148 offset indicates an offset to the amount of time that the payment module 100 holds the authorization grant token 1140 valid for initiation of a transaction with the machine 120 associated with the payment module 100. For example, the expiration period offset 1148 depends on the history and credit of the user of mobile device 150 or a period predefined by the user of mobile device 150.

[00156] In some implementations, the authorization grant token 1140 further includes the authorization code 1104 that was included in the authorization request 1130. In some implementations, when the authorization code 1104 is the hash value, the server 130 encrypts the authorization grant token 1140 including the hashed value with the shared secret encryption key associated with payment module 100. Subsequently, when mobile device 150 sends the authorization grant token 1140 to payment module 100 after detecting a trigger condition, the payment module 100 decrypts the authorization grant token 1140 using the secret key known only to server 130 and payment module 100 (which authenticates the message and the authorization grant), and then matches the hash value included in the decrypted authorization

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1522 of 1551

grant token 1140 to previously broadcast valid (unexpired) hash values (i.e., auth codes) to determine validity of the (which was known only by payment module 100).

[00157] Figure 24D illustrates a block diagram of transaction information 1150 generated by the payment module 100 (e.g., in step 1254 of the process 1250 in Figure 25B) in accordance with some implementations. In some implementations, the transaction information 1150 includes: a transaction ID 1152 for the respective transaction, a module ID 1154, a user ID 1156, (optionally) the authorization code 1158, transaction status information 1160, the transaction amount 1162, and other information 1164.

[00158] In some implementations, the transaction ID 1152 is a unique identifier corresponding to the respective transaction. In some implementations, the transaction ID 1152 is encoded based on or associated with the time and/or date on which and the location at which the respective transaction took place.

[00159] In some implementations, the module ID 1154 is a unique identifier corresponding to the payment module 100 that performed the respective transaction.

[00160] In some implementations, the user ID 1156 is an identifier associated with the user of the mobile device 150 that initiated the respective transaction.

[00161] In some implementations, the authorization code 1158 corresponds to the original authorization code (e.g., auth code 1104, Figures 24 A-24C) and/or authorization grant token (e.g., auth grant token 1140, Figure 24C) that was used to initiate the respective transaction. In some implementations, the authorization code 1156 is encrypted with a unique encryption key corresponding to the payment module 100.

[00162] In some implementations, the transaction status information 1160 includes an indication whether the respective transaction was completed, not-completed, or aborted. For example, the respective transaction is incomplete if a jam occurred at the payment accepting unit 120 and the user did not receive the product associated with the respective transaction. For example, if the user walks away from the payment accepting unit 120 after money was credited for the respective transaction, the respective transaction is aborted. In another example, if respective transaction times out after a predetermined time period because the user failed to select a product at the payment accepting unit 120, the respective transaction is aborted. In

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1523 of 1551

another example, if the user actuates a bill or coin return mechanism of the payment accepting unit 120, the respective transaction is aborted.

[00163] In some implementations, the transaction amount 1162 indicates the amount of the respective transaction or the amount of each of multiple transactions (e.g., in a multi-vend scenario). In some implementations, the transaction amount 1162 is encrypted with a unique encryption key corresponding to the payment module 100.

[00164] In some implementations, the other information 1164 includes other information related to the respective transaction such as the items dispensed by the payment accepting unit 120 and the type of transaction (e.g., coins, bills, credit card, manual mode, hands-free mode, etc.). In some implementations, the other information 1164 includes other information related to the payment module 100 and/or the payment accepting unit 120 associated with the payment module 100. For example, the other information 1164 includes a verification request to the server 130 in order to implement new firmware. In another example, the other information 1164 includes transaction information from one or more previous interrupted transactions. In another example, the other information 1164 includes transaction information for one or more transactions paid via bills and/or coins. In another example, the other information 1164 includes inventory information as to one or more products of the payment accepting unit 120.

[00165] Figure 25A illustrates a schematic flow diagram of a process 1200 for providing a representation of a machine event at a mobile device in accordance with some implementations. In some implementations, the payment processing system includes one or more payment modules 100 (e.g., each associated with a respective payment accepting unit 120 such an automatic retailing machine for dispensing goods and/or services), one or more mobile devices 150 (e.g., each executing the application 140 for the payment processing system either as a foreground or background process), and the server 130. The server 130 manages the payment processing system and, in some cases, supplies, operates, and/or manufactures the one or more payment modules 100. For brevity, the process 1200 will be described with respect to a respective payment module 100 associated with a respective payment accepting unit 120 (sometimes also herein called the "machine 120") and a respective mobile device 150 in the payment processing system.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1524 of 1551

[00166] In some implementations, the process 1200 occurs after the mobile device 150 sends the AuthGrant in Figure 8C. In some implementations, the process 1200 occurs after the mobile device 150 sends the authorization grant to the payment module 100 in operation 1012 of process 1000 in Figure 23.

[00167] The payment module 100 obtains (1202) an indication corresponding to an event at the machine 120. For example, after the process 1000 in Figure 23, the user of the mobile device 150 selects a product to purchase from the machine 120 by interacting with one or more input mechanisms of the machine 120 (e.g., buttons 126 or a touch screen display 124 shown in Figure 19), and the machine 120 dispenses the selected product. Continuing with this example, after the product is dispensed, the transaction is complete and the payment module 100 obtains an indication from the machine of the completed transaction. In some implementations, the indication includes the amount of the transaction and (optionally) machine status information associated with the machine 120 such as inventory information as to one or more products of the payment accepting unit 120 and/or the like. In some implementations, the indication includes status information indicating that the transaction was aborted (e.g., via actuation of a coin return mechanism at the machine 120) or that there was an error with the transaction (e.g., a vending jam or other malfunction with the machine 120).

[00168] After obtaining the indication corresponding to completion of the first transaction, the payment module 100 generates (1204) a notification corresponding to the event at the machine 120.

[00169] The payment module 100 sends (1206), via a short-range communication capability (e.g., BLE), the notification to the mobile device 150. In some embodiments, in addition to the notification corresponding to the event at machine 120, the payment module 100 sends a promotion or advertisement to the mobile device 150 that is targeted to the user of the mobile device 150 based on the transaction or the user ID included in the AuthGrant or authorization grant token that initiated the transaction. In some embodiments, in addition to the notification corresponding to the event at machine 120, the payment module 100 sends a pseudo randomly selected promotion or advertisement to the mobile device 150 that is selected from a set of promotions or advertisements stored by the payment module 100. For example, the promotion is a coupon for a free soda following the purchase of ten sodas from the machine 120

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1525 of 1551

by the user of the mobile device 150. For example, the promotion is a random 50% off coupon or free soda coupon. For example, the transaction corresponds to a vended soda and the advertisement corresponds to a new soda from the same company that produces the vended soda.

[00170] The mobile device 150 provides (1208) a representation of the notification. For example, in Figure 26A, the mobile device 150 displays user interface 1302 on touch screen 152 with a message 1306 that indicates that the first transaction is complete. For example, in Figure 26C, the mobile device 150 displays user interface 1320 on touch screen 152 with a message 1322 that indicates that the transaction was aborted. For example, in Figure 26D, the mobile device 150 displays user interface 1330 on touch screen 152 with a message 1332 that indicates that there was an error with the transaction. For example, the mobile device 150 also displays a representation of the promotion of advertisement on the user interface for the application 140.

[00171] Figure 25B illustrates a schematic flow diagram of a process 1250 for processing acknowledgement information in accordance with some implementations. In some implementations, the payment processing system includes one or more payment modules 100 (e.g., each associated with a respective payment accepting unit 120 such an automatic retailing machine for dispensing goods and/or services), one or more mobile devices 150 (e.g., each executing the application 140 for the payment processing system either as a foreground or background process), and the server 130. The server 130 manages the payment processing system and, in some cases, supplies, operates, and/or manufactures the one or more payment modules 100. For brevity, the process 1250 will be described with respect to a respective payment module 100 associated with a respective payment accepting unit 120 (machine 120) and a respective mobile device 150 in the payment processing system.

[00172] In some implementations, the process 1250 occurs after the mobile device 150 sends the AuthGrant in Figure 8C. In some implementations, the process 1250 occurs after the mobile device 150 sends the authorization grant to the payment module 100 in operation 1012 of process 1000 in Figure 23.

[00173] The payment module 100 obtains (1252) an indication corresponding to completion of a first transaction from the machine 120. For example, after the process 1000 in Figure 23, the user of the mobile device 150 selects a product to purchase from the machine 120 by interacting with one or more input mechanisms of the machine 120 (e.g., buttons 126 or a

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1526 of 1551

touch screen display 124 shown in Figure 19), and the machine 120 dispenses the selected product. Continuing with this example, after the product is dispensed, the transaction is complete and the payment module 100 obtains an indication from the machine of the completed transaction. In some implementations, the indication includes the amount of the transaction and (optionally) machine status information associated with the machine 120 such as inventory information as to one or more products of the payment accepting unit 120 and/or the like.

[00174] After obtaining the indication corresponding to completion of the first transaction, the payment module 100 generates (1254) a first notification with first transaction information based on the indication, and the payment module 100 stores the first transaction information. In some implementations, the first transaction information includes a transaction ID for the first transaction, a module ID corresponding to payment module 100, a user ID corresponding to the mobile device 150, transaction status information indicating that the first transaction is complete, and the transaction amount indicated by the indication. In some implementations, the payment module 100 retains the authorization code included in the original broadcasted packet and/or the authorization grant token and includes the authorization code in the first transaction information. In some implementations, the authorization code is encrypted with a secret key corresponding to the payment module 100, which is shared with the server 130 but not the mobile device 150. In some implementations, the first transaction information further includes other information such as the machine status information included in the first notification or transaction information corresponding to previous interrupted transaction(s). See Figure 24D and the accompanying text for further discussion regarding transaction information 1150.

[00175] The payment module 100 sends (1256), via a short-range communication capability (e.g., BLE), the first notification with first transaction information to the mobile device 150. In some embodiments, in addition to first transaction information corresponding to completion of the first transaction at machine 120, the first notification includes a promotion or advertisement to the mobile device 150 that is targeted to the user of the mobile device 150 based on the transaction or the user ID included in the AuthGrant or authorization grant token that initiated the transaction. In some embodiments, in addition to first transaction information corresponding to completion of the first transaction at machine 120, the first notification includes a pseudo randomly selected promotion or advertisement to the mobile device 150 that is selected from a set of promotions or advertisements stored by the payment module 100. For example, the

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1527 of 1551

promotion is a coupon for a free soda following the purchase of ten sodas from the machine 120 by the user of the mobile device 150. For example, the promotion is a random 50% off coupon or free soda coupon. For example, the transaction corresponds to a vended soda and the advertisement corresponds to a new soda from the same company that produces the vended soda.

[00176] The mobile device 150 provides (1258) a representation of the first notification. For example, in Figure 26A, the mobile device 150 displays user interface 1302 on touch screen 152 with a message 1306 that indicates that the first transaction is complete. For example, the mobile device 150 also displays a representation of the promotion of advertisement on the user interface for the application 140.

[00177] The mobile device 150 sends (1260), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), the first transaction information to the server 130.

[00178] The server 130 processes (1262) the first transaction information. For example, the server 130 debits the account of the user associated with the user ID in the first transaction information in the amount indicated by the first transaction information.

[00179] The server 130 sends (1264), via a long-range communication capability (e.g., GSM, CDMA, Wi-Fi, or the like), first acknowledgment information to the mobile device 150. In some implementations, the first acknowledgment information acknowledges that the server 130 received the first transaction information. In some implementations, the first acknowledgment information includes the user ID, the module ID, the transaction ID, and (optionally) the authorization grant included in the transaction information (e.g., auth grant 1158, Figure 24D).

[00180] After receiving the first acknowledgement information, the mobile device 150 sends (1266), via a short-range communication capability (e.g., BLE), the first acknowledgment information to the payment module 100.

[00181] After receiving the first acknowledgment information, the payment module 100 deletes (1268) the stored first transaction information.

[00182] Attention is now directed towards implementations of user interfaces and associated processes that may be implemented on the mobile device 150 with zero or more speakers, zero or more microphones, and a display. For example, the display is a touch screen

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1528 of 1551

(sometimes also herein called a "touch screen display") enabled to receive one or more contacts and display information (e.g., media content, websites and web pages thereof, user interface for the application 140, and/or user interfaces for applications). Figures 26A-26D illustrate example user interfaces for providing a representation of a machine event at a mobile device in accordance with some implementations.

[00183] Figures 26A-26D show user interfaces displayed on mobile device 150 (e.g., a mobile phone); however, one skilled in the art will appreciate that the user interfaces shown in Figures 26A-26D may be implemented on other similar computing devices. The user interfaces in Figures 26A-26D are used to illustrate the processes described herein, including the process described with respect to Figures 25A-25B and 27A-27B.

[00184] For example, a user of the mobile device 150 approaches a machine 120 (e.g., vending machine 78x928 as shown in Figures 10A-10D) and executes application 140 on the mobile device 150 so as to perform an electronic transaction with the machine 120. For example, with reference to Figures 10C-10D, the user of the mobile device 150 initiates a transaction with the machine 120 (e.g., vending machine 78x928) by performing a swipe gesture at a location corresponding to the representation of the dollar bill (e.g., a substantially vertical swipe gesture from a location corresponding to the representation of the dollar bill to the top edge of the mobile device 150).

[00185] Figure 26A illustrates the mobile device 150 displaying a user interface 1302 of the application 140 on touch screen 152 after the user of the mobile device 150 initiates and performs a transaction with the machine 120. In Figure 26A, the user interface 1302 includes prepaid balance 1304 which indicates that $1.00 has been deducted from the prepaid balance after performing a transaction with the machine 120 as compared to the prepaid balance in Figure 10C-10D (i.e., $9.00 in Figures 10C-10D and $8.00 in Figure 26A). In Figure 26A, the user interface 1302 also includes a message 1306 indicating that the transaction with the machine 120 is complete.

[00186] Figure 26B illustrates the mobile device 150 displaying a user interface 1310 of the application 140 on touch screen 152 after the user of the mobile device 150 initiates a transaction with the machine 120 and an error with the transaction occurs or the transaction is aborted. In Figure 26B, the user interface 1310 shows the representation of the dollar bill sliding

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1529 of 1551

onto the touch screen 152 (e.g., in a substantially top to bottom manner). In Figure 26B, the interface 1310 includes prepaid balance 1312 which indicates that no money has been deducted from the prepaid balance after performing a transaction with the machine 120 as compared to the prepaid balance in Figure 10C-10D (i.e., $9.00 in Figures 10C-10D and $9.00 in Figure 26B).

[00187] Figure 26C illustrates the mobile device 150 displaying a user interface 1320 of the application 140 on touch screen 152 after the representation of the dollar bill slides onto the touch screen 152 in Figure 26B due to the transaction being aborted. For example, the user aborts the transaction by actuating a coin return mechanism of the machine 120. In another example, the user aborts the transaction by selection an abort affordance on the interface of the application 140 (not shown). In Figure 26C, the user interface 1320 includes a message 1322 indicating that the transaction with the machine 120 was aborted and that the user's account was not debited for the aborted transaction.

[00188] Figure 26D illustrates the mobile device 150 displaying a user interface 1330 of the application 140 on touch screen 152 after the representation of the dollar bill slides onto the touch screen 152 in Figure 26B due to the occurrence of an error with the transaction. For example, a malfunction with the machine 120 (e.g., a vending jam or stuck item) causes the error to occur. In Figure 26D, the user interface 1330 is associated with the application 140 executed on the mobile device 150. In Figure 26D, the user interface 1330 includes a message 1332 indicating that an error occurred during the transaction with the machine 120 and that the user's account was not debited for the transaction.

[00189] Figures 27A-27B illustrate a flowchart diagram of a method 1400 of presenting representations of payment accepting unit events in accordance with some implementations. In some implementations, the method 1400 is performed by a device with one or more processors, memory, one or more output devices, and two or more communication capabilities. For example, in some implementations, the method 1400 is performed by the mobile device 150 (Figures 5 and 21) or a component thereof (e.g., the application 140). In some implementations, the method 1400 is governed by instructions that are stored in a non-transitory computer readable storage medium (e.g., the memory 860, Figure 21) and the instructions are executed by one or more processors (e.g., the processing unit 850, Figure 21) of the device. Optional operations are indicated by dashed lines (e.g., boxes with dashed-line borders).

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1530 of 1551

[00190] After sending a request to a payment module via a first communication capability transaction to initiate a transaction with a payment accepting unit (e.g., an offline-payment operated machine such as a vending machine or kiosk) associated with the payment module, the mobile device obtains (1402) a notification from the payment module via the first communication capability, where the notification indicates an event at the payment accepting unit associated with the payment module. In some implementations, method 1400 occurs after the mobile device 150 sends the AuthGrant in Figure 8C. In some implementations, method 1400 occurs after the mobile device 150 sends the authorization grant to the payment module 100 in operation 1012 of process 1000 in Figure 23. Operation 1206 of Figure 25A, for example, shows the mobile device 150 receiving a notification sent by the payment module 100 (e.g., the adapter module 100, Figures 5 and 20) sent via the first communication capability (e.g., a short-range communication technology/protocol such as BLE). The notification indicates an event at the payment accepting unit (e.g., the payment accepting unit 120, Figures 5 and 19) (sometimes also herein called "machine 120") associated with the payment module 100.

[00191] In some implementations, the first communication capability corresponds (1404) to a short-range communication protocol. As described above, the short-range communication protocols include BLE, NFC, and/or other protocols utilizing non-persistent communication channels.

[00192] In response to obtaining the notification, the mobile device provides (1406) a representation of the notification to a user of the mobile device via the one or more output devices of the mobile device. For example, in Figure 26A, the mobile device 150 displays user interface 1302 on touch screen 152 with a message 1306 that indicates that the first transaction is complete. For example, in Figure 26C, the mobile device 150 displays user interface 1320 on touch screen 152 with a message 1322 that indicates that the transaction was aborted. For example, in Figure 26D, the mobile device 150 displays user interface 1330 on touch screen 152 with a message 1332 that indicates that there was an error with the transaction.

[00193] In some implementations, the one or more output devices of the mobile device include (1408) at least one of: a display, one or more speakers, one or more LEDs, and a vibration mechanism. For example, the mobile device 150 includes one or more of a display

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1531 of 1551

(e.g., the touch screen 152, Figures 10A-10D), one or more speakers, one or more LEDs, and a vibration mechanism.

[00194] In some implementations, the representation of the notification is at least one of (1410): a message displayed on the display of the mobile device; a banner notification displayed on a display of the mobile device; a vibration alert from the vibration mechanism of the mobile device; an aural alert from the one or more speakers of the mobile device; and a visual alert from the one or more LEDs of the mobile device. For example, in Figures 26B-26D, the representation of the notification includes messages 1306, 1322, and 1332 displayed on the touch screen 152 of the mobile device 150. In another example, the representation of the notification is a predefined sequence of vibrations provided by the vibration mechanism of the mobile device 150. In another example, the representation of the notification is a predefined sequence of tones provided by the one or more speakers of the mobile device 150. In another example, the representation of the notification is a predefined sequence of blinking LEDs of the mobile device 150.

[00195] In some implementations, the notification indicates (1412) abortion of a transaction initiated by the user of the mobile device. In Figure 26C, for example, the user interface 1320 includes the message 1322 indicating that the transaction has been aborted. For example, the user aborts the transaction by actuating a coin return mechanism of the machine 120. In another example, the user aborts the transaction by selection an abort affordance on the interface of the application 140 (not shown).

[00196] In some implementations, the notification indicates (1414) completion of a transaction between the user of the mobile device and the payment accepting unit. In Figure 26A, for example, the user interface 1302 includes the message 1306 indicating that completion of the transaction with the machine 120 initiated by the user of the mobile device 150.

[00197] In some implementations, the notification indicating completion of the transaction at least includes (1416) an amount of the completed transaction. In Figure 26A, for example, the user interface 1302 includes prepaid balance 1304 which indicates that $1.00 has been deducted from the prepaid balance after performing a transaction with the machine 120 as compared to the prepaid balance in Figure 10C-10D (i.e., $9.00 in Figures 10C-10D and $8.00 in Figure 26A).

[00198] In some implementations, the mobile device sends (1418) at least a portion of the notification to a server via a second communication capability distinct from the first

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1532 of 1551

communication capability. Operation 1260 of Figure 25B, for example, shows the mobile device 150 sending first transaction information to the server 130 for a completed transaction via the second communication capability (e.g., a long-range communication protocols such as Wi-Fi, CDMA, GSM, and/or the like). For example, the first transaction information at least includes the amount of the first completed transaction.

[00199] In some implementations, the first communication capability corresponds (1420) to a short-range communication protocol and the second communication capability corresponds to a long-range communication protocol. For example, the first communication capability of the mobile device 150 is a radio/transceiver means for communicating via one or more short-range communication protocols such as BLE, NFC, and/or the like (i.e., a non-persistent communication channel). For example, the second communication capability of the mobile device 150 is a radio/transceiver means for communicating via one or more long-range communication protocols such as Wi-Fi, CDMA, GSM, and/or the like.

[00200] In some implementations, the notification indicates (1422) failure of a transaction initiated by the user of the mobile device or a malfunction associated with the payment accepting unit. In Figure 26D, for example, the user interface 1330 includes the message 1332 indicating that there was an error with the transaction. For example, the transaction fails due to a vending jam or other malfunction. In another example, the payment accepting unit experiences a malfunction due to an open door or the like. In some implementations, at least a portion of the failure/malfunction notification is sent to the sever 130 and an alert is subsequently sent to the operator of the payment accepting unit (e.g., the machine 120) by the server 130.

[00201] It should be understood that the particular order in which the operations in Figures 27A-27B have been described is merely for example purposes and is not intended to indicate that the described order is the only order in which the operations could be performed. One of ordinary skill in the art would recognize various ways to reorder the operations described herein. Additionally, it should be noted that details of other processes described herein with respect to other methods described herein are also applicable in an analogous manner to the method 1400 described above with respect to Figures 27A-27B.

[00202] Figure 28A illustrates a block diagram of an offline-payment operated machine 1500 in accordance with some implementations. For example, the offline-payment operated

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1533 of 1551

machine 1500 (e.g., a form of the machine 120) is an electro-mechanical machine capable of accepting currency (e.g., coins), which is not connected to any networks (e.g., telephone, cellular, or Wi-Fi). For example, the offline-payment operated machine 1500 is a washer or dryer at a laundromat, a parking meter, a car wash payment kiosk, or other offline-payment operated machine that dispenses goods and/or services.

[00203] In Figure 28A, the offline-payment operated machine 1500 includes a microswitch 1502, a control unit 1506, a power supply 1508, a transistor 1510, and an operation unit 1512. The components of the offline-payment operated machine 1500 in Figure 28A are examples and one of skill in the art will appreciate that various other components may be included in or excluded from the offline-payment operated machine 1500.

[00204] In Figure 28A, the microswitch 1502 is a leveraged microswitch with lever 1504. For example, the microswitch 1502 is a CHERRY BRAND™ microswitch with a normally open terminal ("NO"), a normally closed terminal ("NC"), and a common terminal. For example, the lever 1504 is incorporated into a coin slot of the offline-payment operated machine 1500 and is depressed whenever a coin slides down the coin slot into a coin reservoir of the offline-payment operated machine 1500 (not shown). For example, when the lever 1504 is depressed and the microswitch 1502 is wired in the NO configuration as shown in Figure 28A, the switch is closed. Continuing with this example, when the switch is closed, control unit 1506 receives a pulse (i.e., a payment acceptance signal) from the common terminal of the microswitch 1502 indicating depression of the lever 1504 from the reception of a US quarter (i.e., $0.25) or coin of another value.

[00205] In some implementations, when the control unit 1506 receives a preset sequence of payment acceptance signals indicative of a preset number of coins being received by the microswitch 1502, the control unit 1506 initiates the operation of the offline-payment operated machine 1500. For example, after receiving the preset sequence of payment acceptance signals (e.g., three pulses indicating reception of three US quarters), the control unit 1506 initiates operation of the offline-payment operated machine 1500 by applying current to the gate of the transistor 1510 which allows current to flow from the power supply 1508 to operation unit 1512. For example, the operation unit 1512 is a motor of a dryer which begins spinning once current flows from the power supply 1508.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1534 of 1551

[00206] In Figure 28A, payment module 1520 (e.g., a form of the adapter module 100, Figures 5 and 20) is configured to be installed in the offline-payment operated machine 1500 so as to retrofit the offline-payment operated machine 1500 to be able to accept electronic payments. In some implementations, the payment module 1520 includes all or some of the components included adapter module 100 in Figure 20 such as processing unit 750, memory 760, a security unit 755, and a communications unit 770. In some implementations, the payment module 1520 also includes a first interface module 1522, a second interface module 1524, and a lead 1536 for drawing power from power supply 1508 of the offline-payment operated machine 1500.

[00207] In Figure 28A, the first interface module 1522 is configured to sample payment acceptance signals from the microswitch 1502 (e.g., a coin receiving switch) via lead 1532 of the offline-payment operated machine 1500. For example, the payment acceptance signals are indicative of a coin being received by the microswitch 1502 which depress lever 1504. In Figure 28A, the second interface module 1524 is configured to sample control signals from the control unit 1506 of the offline-payment operated machine 1500 via lead 1534 that initiate an operation of the offline-payment operated machine (e.g., the application of current to the gate of the transistor 1510) in response to receiving a preset sequence of payment acceptance signals from the microswitch 1502 (e.g., the coin receiving switch) indicative of the preset number of coins.

[00208] Figure 28B illustrates signals sampled by the payment module 1520 in accordance with some implementations. In Figure 28B, sample 1550 represents a preset sequence of payment acceptance signals sampled by the first interface module 1522 via lead 1532 that are sent from the microswitch 1502 to the control unit 1506. For example, the preset sequence of payment acceptance signals indicative of the preset number of coins include pulses (i.e., payment acceptance signals) 1552, 1554, 1556, and 1558. For example, the leading edges of pulses 1552, 1554, 1556, and 1558 at times 1582, 1584, 1586, and 1588 indicate reception of a coin by microswitch 1502 which causes the switch to close when wired in the NO configuration as shown in Figure 28A. In Figure 28B, sample 1570 represents a control signal sampled by the second interface module 1524 via lead 1534 that is sent from the control unit 1506 to transistor 1510. In Figure 28B, the sample 1570 includes a pulse 1572 that is sent from the control unit 1506 to transistor 1510 at time 1590 after receiving the preset sequence of payment acceptance signals from the microswitch 1502 (i.e., pulses 1552, 1554, 1556, and 1558).

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1535 of 1551

[00209] Figures 29A-29B illustrate a flowchart diagram of a method of retrofitting an offline-payment operated machine to accept electronic payments in accordance with some implementations. In some implementations, the method 1600 is performed by a payment module with one or more processors and memory. In some implementations, the payment module also includes a short-range communication capability corresponding to a short-range communication protocol (e.g., a non-persistent communication channel such as BLE, NFC, and/or the like), where the short-range communication capability is configured to communicate with one or more mobile devices, where each of the one or more mobile devices is configured with a complimentary short-range communication capability and a long-range communication capability corresponding to a long-range communication protocol (e.g., Wi-Fi, CDMA, GSM, and/or the like).

[00210] In some implementations, the payment module is coupled with an offline-payment operated machine (e.g., the payment accepting unit 120, Figures 5 and 19 (sometimes also herein called "machine 120"), or the offline-payment operated machine 1500, Figure 28A) such as dryer or washer in a laundromat, a parking meter, a car wash payment kiosk, or the like. In some implementations, the offline-payment operated machine includes a coin receiving switch (e.g., the microswitch 1502, Figure 28A) and a control unit (e.g., the control unit 1506, Figure 28A). In some implementations, the payment module further includes: (A) a first interface module (e.g., the first interface module 1522, Figure 28A) configured to sample payment acceptance signals from the coin receiving switch of the offline-payment operated machine, where the signals are indicative of a coin being received by the coin receiving switch; and (B) a second interface module (e.g., the second interface module 1524, Figure 28A) configured to sample control signals from the control unit of the offline-payment operated machine that initiate an operation of the offline-payment operated machine in response to receiving a preset sequence of payment acceptance signals from the coin receiving switch indicative of the preset number of coins. By sampling and storing these signals, the payment module 1520 is able to simulate operation of a respective coin receiving switch in response to receiving the correct/preset number of coins so as to trigger operation of the offline-payment operated machine in response to completion of an electronic payment.

[00211] For example, in some implementations, the method 1600 is performed by the adapter module 100 (Figures 5 and 20) or payment module 1520 (Figure 28A). In some

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1536 of 1551

implementations, the method 1600 is governed by instructions that are stored in a non-transitory computer readable storage medium (e.g., the memory 760, Figure 20) and the instructions are executed by one or more processors (e.g., the processing unit 750, Figure 20) of the payment module. Optional operations are indicated by dashed lines (e.g., boxes with dashed-line borders).

[00212] In some implementations, the payment module detects (1602), via the first interface module, a preset sequence of payment acceptance signals from the coin receiving switch that causes the control unit to initiate the operation of the offline-payment operated machine, where the preset sequence of payment acceptance signals are indicative of a preset number of coins received by the coin receiving switch. For example, with reference to Figures 28A-28B, the first interface module 1522 of the payment module 1520 samples payment acceptance signals via lead 1532 from the microswitch 1502 to the control unit 1506. For example, each of the payment acceptance signals is indicative of reception of a coin by the microswitch 1502. Continuing with this example, the second interface module 1524 of the payment module 1520 samples control signals via lead 1534 from the control unit 1506 to the transistor 1510. The payment module 1520 detects a preset sequence of payment acceptance signals from the microswitch 1502 that causes the control unit 1506 to apply a current to the gate of the transistor 1510 (e.g., the control signals). For example, the preset sequence of payment acceptance signals is indicative of a preset number of coins received by the microswitch 1502 to cause operation of the offline-payment operated machine 1500. For example, the application of current to the gate of the transistor 1510 allows current to flow from the power supply 1508 to the operation unit 1512 so that the operation. For example, the operation unit 1512 is a motor of a dryer which begins spinning once current flows from the power supply 1508.

[00213] In some implementations, the payment module determines (1604) the predefined signal sequence to emulate the preset sequence of payment acceptance signals from the coin receiving switch. In some implementations, after detecting the preset sequence of payment acceptance signals that causes the control unit 1506 to initiate the operation of the offline-payment operated machine 1500, the payment module 1520 determines a predefined signal sequence to emulate the preset sequence of payment acceptance signals. In some implementations, the money value associated with each pulse in the preset sequence of payment acceptance signals from the microswitch 1502, indicative of the preset number of coins to initiate the operation of the offline-payment operated machine 1500, is a default currency (e.g., USD)

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1537 of 1551

and amount (e.g., $0.25) set in the firmware of the payment module 1520. In some implementations, the money value associated with the each pulse in the preset sequence of payment acceptance signals from the microswitch 1502, indicative of the preset number of coins to initiate the operation of the offline-payment operated machine 1500, is set by the server 130 and can be changed remotely by using the mobile device 150 as a communications bridge to send information indicating the value of a pulse from the server 130 to the mobile device 150 via the second communication capability (e.g., GSM, CDMA, or Wi-Fi) and forwarding the information from the mobile device to the payment module 1520 via the first communication capability (e.g., BLE). For instance, in most cases, each pulse is US $0.25.

[00214] In some implementations, determining the predefined signal sequence includes (1606) at least one of: identifying a count of pulses in the present sequence of payment acceptance signals; identifying amplitude of pulses in the present sequence of payment acceptance signals; identifying shape of pulses in the present sequence of payment acceptance signals; and identifying an interval between pulses. In some implementations, after detecting the preset sequence of payment acceptance signals (e.g., the sample 1550, Figure 28B), the payment module 1520 determines a predefined signal sequence to emulate the preset sequence of payment acceptance signals by identifying a count of pulses in the preset sequence of payment acceptance signals, an interval between pulses in the preset sequence of payment acceptance signals, the shape of pulses in the preset sequence of payment acceptance signals, and an amplitude of pulses in the preset sequence of payment acceptance signals.

[00215] The payment module receives (1608) a request via the short-range communication capability from a respective mobile device to perform an operation of the offline-payment operated machine. For example, with reference to Figure 8C, the payment module 1520 (Figure 28A) receives the AuthGrant from the mobile device 150 via the short-range communication capability (e.g., BLE) indicating that the user of the mobile device 150 wishes to perform the operation of the offline-payment operated machine 1500 (Figure 28A). For example with reference to operation 1012 in Figure 23, the payment module 1520 (Figure 28A) receives an authorization grant token from the mobile device 150 via the short-range communication capability (e.g., BLE) indicating that the user of the mobile device 150 wishes to perform the operation of the offline-payment operated machine 1500 (Figure 28A).

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1538 of 1551

[00216] The payment module validates (1610) the request. Validation of the request indicates (1612) that the respective mobile device is authorized to initiate payment for the operation by a remote server via the long-range communication capability. In some implementations, the payment module 1520 validates the request from the mobile device 150 by determining whether the AuthGrant or the authorization grant token includes a valid authorization code.

[00217] In accordance with a determination that the request is valid, the payment module causes (1614) the payment operated machine to perform the operation by issuing a predefined signal sequence to the control unit, where the predefined signal sequence emulates a signal sequence that would be issued by the coin receiving switch in response to receiving a preset number of coins. For example, with reference to Figure 28B, the payment module 1520 issues a predefined signal sequence with first interface module 1522 to the control unit 1506 that emulates sample 1550 in Figure 28B. Continuing with this example, in response to receiving the predefined signal sequence from the payment module 1520 control unit 1506 causes initiation of the operation of the offline-payment operated machine 1500 by applying current to the gate of the transistor 1510 which allows current to flow from the power supply 1508 to operation unit 1512. In some implementations, the control unit 1506 causes initiation of the operation by setting a timer to an amount of time corresponding to the preset number of coins whereby current flows to the gate of the transistor 1510 for the set amount of time. For example, the preset number of coins is a number of a coins required to run the offline-payment operated machine 1500 by for a default amount of time and subsequent coins may be added to extend the amount of time that the offline-payment operated machine 1500 by will run. In some implementations, the preset number of coins is a number of a coins required to cause the offline-payment operated machine 1500 to dispense a purchased item, such as laundry detergent.

[00218] Alternatively, in some implementations, in accordance with a determination that the request is valid, the offline-payment operated machine 1500 displays credit to the user (e.g., via one of the displays 122 or 124 shown in Figure 19) and the user interacts with the input mechanisms of the offline-payment operated machine 1500 120 (e.g., via the buttons 126 or a touch screen display 124 shown in Figure 19) to perform the operation of the machine. For example, if the offline-payment operated machine 1500 is a dryer, the user of the mobile device 150 selects the appropriate spin cycle via input mechanisms of the dryer, and when the user of

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1539 of 1551

the mobile device 150 selects a start/run input mechanism of the dryer, control unit 1506 of the dryer causes initiation of the operation of the dryer (e.g., starting a motor that corresponds to operation unit 1512 in Figure 28A).

[00219] In some implementations, prior to sending the operation information and after causing the offline-payment operated machine to perform the operation by issuing the predefined signal sequence to the control unit, the payment module obtains (1616) a notification from the offline-payment operated machine indicating initiation of the operation of the offline-payment operated machine and the preset number of coins. For example, after issuing the preset signal sequence to control unit 1506, the payment module 1520 (Figure 28A) obtains a notification indicating that the control unit 1506 sent control signals to initiate operation of the offline-payment operated machine 1500 in response to receiving the predefined signal sequence. For example, the notification is obtained by the second interface module 1524 (e.g., the sample 1570, Figure 28B) sampling controls signals sent by control unit 1506 (e.g., application of current to the gate of the transistor 1510 which allows current to flow from the power supply 1508 to operation unit 1512).

[00220] In response to receiving the notification, the payment module (1618): generates the operation information based at least in part on the notification; and stores the generated operation information in the memory. For example, after obtaining the notification, the payment module 1520 (Figure 28A) generates operation information corresponding to performance of the operation and the preset number of coins associated with the predefined signal sequence (e.g., the amount required to initiate operation of the offline-payment operated machine 1500) and stores the operation information in memory local to the payment module 1520 (e.g., the memory 760, Figure 20).

[00221] In some implementations, the payment module sends (1620) operation information corresponding to the operation to the respective mobile device via the short-range communication capability. For example, after operation 1618, the payment module 1520 (Figure 28A) sends the operation information to the mobile device 150 via the first communication capability of the mobile device 150 such as a radio/transceiver means for communicating via one or more short-range communication protocols such as BLE, NFC, and/or the like (i.e., a non-persistent communication channel)

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1540 of 1551

[00222] It should be understood that the particular order in which the operations in Figures 29A-29B have been described is merely for example purposes and is not intended to indicate that the described order is the only order in which the operations could be performed. One of ordinary skill in the art would recognize various ways to reorder the operations described herein. Additionally, it should be noted that details of other processes described herein with respect to other methods described herein (e.g., the method 1700 in Figure 30) are also applicable in an analogous manner to the method 1600 described above with respect to Figures 29A-29B.

[00223] Figure 30 illustrates a flowchart diagram of a method 1700 of enabling a payment operated machine to accept electronic payments in accordance with some implementations. In some implementations, the method 1700 is performed by an offline-payment operated machine (e.g., the payment accepting unit 120, Figures 5 and 19 (sometimes also herein called "machine 120"), or the offline-payment operated machine 1500, Figure 28A) such as dryer or washer in a laundromat, a parking meter, a car wash payment kiosk, or the like.

[00224] In some implementations, the offline-payment operated machine includes a control unit (e.g., the control unit 1506, Figure 28A), memory, and a coin receiving switch (e.g., the microswitch 1502, Figure 28A). In some implementations, the offline-payment operated machine also includes a short-range communication capability corresponding to a short-range communication protocol (e.g., a non-persistent communication channel such as BLE, NFC, and/or the like), where the short-range communication capability is configured to communicate with one or more mobile devices, where each of the one or more mobile devices is configured with a complimentary short-range communication capability and a long-range communication capability corresponding to a long-range communication protocol (e.g., Wi-Fi, CDMA, GSM, and/or the like). For example, in some implementations, the method 1700 is performed by the machine 120, (Figures 5 and 19). In some implementations, the method 1700 is governed by instructions that are stored in a non-transitory computer readable storage medium and the instructions are executed by the control unit of the offline-payment operated machine.

[00225] The offline-payment operated machine receives (1702) a request via a short-range communication capability from a respective mobile device to perform an operation of the offline-payment operated machine. For example, with reference to Figure 8C, the payment module 1520 (Figure 28A) receives the AuthGrant from the mobile device 150 via the short-

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1541 of 1551

range communication capability (e.g., BLE) indicating that the user of the mobile device 150 wishes to perform the operation of the offline-payment operated machine 1500 (Figure 28A). For example with reference to operation 1012 in Figure 23, the payment module 1520 (Figure 28A) receives an authorization grant token from the mobile device 150 via the short-range communication capability (e.g., BLE) indicating that the user of the mobile device 150 wishes to perform the operation of the offline-payment operated machine 1500 (Figure 28A).

[00226] The offline-payment operated machine validates (1704) the request. Validation of the request indicates (1706) that the respective mobile device is authorized to initiate payment for the operation by a remote server via the long-range communication capability. In some implementations, the payment module 1520 validates the request from the mobile device 150 by determining whether the AuthGrant or the authorization grant token includes a valid authorization code.

[00227] In accordance with a determination that the request is valid, the offline-payment operated machine performs (1708) the operation by issuing a predefined signal sequence to the control unit, where the predefined signal sequence emulates a preset number of coins received by the coin receiving switch. For example, in accordance with a determination that the request is valid, the offline-payment operated machine or a component thereof issues a predefined signal sequence to the control unit 1506 that emulates sample 1550 in Figure 28B. Continuing with this example, in response to receiving the predefined signal sequence from the payment module 1520, control unit 1506 causes initiation of the operation of the offline-payment operated machine 1500 by applying current to the gate of the transistor 1510 which allows current to flow from the power supply 1508 to operation unit 1512. In another example, in accordance with a determination that the request is valid, the control unit 1506 causes initiation of the operation of the offline-payment operated machine 1500 by applying current to the gate of the transistor 1510 which allows current to flow from the power supply 1508 to operation unit 1512.

[00228] It should be understood that the particular order in which the operations in Figure 30 have been described is merely for example purposes and is not intended to indicate that the described order is the only order in which the operations could be performed. One of ordinary skill in the art would recognize various ways to reorder the operations described herein. Additionally, it should be noted that details of other processes described herein with respect to

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1542 of 1551

other methods described herein (e.g., the method 1600 in Figures 29A-29B) are also applicable in an analogous manner to the method 1700 described above with respect to Figure 30.

MISCELLANEOUS

[00229] It should be noted that relative terms are meant to help in the understanding of the technology and are not meant to limit the scope of the invention. Similarly, unless specifically stated otherwise, the terms used for labels (e.g., "first," "second," and "third") are meant solely for purposes of designation and not for order or limitation. The term "short" in the phrase "short-range" (in addition to having technology specific meanings) is relative to the term "long" in the phrase "long-range."

[00230] The terms "may," "might," "can," and "could" are used to indicate alternatives and optional features and only should be construed as a limitation if specifically included in the claims.

[00231] It should be noted that, unless otherwise specified, the term "or" is used in its nonexclusive form (e.g., "A or B" includes A, B, A and B, or any combination thereof, but it would not have to include all of these possibilities). It should be noted that, unless otherwise specified, "and/or" is used similarly (e.g., "A and/or B" includes A, B, A and B, or any combination thereof, but it would not have to include all of these possibilities). It should be noted that, unless otherwise specified, the terms "includes" and "has" mean "comprises" (e.g., a device that includes, has, or comprises A and B contains A and B, but optionally may contain C or additional components other than A and B). It should be noted that, unless otherwise specified, the singular forms "a," "an," and "the" refer to one or more than one, unless the context clearly dictates otherwise.

[00232] It is to be understood that the inventions, examples, and implementations described herein are not limited to particularly exemplified materials, methods, and/or structures. It is to be understood that the inventions, examples, and implementations described herein are to be considered preferred inventions, examples, and implementations whether specifically identified as such or not.

[00233] The terms and expressions that have been employed in the foregoing specification are used as terms of description and not of limitation, and are not intended to exclude equivalents

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1543 of 1551

of the features shown and described. While the above is a complete description of selected implementations of the present invention, it is possible to practice the invention using various alternatives, modifications, adaptations, variations, and/or combinations and their equivalents. It will be appreciated by those of ordinary skill in the art that any arrangement that is calculated to achieve the same purpose may be substituted for the specific embodiment shown. It is also to be understood that the following claims are intended to cover all of the generic and specific features of the invention herein described and all statements of the scope of the invention that, as a matter of language, might be said to fall therebetween.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1544 of 1551

CLAIMS

1. A method of presenting representations of payment accepting unit events, comprising:

at a mobile device with one or more processors, memory, one or more output devices including a display, and one or more radio transceivers:

identifying one or more payment accepting units in proximity to the mobile device that are available to accept payment from a mobile payment application executing on the mobile device, the identifying based at least in part on an identifier corresponding to the one or more payment accepting units, wherein the one or more payment accepting units are payment operated machines that accept payment for dispensing of products and/or services;

displaying a user interface of the mobile payment application on the display of the mobile device, the user interface being configured to display a visual indication of the one or more payment accepting units and accept user input to (i) receive selection by a user of the mobile device of an available payment accepting unit of the one or more payment accepting units and (ii) trigger payment by the mobile payment application for a transaction initiated by the user of the mobile device with the available payment accepting unit of the one or more payment accepting units;

establishing via the one or more radio transceivers a wireless communication path including the mobile device and the available payment accepting unit of the one or more payment accepting units;

after establishing the wireless communication path, enabling user interaction with the user interface of the mobile payment application to complete the transaction;

exchanging information with the available payment accepting unit via the one or more radio transceivers, in conjunction with the transaction; and

after exchanging the information, displaying, on the display, an updated user interface of the mobile payment application to the user of the mobile device.

2. The method of claim 1, wherein the updated user interface of the mobile payment application includes at least one of:

a message displayed on the display of the mobile device;

a banner notification displayed on a display of the mobile device; and/or

a visual alert from one or more LEDs of the mobile device.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1545 of 1551

3. The method of claim 1, wherein the information indicates completion of the transaction between the user of the mobile device and the available payment accepting unit.

4. The method of claim 3, wherein the mobile device includes a long-range transceiver and the information at least includes an amount of the completed transaction, and the method further comprises:

sending at least the amount of the completed transaction to a server via the long-range transceiver.

5. The method of claim 1, wherein the information indicates abortion of the transaction initiated by the user of the mobile device.

6. The method of claim 1, wherein the information indicates failure of the transaction initiated by the user of the mobile device or a malfunction associated with the available payment accepting unit.

7. The method of claim 1, wherein the mobile device includes an accelerometer and the method further comprises:

based on data from the accelerometer, determining whether the user is walking away from the available payment accepting unit; and

in accordance with a determination that the user is walking away from the available payment accepting unit, canceling the wireless communication path.

8. The method of claim 1, wherein the information reflects availability of the available payment accepting unit to conduct a transaction.

9. The method of claim 1, further comprising:

in addition to exchanging the information, receiving, via the one or more radio transceivers, a coupon that is targeted to the user of the mobile device based on the transaction.

10. The method of claim 1, wherein the user interface of the mobile payment application, after establishing the wireless communication path, indicates that the wireless communication path has been established with the available payment accepting unit.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1546 of 1551

11. The method of claim 1, wherein the user interface of the mobile payment application, after establishing the wireless communication path, includes:

a visual representation of the available payment accepting unit;

an indication of a prepared balance; and

an affordance that when slid, indicates the initiation of the transaction;

wherein the affordance is slid in response to receiving a user input of swipe on the affordance displayed on the display of the mobile device.

12. The method of claim 1, wherein the payment operated machines include a payment activated washer, a payment activated dryer, a vending machine, a parking meter, a toll booth, an arcade game, a kiosk, a photo booth, or a ticket dispensing machine.

13. A mobile device, comprising:

one or more radio transceivers;

one or more output devices including a display;

one or more processors; and

memory storing one or more programs to be executed by the one or more processors, the one or more programs comprising instructions for:

identifying one or more payment accepting units in proximity to the mobile device that are available to accept payment from a mobile payment application executing on the mobile device, the identifying based at least in part on an identifier corresponding to the one or more payment accepting units, wherein the one or more payment accepting units are payment operated machines that accept payment for dispensing of products and/or services;

displaying a user interface of the mobile payment application on the display of the mobile device, the user interface being configured to display a visual indication of the one or more payment accepting units and accept user input to (i) receive selection by a user of the mobile device of an available payment accepting unit of the one or more payment accepting units and (ii) trigger payment by the mobile payment application for a transaction initiated by the user of the mobile device with the available payment accepting unit of the one or more payment accepting units;

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1547 of 1551

establishing via the one or more radio transceivers a wireless communication path including the mobile device and the available payment accepting unit of the one or more payment accepting units;

after establishing the wireless communication path, enabling user interaction with the user interface of the mobile payment application to complete the transaction;

exchanging information with the available payment accepting unit via the one or more radio transceivers, in conjunction with the transaction; and

after exchanging the information, displaying, on the display, an updated user interface of the mobile payment application to the user of the mobile device.

14. The mobile device of claim 13, wherein identifying the one or more payment accepting units includes identifying a payment activated washer, a payment activated dryer, a vending machine, a parking meter, a toll booth, an arcade game, a kiosk, a photo booth, or a ticket dispensing machine.

15. A non-transitory computer readable storage medium storing one or more programs, the one or more programs comprising instructions, which, when executed by a mobile device with one or more processors, one or more output devices including a display, and one or more radio transceivers, cause the mobile device to perform operations comprising:

identifying one or more payment accepting units in proximity to the mobile device that are available to accept payment from a mobile payment application executing on the mobile device, the identifying based at least in part on an identifier corresponding to the one or more payment accepting units, wherein the one or more payment accepting units are payment operated machines that accept payment for dispensing of products and/or services;

displaying a user interface of the mobile payment application on the display of the mobile device, the user interface being configured to display a visual indication of the one or more payment accepting units and accept user input to (i) receive selection by a user of the mobile device of an available payment accepting unit of the one or more payment accepting units and (ii) trigger payment by the mobile payment application for a transaction initiated by the user of the mobile device with the available payment accepting unit of the one or more payment accepting units;

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1548 of 1551

establishing via the one or more radio transceivers a wireless communication path including the mobile device and the available payment accepting unit of the one or more payment accepting units;

after establishing the wireless communication path, enabling user interaction with the user interface of the mobile payment application to complete the transaction;

exchanging information with the available payment accepting unit via the one or more radio transceivers, in conjunction with the transaction; and

after exchanging the information, displaying, on the display, an updated user interface of the mobile payment application to the user of the mobile device.

16. The non-transitory computer readable storage medium of claim 15, wherein the updated user interface of the mobile payment application includes at least one of:

a message displayed on the display of the mobile device;

a banner notification displayed on a display of the mobile device; and/or

a visual alert from one or more LEDs of the mobile device.

17. The non-transitory computer readable storage medium of claim 15, wherein:

the information indicates completion of the transaction between the user of the mobile device and the available payment accepting unit;

the information at least includes an amount of the completed transaction; and

the instructions further cause the mobile device to send at least the amount of the completed transaction to a server.

18. The non-transitory computer readable storage medium of claim 15, wherein the information indicates abortion of the transaction initiated by the user of the mobile device.

19. The non-transitory computer readable storage medium of claim 15, wherein the information indicates failure of the transaction initiated by the user of the mobile device or a malfunction associated with the available payment accepting unit.

20. The non-transitory computer readable storage medium of claim 15, wherein identifying the one or more payment accepting units includes identifying a payment activated washer, a

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1549 of 1551

payment activated dryer, a vending machine, a parking meter, a toll booth, an arcade game, a kiosk, a photo booth, or a ticket dispensing machine.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1550 of 1551

ABSTRACT

A mobile device presents representations of payment accepting unit events on a display, by identifying a payment accepting unit that is available to accept payment from a mobile payment application executing on the mobile device, displaying a visual indication of the payment accepting unit and accepting user input to receive selection of the payment accepting unit and trigger payment, establishing a wireless communication path including the mobile device and the payment accepting unit, enabling user interaction with the user interface to complete the transaction, exchanging information with the available payment accepting unit via the one or more radio transceivers in conjunction with the transaction, and displaying an updated user interface of the mobile payment application.

Draft Only

CSC ServiceWorks - Ex. 1002
Page 1551 of 1551