US 20250252418A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2025/0252418 A1**

Dunjic et al. (43) **Pub. Date: Aug. 7, 2025**

(54) **TOKEN MANAGEMENT SERVER AND METHOD OF PROCESSING LIMITED-USE TOKENS**

(71) Applicant: **The Toronto-Dominion Bank**, Toronto (CA)

(72) Inventors: **Milos Dunjic**, Oakville (CA); **Zhihong Luo**, Vaughan (CA)

(21) Appl. No.: **19/191,059**

(22) Filed: **Apr. 28, 2025**

Related U.S. Application Data

(63) Continuation of application No. 16/141,330, filed on Sep. 25, 2018, now Pat. No. 12,314,920.

Publication Classification

(51) **Int. Cl.**

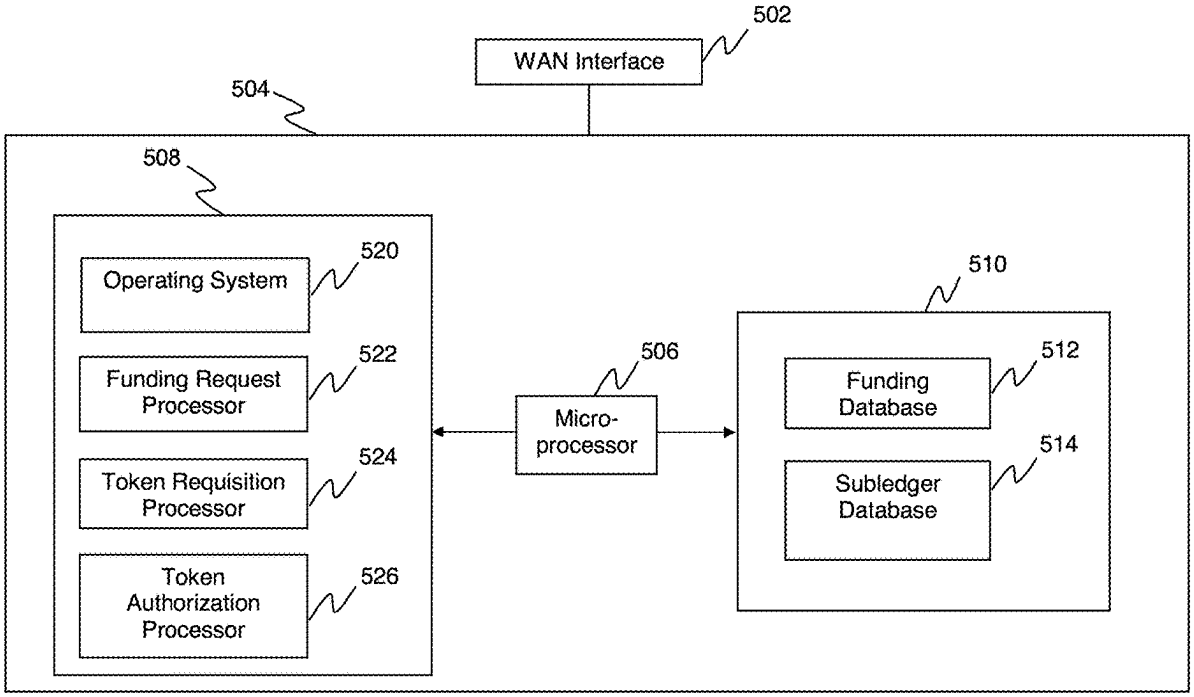
G06Q 20/20	(2012.01)
G06Q 20/34	(2012.01)
G06Q 20/38	(2012.01)
G06Q 20/40	(2012.01)

(52) **U.S. Cl.**

CPC ***G06Q 20/202*** (2013.01); ***G06Q 20/342*** (2013.01); ***G06Q 20/3821*** (2013.01); ***G06Q 20/40*** (2013.01)

(57) **ABSTRACT**

A computer server includes a memory and a data processor. The memory stores a token database and computer processing instructions. The computer processing instructions cause the data processor to receive from a POS station via a payment network a token authorization request that includes a limited-use token and an authorization value, locate in the token database a token record that stores a subledger identifier in association with the limited-use token, and extract the subledger identifier from the located token record. The computer processing instructions also cause the data processor to locate in a subledger database a subledger that is associated with the subledger identifier, confirm that a balance value associated with the located subledger is at least equal to the authorization value, and initiate a transfer from a pooling ledger, distinct from the subledger, of a transfer amount that is equal to the authorization value.



500

FIG. 1

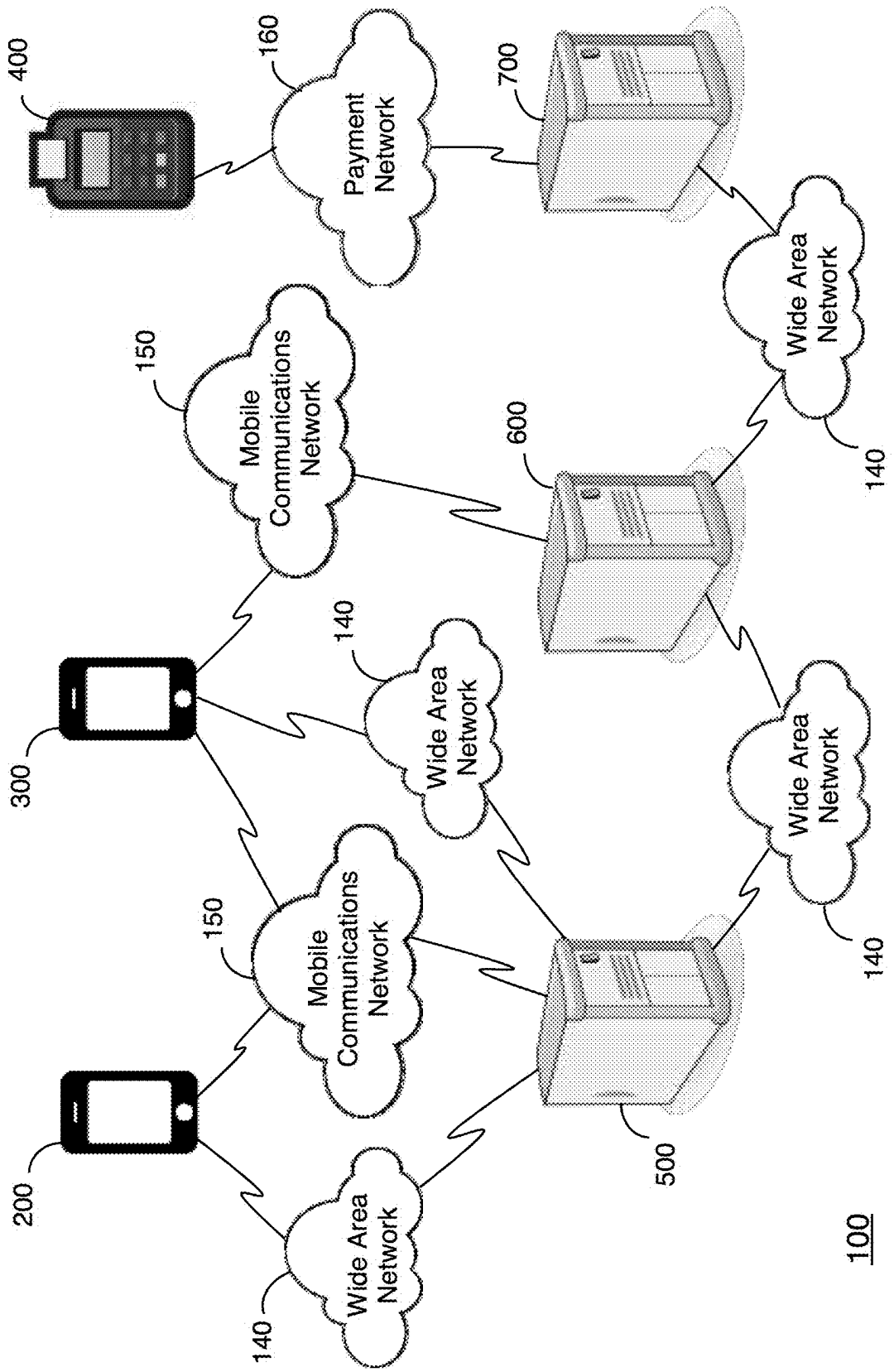
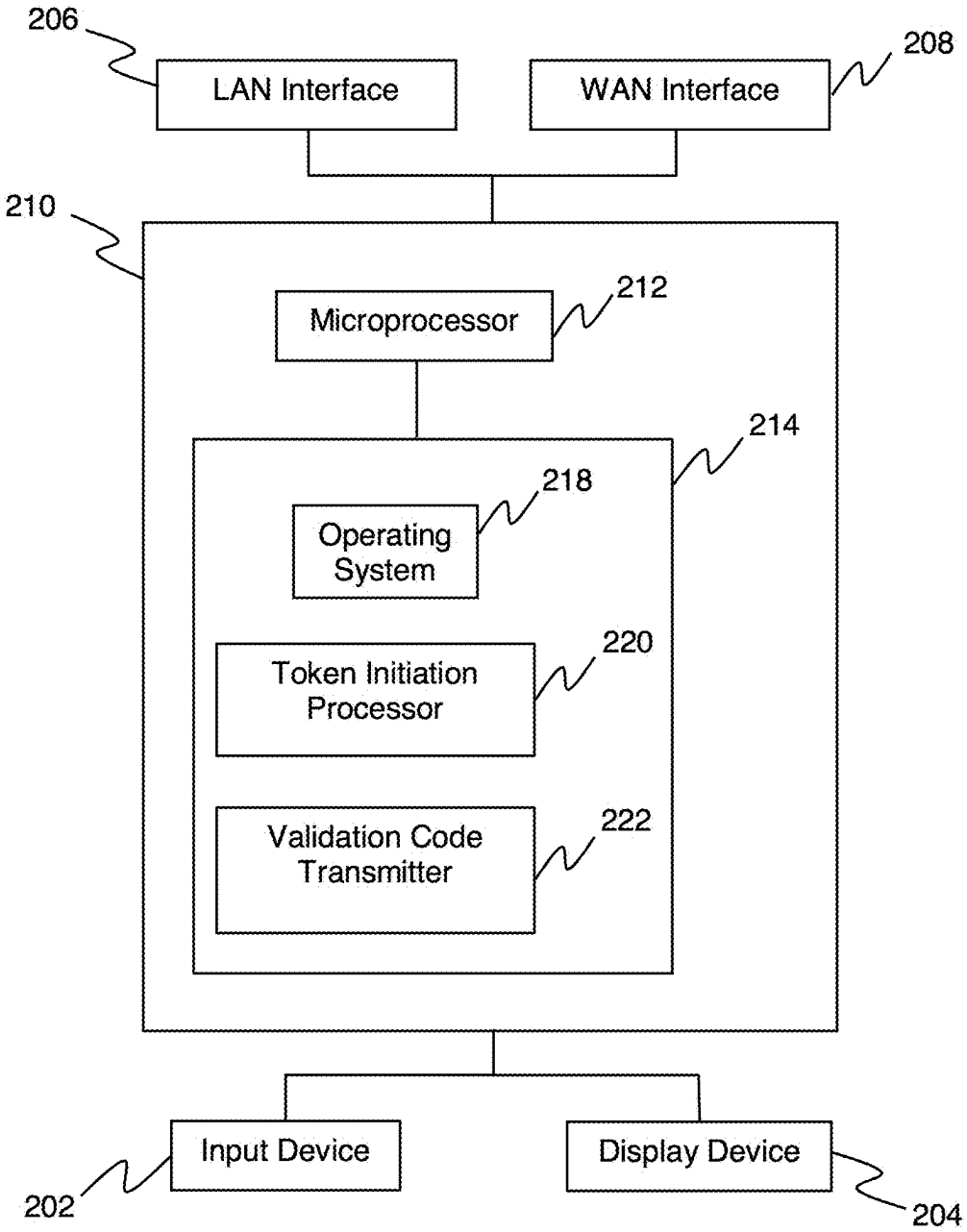

400
160
Payment Network
700
150
Mobile Communications Network
600
140
Wide Area Network
300
140
Wide Area Network
150
Mobile Communications Network
140
Wide Area Network
200
500
140
Wide Area Network
100

FIG. 2


206
LAN Interface
208
WAN Interface
210
Microprocessor
212
214
218
Operating System
220
Token Initiation Processor
222
Validation Code Transmitter
Input Device
202
Display Device
204

200

FIG. 3

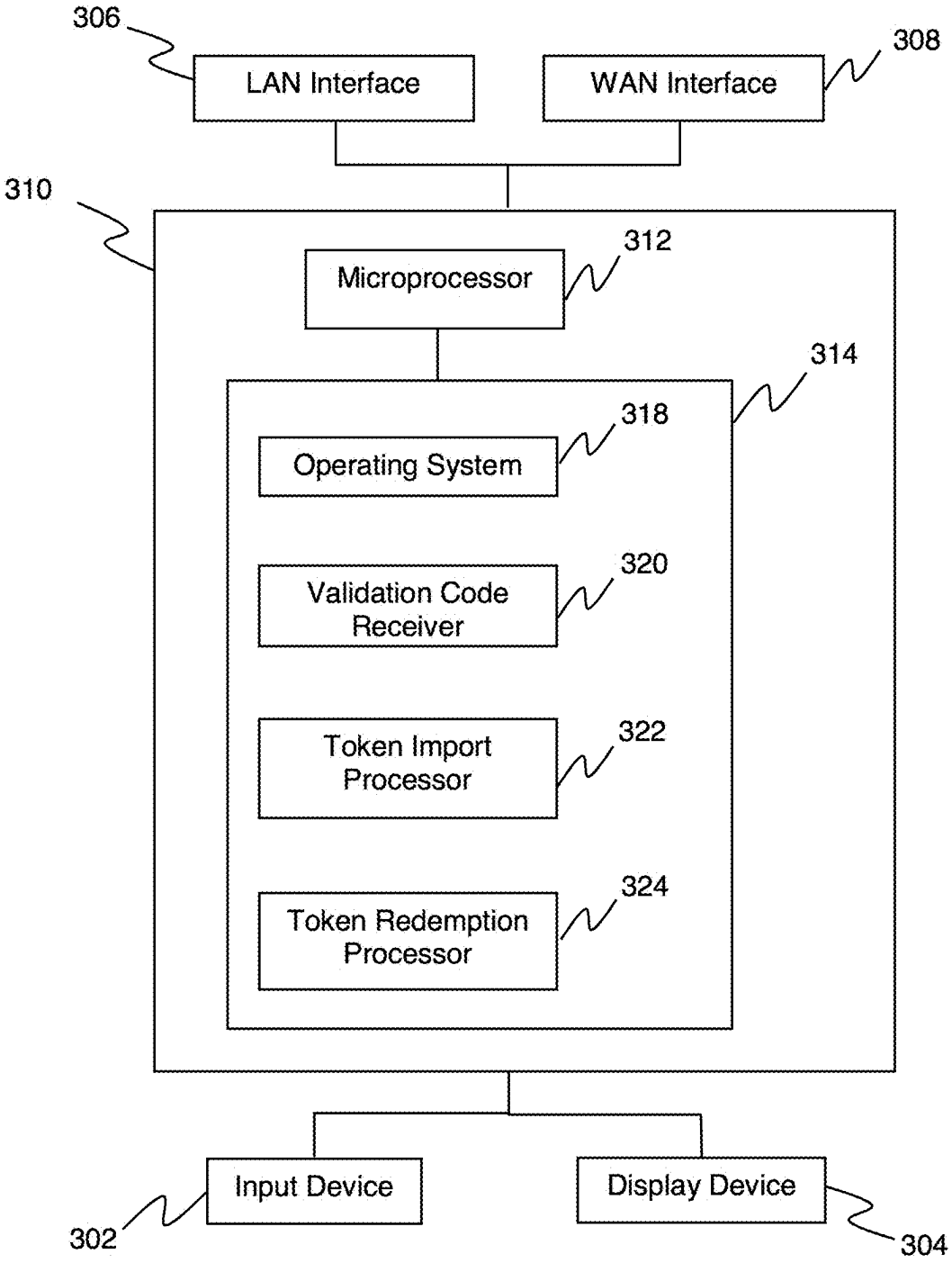
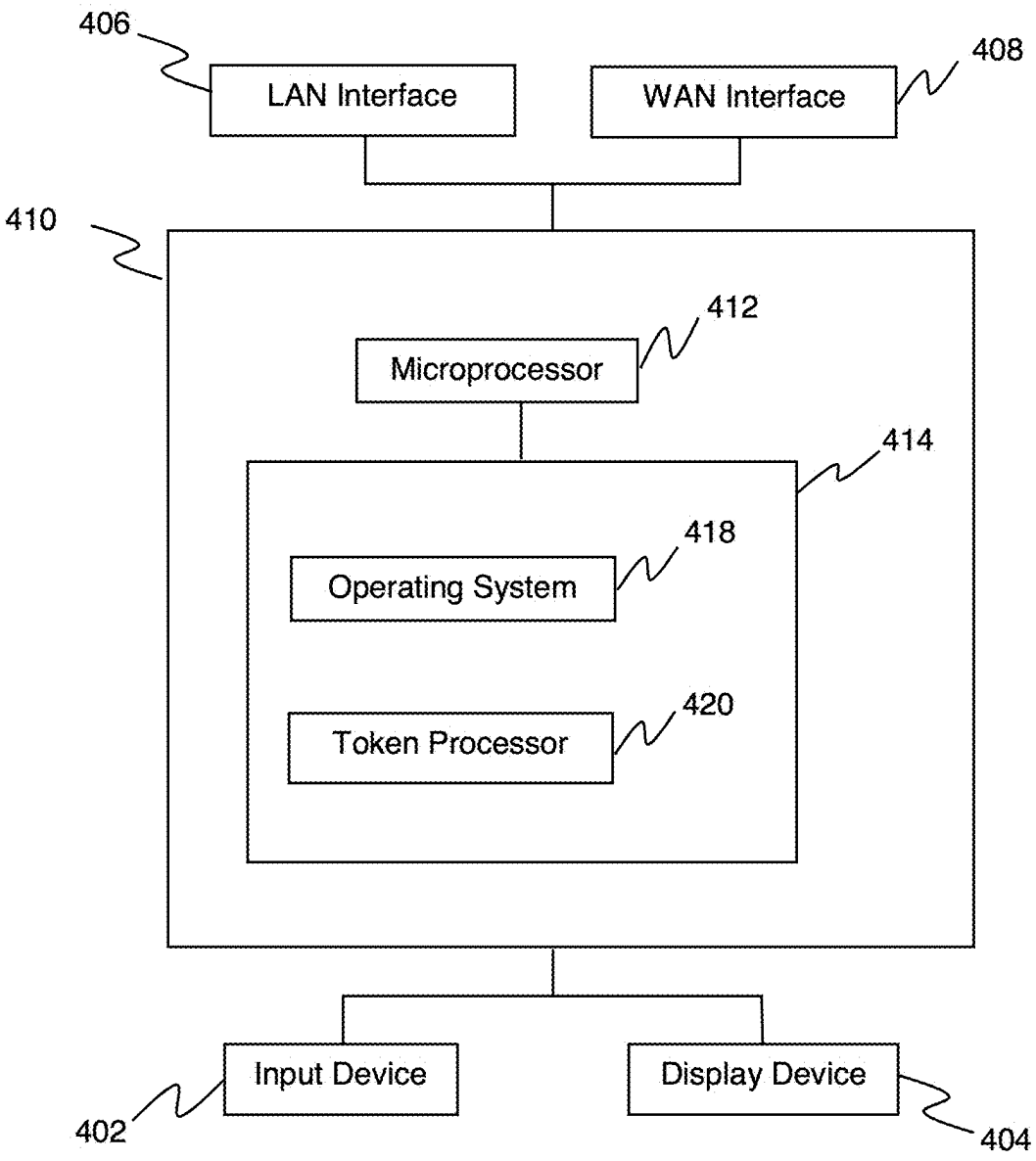

306
LAN Interface
308
WAN Interface
310
312
Microprocessor
314
318
Operating System
320
Validation Code Receiver
322
Token Import Processor
324
Token Redemption Processor
Input Device
Display Device
302
304
300

FIG. 4


406
LAN Interface
WAN Interface
408
410
412
Microprocessor
414
418
Operating System
420
Token Processor
Input Device
Display Device
402
404

400

FIG. 5

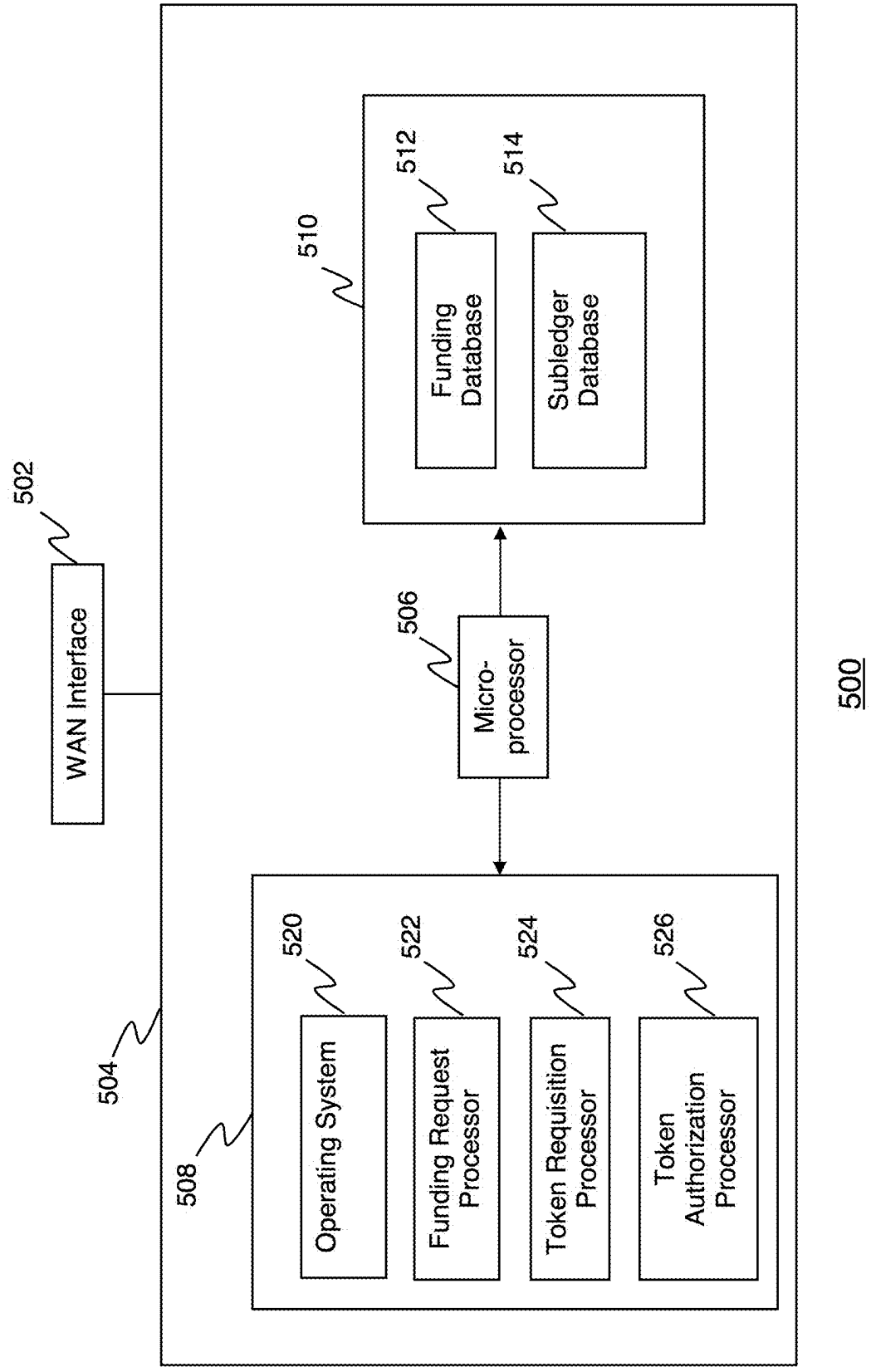

500
502
WAN Interface
504
506
Micro-processor
508
510
512
Funding Database
514
Subledger Database
520
Operating System
522
Funding Request Processor
524
Token Requisition Processor
526
Token Authorization Processor

FIG. 6

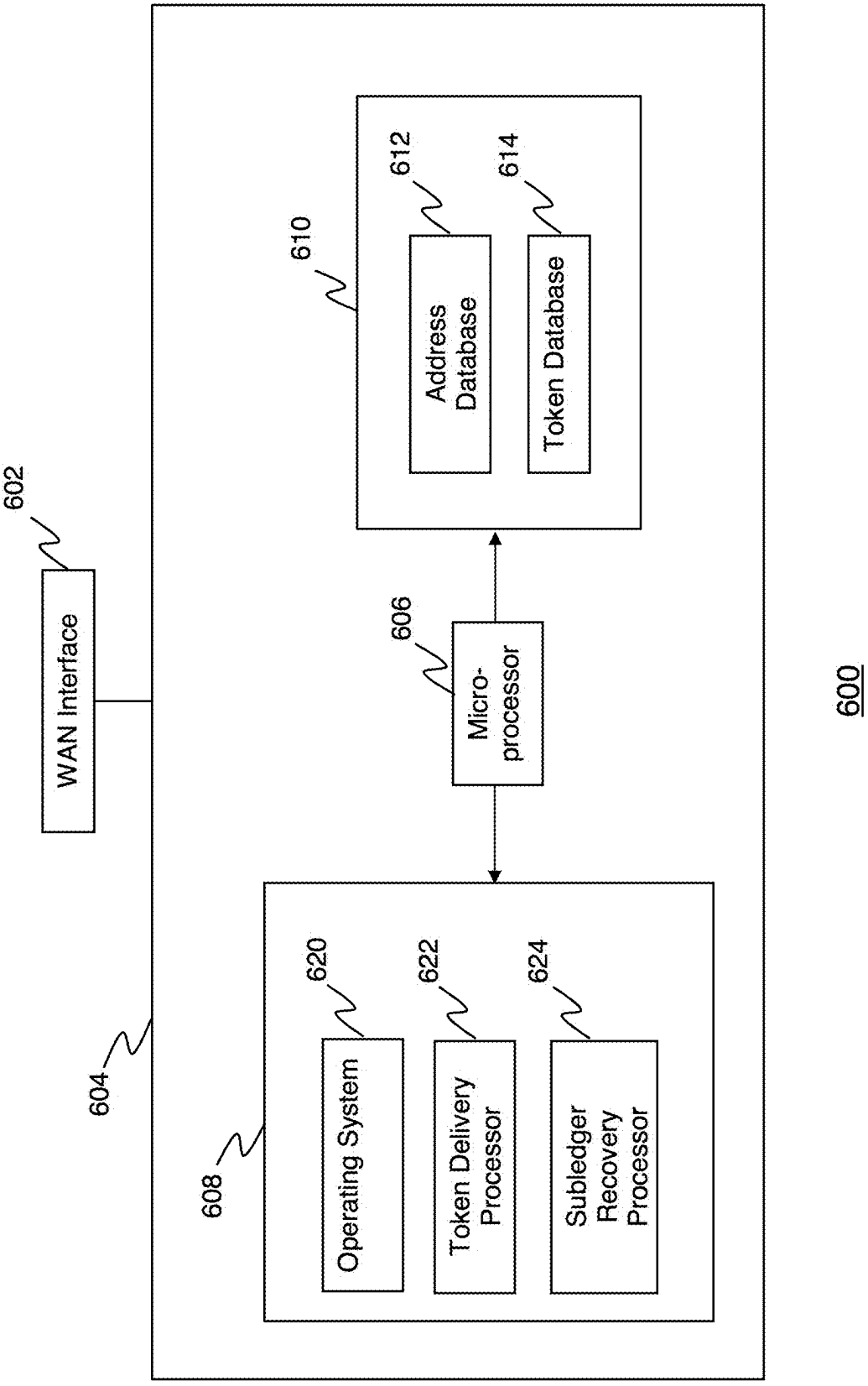

602
WAN Interface
604
606
Micro-processor
608
610
612
Address Database
614
Token Database
620
Operating System
622
Token Delivery Processor
624
Subledger Recovery Processor
600

FIG. 7A

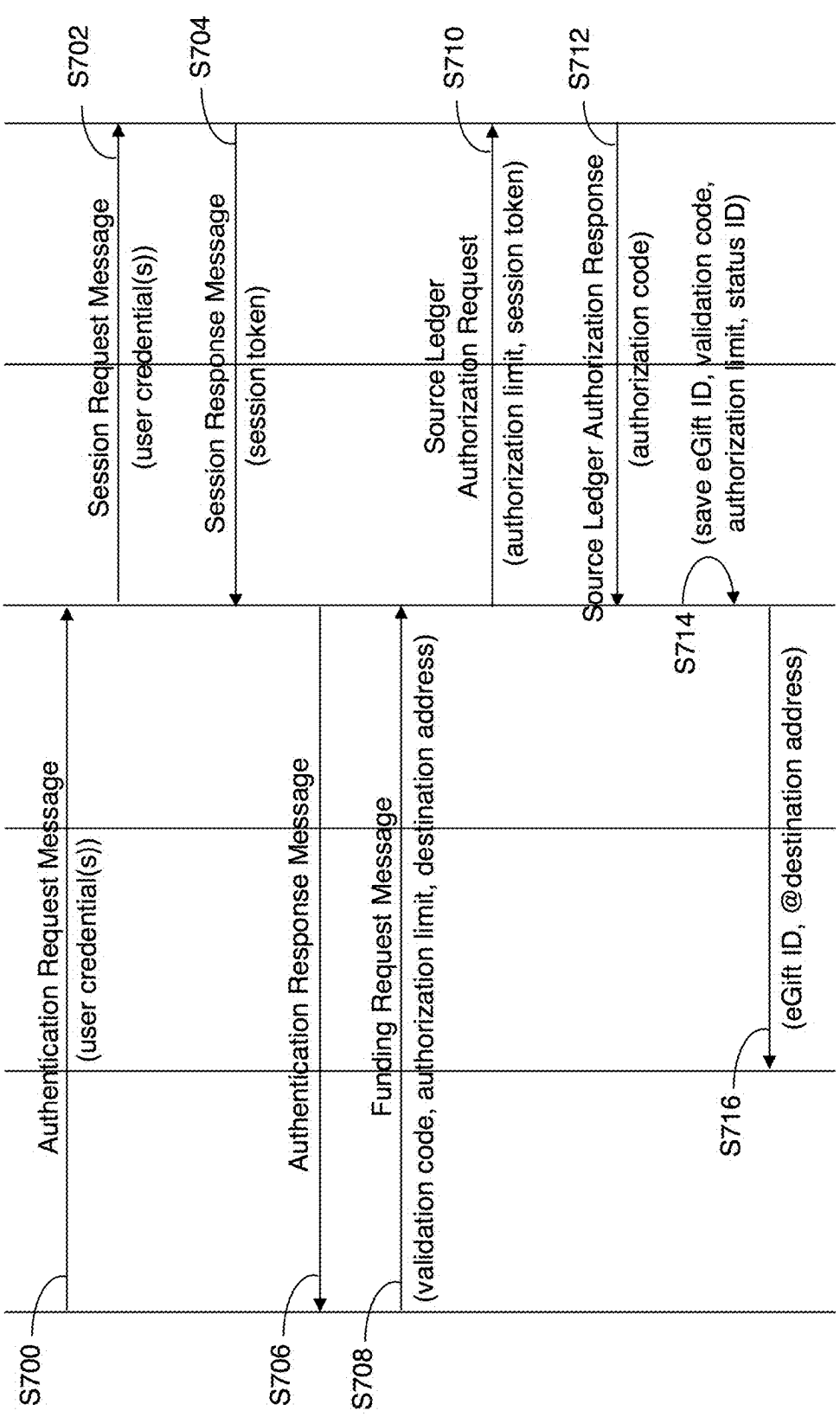

PAYOR APPLIANCE
PAYEE APPLIANCE
POS STATION
TOKEN MANAGEMENT SERVER
TSP SERVER
AUTHORIZATION SERVER
S700
Authentication Request Message
(user credential(s))
S702
Session Request Message
(user credential(s))
S704
Session Response Message
(session token)
S706
Authentication Response Message
S708
Funding Request Message
(validation code, authorization limit, destination address)
S710
Source Ledger Authorization Request
(authorization limit, session token)
S712
Source Ledger Authorization Response
(authorization code)
S714
(save eGift ID, validation code, authorization limit, status ID)
S716
(eGift ID, @destination address)

FIG. 7B

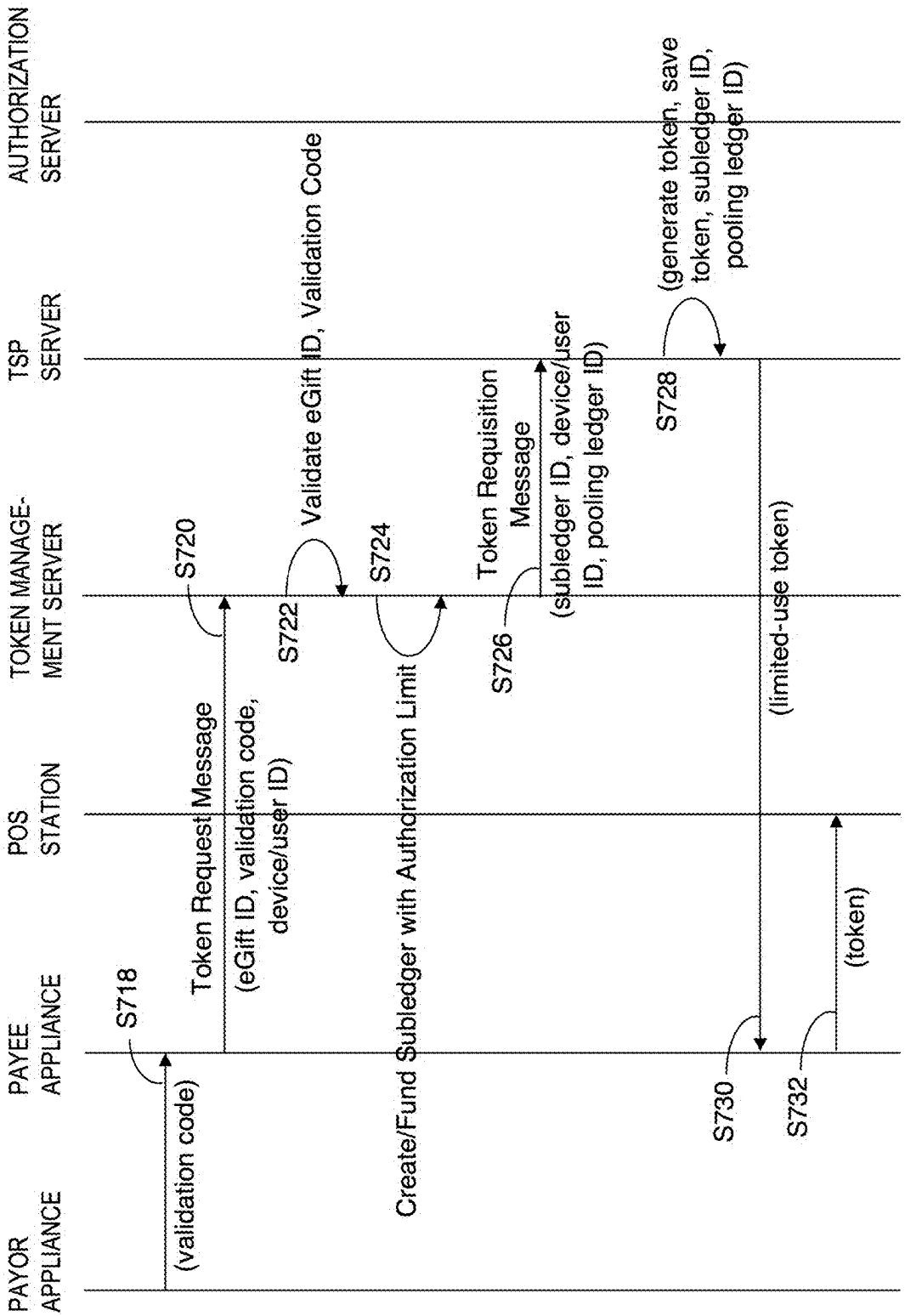

PAYOR APPLIANCE
PAYEE APPLIANCE
POS STATION
TOKEN MANAGE-MENT SERVER
TSP SERVER
AUTHORIZATION SERVER
S718
(validation code)
Token Request Message
(eGift ID, validation code, device/user ID)
S720
Validate eGift ID, Validation Code
S722
Create/Fund Subledger with Authorization Limit
S724
Token Requisition Message
(subledger ID, device/user ID, pooling ledger ID)
S726
(generate token, save token, subledger ID, pooling ledger ID)
S728
(limited-use token)
(token)
S730
S732

FIG. 7C

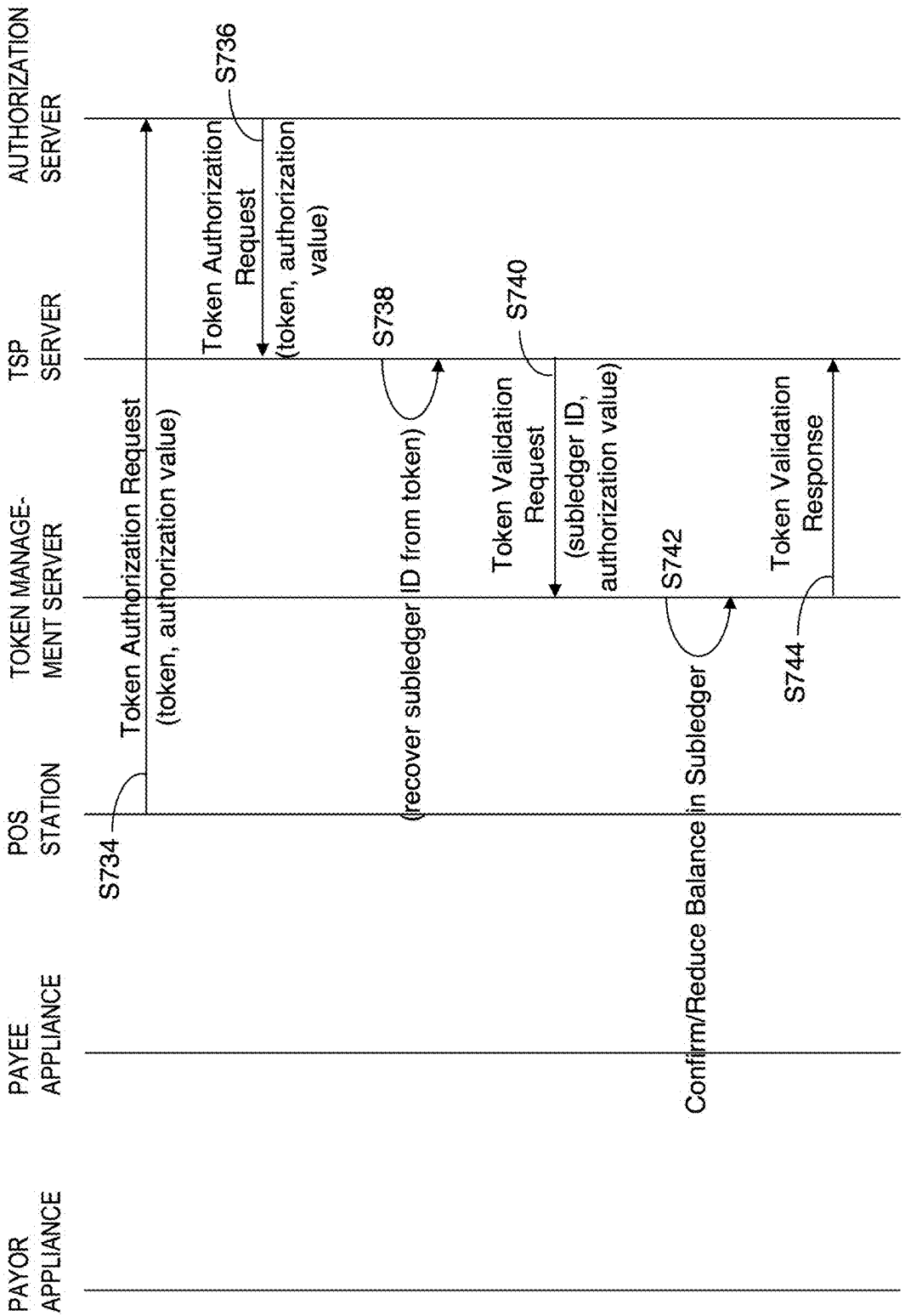
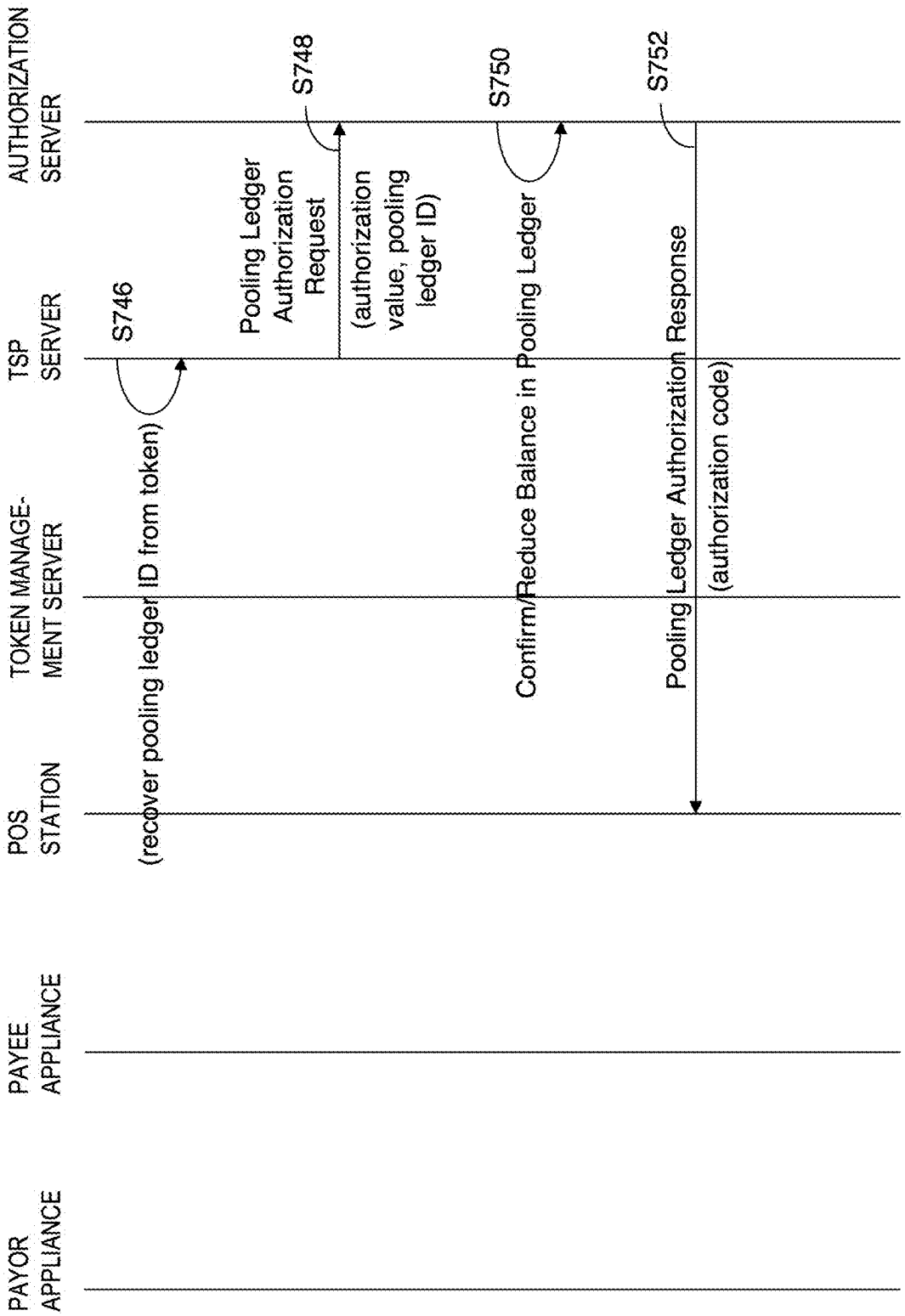

PAYOR APPLIANCE
PAYEE APPLIANCE
POS STATION
TOKEN MANAGE-MENT SERVER
TSP SERVER
AUTHORIZATION SERVER
S734
Token Authorization Request (token, authorization value)
S736
Token Authorization Request (token, authorization value)
S738
(recover subledger ID from token)
S740
Token Validation Request (subledger ID, authorization value)
S742
Confirm/Reduce Balance in Subledger
S744
Token Validation Response

FIG. 7D


PAYOR APPLIANCE
PAYEE APPLIANCE
POS STATION
TOKEN MANAGE-MENT SERVER
TSP SERVER
AUTHORIZATION SERVER
S746
(recover pooling ledger ID from token)
Pooling Ledger Authorization Request
S748
(authorization value, pooling ledger ID)
S750
Confirm/Reduce Balance in Pooling Ledger
S752
Pooling Ledger Authorization Response
(authorization code)

TOKEN MANAGEMENT SERVER AND METHOD OF PROCESSING LIMITED-USE TOKENS

FIELD

[0001] This patent application relates to a method and network for processing stored-value card data via a computer network.

BACKGROUND

[0002] Stored-value cards (also known as gift cards) allow consumers to make purchases anonymously at participating merchants. In contrast to a closed-loop stored-value card, particulars of the account associated with an open-loop stored-value card are not stored locally on the stored-value card but are instead stored in an online database.

[0003] When an open-loop stored-value card is presented to a merchant to effect payment for a transaction, the merchant's point-of-sale terminal reads card data from the stored-value card and transmits the card data and the desired redemption amount over a stored-value card network to a gift card issuer server. The gift card issuer server then determines from the online database whether the balance in the gift card account is sufficient to complete the transaction.

[0004] In order to maintain the security requirements of payment networks, the stored-value card network is maintained separate from the payment networks. Therefore, the merchant's point-of-sale terminal must be configured to access both the stored-value card network and the payment network.

SUMMARY

[0005] This patent application discloses a token management server, a token processing network, and an associated method in which a token is used to effect a transfer from a payment network ledger after confirming a balance in a stored-value card ledger.

[0006] In accordance with a first aspect of this disclosure, there is provided a token management server that includes a memory and a data processor. The memory may store a token database and a plurality of computer processing instructions

[0007] The computer processing instructions cause the data processor to receive from a point-of-sale station, via a payment network, a token authorization request that includes a limited-use token and an authorization value, locate in the token database a token record that stores a subledger identifier in association with the limited-use token, and extract the subledger identifier from the located token record.

[0008] The computer processing instructions also cause the data processor to locate in a subledger database a subledger that is associated with the subledger identifier, confirm that a balance value associated with the located subledger is at least equal to the authorization value, and initiate a transfer from a pooling ledger distinct from the subledger of a transfer amount that is equal to the authorization value.

[0009] In accordance with a second aspect of this disclosure, there is provided a token processing network that includes a token service provider server, a token database, and a subledger database.

[0010] The token service provider server may be configured to receive from a point-of-sale station, via a payment network, a token authorization request that includes the limited-use token and an authorization value, locate in the token database a token record that stores a subledger identifier in association with the limited-use token, and extract the subledger identifier from the located token record.

[0011] The token service provider server may also be configured to locate in the subledger database a subledger that is associated with the subledger identifier, confirm that a balance value associated with the located subledger is at least equal to the authorization value, and initiate a transfer from a pooling ledger distinct from the subledger of a transfer amount that is equal to the authorization value.

[0012] In accordance with a third aspect of this disclosure, there is provided a method of processing limited-use tokens that involves a computer server receiving from a point-of-sale station, via a payment network, a token authorization request that includes a limited-use token and an authorization value, locating in a token database a token record that stores a subledger identifier in association with the limited-use token, and extracting the subledger identifier from the located token record.

[0013] The method may also involve the computer server locating in a subledger database a subledger that is associated with the subledger identifier, confirming that a balance value associated with the located subledger is at least equal to the authorization value, and initiating a transfer from a pooling ledger distinct from the subledger of a transfer amount that is equal to the authorization value.

[0014] In one implementation, the limited-use token is stored in the located token record in association with the subledger identifier and a ledger identifier, and the pooling ledger is associated with the ledger identifier.

[0015] The computer server may initiate the transfer from the pooling may by reducing the balance value of the located subledger by the authorization value, extracting the ledger identifier from the located token record, and obtaining authorization for a funds transfer of the transfer amount from the pooling ledger that is associated with the extracted ledger identifier.

[0016] In one implementation, prior to the receiving the token authorization request the computer server receives from one communications device, via one communications channel, a token request that includes a reference identifier and a credential, locates in a funding database a database record that is associated with the reference identifier, and extracts a validation code from the located database record,

[0017] The computer server then confirms that the credential matches the validation code, generates the subledger identifier, initializes the balance value of the located subledger equal to the authorization limit, saves the subledger identifier in the token record in association with the limited-use token, and provides the one communications device with the limited-use token via a communications channel other than the one communications channel.

[0018] Prior to receiving the token request, the computer server may receive from another communications device a funding request that includes the validation code and an authorization limit, and initiate a transfer into the pooling ledger of a funding amount that is equal to the authorization limit.

[0019] The computer server may then save the reference identifier in the located database record of the funding

database in association with the validation code, and provide the one communications device with the reference identifier.

[0020] The computer server may also receive a user identifier from the one communications device, and initiate the transfer of the funding amount by obtaining authorization for a funds transfer of the funding amount from a source ledger that is associated with the user identifier.

[0021] The token request may also include a device identifier, and the computer server may provide the one communications device with the limited-use token by locating in an address database a destination address that is associated with the device identifier, and transmit the limited-use token to the destination address.

[0022] Since, in accordance with the foregoing aspects of the disclosure, the token processing network (or token management server) receives a limited-use token (from the communications device), but does not initiate the transfer of funds for the transaction from the stored-value account (subledger) that is linked to the limited-use token, possession of a limited-use token does not provide the recipient with access to the payment network account (pooling ledger) from which payment for the transaction is effected. Therefore, the security of the token processing network is enhanced in comparison to conventional stored-value card networks.

[0023] Further, since, prior to initiating the transfer from the pooling ledger, the token processing network (or token management server) confirms the balance value associated with the subledger, the institution server that maintains the pooling ledger is not tasked with responding to a request for a transfer unless the balance value associated with the subledger is already determined to be sufficient. Therefore, the load on the institution server, and the network traffic to and from that server, responding to transfer requests is less than conventional stored-value card networks.

[0024] Moreover, the point-of-sale station can transmit the limited-use token to the institution server over a payment network. Therefore, a merchant's point-of-sale station need not be specifically configured to access both a stored-value card network and a payment network.

BRIEF DESCRIPTION OF THE DRAWINGS

[0025] An exemplary token management server, a token processing network, and method of processing limited-use tokens will now be described, with reference to the accompanying drawings, in which:

[0026] FIG. **1** is a schematic view of an exemplary token processing network, depicting a plurality of communications devices, a point-of-sale station, a token management server, a token service provider server, and an authorization server;

[0027] FIG. **2** is a schematic view of an exemplary first communications device;

[0028] FIG. **3** is a schematic view of an exemplary second communications device;

[0029] FIG. **4** is a schematic view of an exemplary point-of-sale station;

[0030] FIG. **5** is a schematic view of an exemplary token management server;

[0031] FIG. **6** is a schematic view of an exemplary token service provider server; and

[0032] FIGS. **7**A, **7**B, **7**C and **7**D together are a message flow diagram that depicts an exemplary method of processing limited-use tokens.

DETAILED DESCRIPTION

Token Processing Network—Overview

[0033] FIG. **1** is a schematic view of a token processing network, denoted generally as **100**. As shown, the token processing network **100** includes a first communications device **200**, a second communications device **300**, a point-of-sale (POS) station **400**, a token management server **500**, a token service provider (TSP) server **600**, and an authorization server **700**.

[0034] The first communications device **200** may be configured to communicate with the token management server **500** via a wide area network **140**, such as the Internet. Alternately, or additionally, the first communications device **200** may be configured to communicate with the token management server **500** via a mobile cellular communications network **150**.

[0035] The second communications device **300** may be configured to communicate with the token management server **500** via the wide area network **140** and/or the mobile cellular communications network **150**. The second communications device **300** is also configured to communicate with the TSP server **600** via the mobile cellular communications network **150**.

[0036] The POS station **400** is configured to communicate with the authorization server **700** via a payment network **160** (e.g. VisaNet, Mastercard Network).

[0037] The token management server **500** is configured to communicate with the first communications device **200** and the second communications device **300** via the wide area network **140** and/or the mobile communications network **150**. The token management server **500** is also configured to communicate with the TSP server **600** via the wide area network **140**.

[0038] The TSP server **600** is configured to communicate with the token management server **500** and the authorization server **700** via the wide area network **140**.

[0039] The authorization server **700** is configured to communicate with the POS station **400** via the payment network **160**, and to communicate with the TSP server **600** via the wide area network **140**.

[0040] The mobile communications network **150** may be configured as a LTE, WiMax, UMTS, CDMA or GSM network, as examples. The mobile communications network **150** typically includes a plurality of wireless base station subsystems (not shown). The communications devices **200**, **300** may communicate with the base station subsystems via wireless links, and the base station subsystems may communicate with the token management server **500** and the TSP server **600** via wired, wireless or optical links. Therefore, the base station subsystems act as a bridge between the wireless links and the servers **500**, **600**.

[0041] As will be discussed in greater detail below, the token management server **500** (either independently, or in association with the TSP server **600**) may receive a limited-use token (e.g. a string of alphabetic and/or numeric characters) and an authorization value, transform the limited-use token into a subledger identifier, and initiate the transfer (from a pooling ledger) of a transfer amount that is equal to the authorization value. However, prior to initiating the transfer from the pooling ledger, the token management server **500** may confirm that a balance in a subledger that is associated with the subledger identifier is at least equal to the authorization value.

[0042] For example, the token management server **500** may receive from the POS station **400** a token authorization request that includes a limited-use token and an authorization value. In response, the token management server **500** (either independently, or in association with the TSP server **600**) may locate a pooling ledger identifier and a subledger identifier that are associated with the limited-use token, determine the balance value of a subledger associated with the subledger identifier, and confirm that the balance value is at least equal to the authorization value. If the balance value is confirmed, the token management server **500** may initiate a transfer, from a pooling ledger (associated with the pooling ledger identifier) of a transfer amount that is equal to the authorization value.

[0043] The token management server **500** may receive (e.g. from the second communications device **300**) a token request that includes a reference identifier and a credential. In response, the token management server **500** may locate a validation code that is associated with the reference identifier, and confirm that the credential matches the validation code. The token management server **500** (either independently, or in association with the TSP server **600**) may then generate the aforementioned subledger identifier, associate the subledger identifier and a pooling ledger identifier with a limited-use token, and provide the second communications device **300** with the limited-use token.

[0044] Further, prior to receiving the token request (e.g. from the second communications device **300**), the token management server may receive (e.g. from the first communications device **200**) a funding request that includes the validation code and an authorization limit. In response, the token management server **500** may initiate a transfer into the pooling ledger of a funding amount that is equal to the authorization limit, and associate the reference identifier with the validation code and the authorization limit.

[0045] Although the token processing network **100** is shown comprising only a single first communications device **200**, a single second communications device **300**, and a single POS station **400**, the token processing network **100** typically includes a plurality of the communications devices **200**, **300** and a plurality of the POS stations **400**.

[0046] Conversely, although the token management server **500** and the TSP server **600** are depicted as distinct servers in FIG. **1**, all or part of the functionality implemented by the TSP server **600** may instead be implemented by the token management server **500** (or vice versa). Moreover, in some situations, all or part of the functionality implemented by the token management server **500** and the TSP server **600** may instead be implemented by the authorization server **700**.

First Communications Device

[0047] The first communications device **200** may be implemented as a wireless communications terminal, such as a portable digital assistant (PDA), a tablet computer or a smartphone. Alternately, the first communications device **200** may be implemented as a wired communications terminal, such as a personal computer or a web server.

[0048] As shown in FIG. **2**, where the first communications device **200** is implemented as a wireless communications terminal or a personal computer, the first communications device **200** may include an input device **202**, a display device **204** and a local area network (LAN) interface **206**. Independently of the implementation of the first communications device **200**, the first communications device **200** may also include a wide area network (WAN) interface **208**, and a data processing system **210** that is in communication with the input device **202** (if present), the display device **204** (if present), the LAN interface **206** (if present) and the WAN interface **208**.

[0049] The input device **202** (if present) may be implemented as a keyboard, touchpad, touchscreen or other input device suitable for allowing the operator to input data and/or commands into the first communications device **200**. The display device **204** may be implemented as a liquid crystal display (LCD) panel, plasma display panel, or other display device suitable for displaying information to the operator of the first communications device **200**.

[0050] The LAN interface **206** (if present) may interface the first communications device **200** with the second communications device **300**. The LAN interface **206** may be configured as a wireless interface that allows the first communications device **200** to communicate directly with the second communications device **300** via a short-range wireless connection, such as a Bluetooth, or a Near Field Communications (NFC) connection, as examples. Alternately, the LAN interface **206** may be configured as a wired interface that allows the first communications device **200** to communicate directly with the second communications device **300** via a wired connection, such as a Universal Serial Bus (USB) connection, as an example.

[0051] The WAN interface **208** interfaces the first communications device **200** with the wide area network **140** and/or the mobile communications network **150**, and allows the first communications device **200** to communicate with the token management server **500**. Further, where the first communications device **200** is implemented as a web server, the WAN interface **208** may allow the second communications device **300** to communicate with the first communications device **200** via the wide area network **140**.

[0052] The data processing system **210** includes a microprocessor **212** and a non-transient computer-readable medium **214**. The non-transient computer-readable medium **214** may be provided as non-volatile electronic computer memory (e.g. FLASH memory), as an example. The non-transient computer-readable medium (memory) **214** may store a device identifier (e.g. an IMEI (International Mobile Equipment Identifier)) that is uniquely associated with the first communications device **200**. The memory **214** may also store computer processing instructions which, when accessed from the memory **214** and executed by the microprocessor **212**, implement at least an operating system **218**, a token initiation processor **220** and a validation code transmitter **222**.

[0053] The operating system **218** allows the first communications device **200** to accept user input from the input device **202** (if present) and to display information on the display device **204** (if present). The operating system **218** also allows the first communications device **200** to communicate with the token management server **500** (via the WAN interface **208**). Further, where the first communications device **200** is implemented as a web server, the operating system **218** also allows the first communications device **200** to communicate with the second communications device **300**.

[0054] The operator of the first communications device **200** may use the first communications device **200** to initiate delivery of a limited-use token to an identified recipient. The token initiation processor **220** may be configured to initiate

the delivery of the token by, for example, transmitting to the token management server **500** a funding request message that includes a validation code and an authorization limit.

[0055] As will be discussed below, the funding request message may also include a destination address (e.g. telephone number, e-mail address) that is associated with the identified recipient, and the token management server **500** may respond to the funding request message, for example, by associating a unique reference identifier with the validation code and the authorization limit, and initiating a transfer (into a pooling ledger) of a funding amount equal to the authorization limit. The token management server **500** may then transmit the reference identifier to the identified recipient at the destination address.

[0056] As will be discussed, the pooling ledger and the subledger may each track monetary funds that are deposited into and/or withdrawn from an associated financial account (e.g. debit account, credit account), and the funding amount may be the quantum of a payment amount that is transferred into the pooling ledger. Alternately, the pooling ledger and the subledger may each track loyalty points that are deposited into and/or withdrawn from an associated loyalty points account, and the funding amount may be the quantum of loyalty points that are transferred into the pooling ledger.

[0057] The funding request message may also include a user identifier that is uniquely associated with the first communications device **200** (or the operator thereof). The token management server **500** may initiate the transfer (into the pooling ledger) of the funding amount, for example, by obtaining authorization (e.g. from the authorization server **700**) for a funds/points transfer of the funding amount from a source ledger that is associated with the user identifier.

[0058] The operator of the first communications device **200** may also use the first communications device **200** to provide the identified recipient with the validation code. If the identified recipient is in possession of the second communications device **300**. and the second communications device **300** is deployed in close proximity to the first communications device **200**, the validation code transmitter **222** may be configured to provide the identified recipient with the validation code by, for example, generating a visual representation of the validation code (e.g. a two-dimensional bar code (QR code)) and displaying the visual representation on the display device **204** for capture by the second communications device **300**.

[0059] Alternately, where the first communications device **200** includes the LAN interface **206** (e.g. the first communications device **200** is implemented as a wireless communications terminal or a personal computer), the validation code transmitter **222** may be configured to provide the second communications device **300** with the validation code by transmitting the validation code to the second communications device **300** via the LAN interface **206**, over a short-range wireless connection or a wired connection established with the second communications device **300**.

[0060] Where the first communications device **200** does not include the LAN interface **206** and/or is not deployed in close proximity to the second communications device **300** (e.g. the first communications device **200** is implemented as a web server), the validation code transmitter **222** may be configured to provide the second communications device **300** with the validation code by transmitting the validation code to the second communications device **300** via the WAN interface **208**. In this variation, the first communications device **200** may receive a request from the second communications device **300** (via the WAN interface **208**) for a limited-use token, and the validation code transmitter **222** may respond to the token request by transmitting the validation code to the second communications device **300** via the WAN interface **208**.

Second Communications Device

[0061] The second communications device **300** may be implemented as a wireless communications terminal, such as a portable digital assistant (PDA), a tablet computer or a smartphone. Alternately, the second communications device **300** may be implemented as a wired communications terminal, such as a personal computer.

[0062] As shown in FIG. **3**, the second communications device **300** may include an input device **302**, a display device **304**, a wide area network (WAN) interface **308**, and a data processing system **310** that is in communication with the input device **302**, the display device **304** and the WAN interface **308**. Where the first communications device **200** is implemented as a wireless communications terminal, the second communications device **300** may also include a local area network (LAN) interface **306** and an image capture device (e.g. CCD image sensor) **309** that is communication with the data processing system **310**.

[0063] The input device **302** may be implemented as a keyboard, touchpad, touchscreen or other input device suitable for allowing the operator to input data and/or commands into the second communications device **300**. The display device **304** may be implemented as a liquid crystal display (LCD) panel, plasma display panel, or other display device suitable for displaying information to the operator of the second communications device **300**.

[0064] The LAN interface **306** (if present) may interface the second communications device **300** with the first communications device **200** and/or the POS station **400**. The LAN interface **306** may be configured as a wireless interface that allows the second communications device **300** to communicate directly with the first communications device **200** and/or the POS station **400** via a short-range wireless connection, such as a Bluetooth, or a Near Field Communications (NFC) connection, as examples. Alternately, the LAN interface **306** may be configured as a wired interface that allows the second communications device **300** to communicate directly with the first communications device **200** and/or the POS station **400** via a wired connection, such as a Universal Serial Bus (USB) connection, as an example.

[0065] The WAN interface **308** interfaces the second communications device **300** with the wide area network **140** and/or the mobile communications network **150**, and allows the second communications device **300** to communicate with the token management server **500** and/or the TSP server **600**. Further, where the first communications device **200** is implemented as a web server, the WAN interface **308** may allow the second communications device **300** to communicate with the first communications device **200** via the wide area network **140**.

[0066] The data processing system **310** includes a microprocessor **312** and a non-transient computer-readable medium **314**. The non-transient computer-readable medium **314** may be provided as non-volatile electronic computer memory (e.g. FLASH memory), as an example. The non-transient computer-readable medium (memory) **314** may store a device identifier (e.g. an IMEI) that is uniquely

associated with the second communications device **300**. The memory **314** may also store computer processing instructions which, when accessed from the memory **314** and executed by the microprocessor **312**, implement at least an operating system **318**, a validation code receiver **320**, a token import processor **322**, and a token redemption processor **324**.

[0067] The operating system **318** allows the second communications device **300** to accept user input from the input device **302** and to display information on the display device **304**. The operating system **318** also allows the second communications device **300** to communicate with the first communications device **200** via the LAN interface **306** (if present), and to communicate with the first communications device **200** via the WAN interface **308** (where the first communications device **200** is implemented as a web server). Further, the operating system **318** allows the second communications device **300** to communicate with the token management server **500** and/or the TSP server **600** (via the WAN interface **308**).

[0068] The operator of the second communications device **300** may use the second communications device **300** to receive a validation code from the first communications device **200**. Where the first communications device **200** is configured to display a visual representation of the validation code on the display device **204**, and the second communications device **300** is deployed in close proximity to the first communications device **200**, the validation code receiver **320** may be configured to receive the validation code from the first communications device **200** by capturing the visual representation via the image capture device **309** (if present), and recovering the validation code from the captured image.

[0069] Alternately, where the second communications device **300** includes the LAN interface **306**, the validation code receiver **320** may be configured to receive the validation code from the first communications device **200** via the LAN interface **206**, over a short-range wireless connection or a wired connection established with the first communications device **200**.

[0070] Where the second communications device **300** does not include the LAN interface **306** or is not deployed in close proximity to the first communications device **200** (e.g. the first communications device **200** is implemented as a web server), the validation code receiver **320** may be configured to receive the validation code from the first communications device **200** via the WAN interface **308**.

[0071] The operator of the second communications device **300** may also use the second communications device **300** to import a limited-use token from the token processing network **100**. The token import processor **322** may be configured to import the limited-use token by transmitting to the token management server **500** a token request that includes a credential and a reference identifier.

[0072] As discussed, the first communications device **200** may have transmitted to the token management server **500** a funding request message that included a validation code and a destination address. The destination address may be a network address (e.g. telephone number, e-mail address) that is associated with the second communications device **300** (or the operator thereof) and, therefore, the token management server **500** may have responded to the funding request message, for example, by associating a reference identifier with the validation code, and transmitting the reference identifier to the second communications device **300** using the specified destination address.

[0073] As will be discussed, the token management server **500** (independently of, or in association with, the TSP server **600**) may respond to the token request, for example, by generating a subledger identifier, associating a limited-use token with the pooling ledger identifier and the subledger identifier, and providing the second communications device **300** with the limited-use token. The token request may also include a user identifier that is uniquely associated with an operator of the second communications device **300**. Therefore, the token management server **500** may provide the second communications device **300** with the limited-use token by locating a device identifier that is associated with the user identifier, and transmitting the limited-use token to a communications device having the device identifier.

[0074] The second communications device **300** may receive the limited-use token, and the token import processor **322** save the limited-use token in the memory **314**.

[0075] Further, prior to at least providing the second communications device **300** with the limited-use token, the token management server **500** may respond to the token request, for example, by locating the validation code that the token management server **500** had previously associated with the reference identifier, and confirming that the credential included in the token request matches the located validation code.

[0076] In this implementation, the second communications device **300** may provide the token management server **500** with the token request via the wide area network **140**, and may receive the limited-use token from the TSP server **600** via the mobile communications network **150**. Therefore, the token management server **500** (independently of, or in association with, the TSP server **600**) may provide the second communications device **300** with the limited-use token over a communications channel that is distinct from the communications channel over which the token management server **500** receives the token request.

[0077] The operator of the second communications device **300** may also use the second communications device **300** to redeem a limited-use token with the token processing network **100**. The token redemption processor **324** may be configured to redeem the limited-use token by reading a user input from the input device **302**, authenticating the operator of the second communications device **300** from the user input, and transmitting the limited-use token to the POS station **400** after successfully authenticating the appliance operator.

[0078] As will be discussed, the POS station **400** may receive the limited-use token from the second communications device **300**, and may respond by generating a token authorization request that includes the limited-use token and an authorization value, and transmitting the token authorization request to the authorization server **700**.

[0079] As discussed, the token management server **500** may have received a funding request message, and may have responded to the funding request message, for example, by initiating a transfer (into a pooling ledger) of a funding amount equal to the authorization limit. The token management server **500** may also have received a token request message, and may have responded to the token request message, for example, by establishing a subledger, associating a subledger identifier with the subledger, associating a limited-use token with a polling ledger identifier and the

subledger identifier, and setting/initializing a balance value of the subledger equal to the authorization limit. Therefore, the token management server **500** (independently of, or in association with, the TSP server **600**) may respond to the token authorization request for example, by locating the pooling ledger identifier and the subledger identifier that the token management server **500** had previously associated with the limited-use token, determining a balance value of the subledger that is associated with the subledger identifier, and confirming that the balance value is at least equal to the authorization value. The token management server **500** may then identify the pooling ledger that is associated with the ledger identifier, and initiate a transfer (from the pooling ledger) of a transfer amount equal to the authorization value.

[0080] Further, as discussed, the pooling ledger and the subledger may each track monetary funds that are deposited into and/or withdrawn from an associated financial account (e.g. debit account, credit account). Therefore, the transfer amount may be the quantum of a payment amount that is transferred from the pooling ledger. Alternately, the pooling ledger and the subledger may each track loyalty points that are deposited into and/or withdrawn from an associated loyalty points account. Therefore, the transfer amount may be the quantum of loyalty points that are transferred from the pooling ledger.

[0081] The token management server **500** may initiate the transfer (from the pooling ledger) of the transfer amount, for example, by obtaining authorization (e.g. from the authorization server **700**) for a funds/points transfer of the transfer amount from the pooling ledger, and reducing the balance value of the subledger by the authorization value.

[0082] The second communications device **300** may receive an authorization response message (e.g. including the current balance value in the subledger) from the authorization server **700** in response to the token authorization request. The token redemption processor **324** may display the contents of the authorization response message on the display device **302**.

Point-of-Sale (POS) Station

[0083] The point-of-sale (POS) station **400** may be implemented as an integrated point-of-sale (POS) terminal, or as a pin-pad device that communicates with an electronic cash register (ECR). Alternately, the point-of-sale (POS) station **400** may be implemented as a computer server, such as a merchant web server.

[0084] As shown in FIG. **4**, the POS station **400** includes a WAN interface **408** and a data processing system **410** that is in communication with the WAN interface **408**. If the POS station **400** is implemented as a POS terminal or as a pin-pad device, the POS station **400** may also include an input device **402**, a display device **404**, and a local area network (LAN) interface **406**. In this latter implementation, the data processing system **410** is in communication with the input device **402**, the display device **404**, the LAN interface **406**, and the WAN interface **408**.

[0085] The input device **402** (if present) may be implemented as a keyboard, touchpad, touchscreen or other input device suitable for allowing the operator to input data and/or commands into the POS station **400**. The display device **404** (if present) may be implemented as a liquid crystal display (LCD) panel, plasma display panel, or other display device suitable for displaying information to the operator of the POS station **400**.

[0086] The LAN interface **406** may interface the POS station **400** with the second communications device **300**. The LAN interface **406** may be configured as a wireless interface that allows the POS station **400** to communicate directly with the second communications device **300** via a short-range wireless connection, such as a Bluetooth, or a Near Field Communications (NFC) connection, as examples. Alternately, the LAN interface **406** may be configured as a wired interface that allows the POS station **400** to communicate directly with the second POS station **400** via a wired connection, such as a Universal Serial Bus (USB) connection, as an example.

[0087] The WAN interface **408** interfaces the POS station **400** with the payment network **160** and allows the POS station **400** to communicate with the financial institution server **700** via the payment network **160**.

[0088] The data processing system **410** includes a microprocessor **412** and a non-transient computer-readable medium **414**. The non-transient computer-readable medium **414** may be provided as non-volatile electronic computer memory (e.g. FLASH memory), as an example. The memory **414** may store computer processing instructions which, when accessed from the memory **414** and executed by the microprocessor **412**, implement at least an operating system **418**, and a token processor **420**.

[0089] The operating system **418** allows the POS station **400** to accept user input from the input device **402** and to display information on the display device **404**. The operating system **418** also allows the POS station **400** to communicate with the authorization server **700** (via the WAN interface **408**).

[0090] The token processor **420** allows the POS station **400** to receive limited-use tokens from the second communications device **300**, accept authorization values from the input device **402**, generate token authorization requests from the limited-use tokens and the authorization values, and transmit the token authorization requests to the authorization server **700** via the payment network **160**. The token processor **420** also allows the POS station **400** receive authorization responses from the authorization server **700**, via the payment network **160**, and to display the results thereof on the display device **404**.

Token Management Server **500**

[0091] As shown in FIG. **5**, the token management server **500** includes a wide area network (WAN) interface **502**, and a data processing system **504** that is in communication with the WAN interface **502**.

[0092] The WAN interface **502** interfaces the token management server **500** with the wide area network **140** and/or the mobile communications network **150**, and allows the token management server **500** to communicate with the first communications device **200** and/or the second communications device **300** via the wide area network **140** and/or the mobile communications network **150**. The WAN interface **502** also allows the token management server **500** to communicate with the POS station **400** and the authorization server **700** via the wide area network **140**.

[0093] The data processing system **504** includes one or more microprocessors **506**, a volatile computer-readable memory **508** and a non-transient computer-readable medium **510**. The non-transient computer-readable medium **510** may be provided as one or more of a magnetic storage drive and a solid-state drive.

[0094] The computer-readable medium **510** may store a funding database **512** and a subledger database **514**. Alternately, the funding database **512** and/or the subledger database **514** may be deployed on a database server (not shown) that is distinct from the token management server **500**, and the token management server **500** may be configured to access the funding database **512** and/or the subledger database **514** via a secure communications channel.

[0095] The funding database **512** may store a plurality of database records each uniquely associated with a respective electronic gift (eGift) (e.g. monetary payment, loyalty points) and a respective (eGift) reference identifier. Each database record of the funding database **512** identifies one of the (eGift) reference identifiers, an associated validation code, and an authorization limit. Each (eGift) reference identifier is uniquely associated with the respective eGift.

[0096] The subledger database **514** may store a plurality of database records each uniquely associated with a respective subledger and a respective subledger identifier. Each database record of the subledger database **514** records deposit/withdrawal entries to the associated subledger, and identifies one of the subledger identifiers and a balance value of the net value of the deposit/withdrawal entries to the subledger. Each subledger identifier is uniquely associated with the respective subledger.

[0097] The computer-readable medium **510** also maintains computer processing instructions stored thereon which, when copied into the volatile computer-readable memory **508**, and executed by the microprocessor(s) **506** from the volatile computer-readable memory **508**, implement at least an operating system **520**, a funding request processor **522**, a token request processor **524** and a token authorization processor **526**.

[0098] The operating system **520** allows the token management server **500** to at least communicate with the communications devices **200**, **300**, the TSP server **600** and the authorization server **700** (via the WAN interface **502**).

[0099] The token management server **500** transforms funding requests (received from the first communications device **200**) into pooling ledger transfers. The funding request processor **522** may be configured to transform the funding requests by, for example, (a) receiving from one of the communications devices (e.g. the first communications device **200**) a funding request that includes a validation code and an authorization limit, and (b) initiating a transfer (into a pooling ledger) of a funding amount equal to the authorization limit.

[0100] The funding request processor **522** may also save a unique (eGift) reference identifier in the funding database **512** in association with the validation code and the authorization limit. The funding request processor **522** may ensure that each reference identifier is unique to the token processing network **100** by saving each new reference identifier in the funding database **512** only after confirming that the reference identifier has not previously been saved to the funding database **512**.

[0101] The token management server **500** (independently of, or in association with, the TSP server **600**) also transforms token requests (received from the second communications device **300**) into limited-use tokens. The token request processor **524** may be configured to transform the token requests by, for example:

[0102] (a) receiving from one of the communications devices (e.g. the second communications device **300**) a token request that includes a (eGift) reference identifier and a credential,

[0103] (b) locating in the funding database **512** the validation code that is associated with the (eGift) reference identifier, and confirming that the credential matches the validation code,

[0104] (c) establishing a subledger in the subledger database **514**, associating a subledger identifier with the subledger in the subledger database **514**, setting/initializing a balance value of the subledger equal to the authorization limit, and saving the balance value in the subledger, and

[0105] (d) providing the one communications device with the limited-use token.

[0106] The token request processor **524** may also generate a unique limited-use token and associate the limited-use token with the subledger identifier and a polling ledger identifier of the pooling ledger. The token request processor **524** may ensure that each limited-use token is unique to the token processing network **100** by generating the limited-use token using a noise generator or a suitable pseudo-random generator. The token request processor **524** may ensure that each subledger identifier is unique to the token processing network **100** by saving each new subledger identifier in the subledger database **514** only after confirming that the subledger identifier has not been previously saved to the subledger database **514**.

[0107] Alternately, the limited-use token may be provided to the one communications device over a communications channel that is different from the communications channel over which the token request processor **524** received the token request. Therefore, as will be discussed, the token management server **500** may receive the token request from the second communications device **300** via the wide area network **140**, and the token request processor **524** may establish a subledger, associate a unique subledger identifier with the subledger, and transmit to the TSP server **600** a token requisition that includes the subledger identifier and a pooling ledger identifier. The TSP server **600** may respond to the token requisition by generating the unique limited-use token, associating the unique limited-use token with the subledger identifier and the pooling ledger identifier, and transmitting the limited-use token to the second communications device **300** via the mobile communications network **150**.

[0108] The token management server **500** (independently of, or in association with, the TSP server **600**) also transforms token authorization requests (received from the POS station **400**) into pooled account authorization requests. The token authorization processor **526** may be configured to transform the token authorization requests by, for example:

[0109] (a) receiving from the POS station **400** a token authorization request that includes a limited-use token and an authorization value,

[0110] (b) locating the subledger identifier that is associated with the limited-use token, and confirming that the balance value of the subledger associated with the subledger identifier in the subledger database **514** is at least equal to the authorization value, and

[0111] (c) locating the pooling ledger identifier that is associated with the limited-use token, and initiating a

transfer from the pooling ledger (associated with the pooling ledger identifier) of a transfer amount equal to the authorization value.

Token Service Provider (TSP) Server

[0112] As shown in FIG. **6**, the TSP server **600** includes a wide area network (WAN) interface **602**, and a data processing system **604** that is in communication with the WAN interface **602**.

[0113] The WAN interface **602** interfaces the TSP server **600** with the wide area network **140** and/or the mobile communications network **150**, and allows the TSP server **600** to communicate with the token management server **500** and the authorization server **700** via the wide area network **140**. The WAN interface **602** also allows the TSP server **600** to communicate with the second communications device **300** via the mobile communications network **150**.

[0114] The data processing system **604** includes one or more microprocessors **606**, a volatile computer-readable memory **608** and a non-transient computer-readable medium **610**. The non-transient computer-readable medium **610** may be provided as one or more of a magnetic storage drive and a solid-state drive.

[0115] The computer-readable medium **610** may store an address database **612** and a token database **614**. Alternately, the address database **612** and/or the token database **614** may be deployed on a database server (not shown) that is distinct from the TSP server **600**, and the TSP server **600** may be configured to access the address database **612** and/or the token database **614** via a secure communications channel.

[0116] The address database **612** may store a plurality of database records each uniquely associated with a respective communications device **200**, **300**. Each database record of the address database **612** stores a device identifier (e.g. an IMEI) that is uniquely associated with the respective communications device **200**, **300**, and a user identifier that is uniquely associated with the operator of the respective communications device **200**, **300**.

[0117] The token database **614** may store a plurality of database records each uniquely associated with a respective limited-use token. Each database record of the token database **614** stores a limited-use token (e.g. a unique sequence of digits) in association with a (eGift) reference identifier and a pooling ledger identifier.

[0118] The computer-readable medium **610** also maintains computer processing instructions stored thereon which, when copied into the volatile computer-readable memory **608**, and executed by the microprocessor(s) **606** from the volatile computer-readable memory **608**, implement at least an operating system **620**, a token delivery processor **622** and a subledger recovery processor **624**.

[0119] The operating system **620** allows the TSP server **600** to at least communicate with the second communications device **300**, the token management server **500** and the authorization server **700** (via the WAN interface **602**).

[0120] The TSP server **600** may transform token requisitions (received from the token management server **500**) into limited-use tokens. The token delivery processor **622** may be configured to transform the token requisitions by, for example:

[0121] (a) receiving (e.g. from the token management server **500**) a token requisition that includes a pooling ledger identifier and a user identifier,

[0122] (b) locating in the address database **612** the device identifier that is associated with the user identifier (e.g. the device identifier of the second communications device **300**),

[0123] (c) generating a unique limited-use token and a unique subledger identifier, and saving the limited-use token in the token database **614** in association with the subledger identifier and the pooling ledger identifier, and

[0124] (d) transmitting the limited-use token to the communications device (e.g. the second communications device **300**) associated with the device identifier.

[0125] The token delivery processor **622** may ensure that each limited-use token and subledger identifier is unique to the token processing network **100** by saving each new limited-use token and each new subledger identifier in the token database **614** only after confirming that the limited-use token and the subledger identifier has not previously saved to the token database **614**.

[0126] The TSP server **600** may also transform token authorization requests (received from the POS station **400** via the financial institution server **700**) into pooled account authorization requests. The subledger recovery processor **624** may be configured to transform the token authorization requests by, for example:

[0127] (a) receiving from the POS station **400** (via the authorization server **700**) a token authorization request that includes a limited-use token and an authorization value,

[0128] (b) locating in the token database **614** the pooling ledger identifier that is associated with the limited-use token, and

[0129] (c) initiating a transfer from the pooling ledger (associated with the pooling ledger identifier) of a transfer amount equal to the authorization value.

Authorization Server

[0130] The authorization server **700** may be administered by a financial or other institution that maintains monetary payment and/or loyalty points accounts for its customers.

[0131] The authorization server **700** maintains (or is in communication with) a ledger database (not shown) and a user profile database (not shown).

[0132] The ledger database includes a plurality of database records each uniquely associated with a respective ledger. Each database record of the ledger database stores a unique ledger identifier and may track monetary funds or loyalty points that are deposited into and/or withdrawn from the associated ledger.

[0133] The user profile database includes a plurality of database records each uniquely associated with a respective customer of the financial institution. Each database record of the user profile database stores one or more user credentials (e.g. userID, password) assigned to the associated customer, in association with at least one of the ledger identifiers.

[0134] As discussed above, the token management server **500** transforms funding requests into pooling ledger transfers and subledger initializations. Therefore, the ledger database maintains at least a pooling ledger (associated with a pooling ledger identifier) and one or more subledgers (each associated with a respective subledger identifier). Further, the authorization server **700** is configured to receive source ledger authorization requests (each including a session token and an authorization limit) from the token management

server **500**, and to determine whether a current balance of funds/points in the associated subledger is at least equal to the authorization limit.

[0135] The token management server **500** (independently of, or in association with, the TSP server **600**) also transforms token authorization requests into pooled ledger authorization requests. Therefore, the authorization server **700** is also configured to receive pooled ledger authorization requests (each including a pooling ledger identifier and an authorization amount) from the token management server **500** and/or the TSP server **600**, and to determine whether a current balance of funds/points in the associated pooling ledger is at least equal to the authorization value.

Method of Processing Limited-Use Tokens

[0136] As discussed, the token processing network **100** implements a method of processing limited-use tokens. A sample embodiment of the token processing method will be discussed with reference to FIGS. **7**A, **7**B, **7**C and **7**D. In this embodiment, the token management server **500** (either independently of, or in association with, the TSP server **600**) associates at least one limited-use token with a pooling ledger identifier and a respective subledger identifier, and subsequently receives from the POS station **400** a token authorization request that includes a limited-use token and an authorization value.

[0137] The token management server **500** (either independently of, or in association with, the TSP server **600**) locates the pooling ledger identifier and the subledger identifier that are associated with the limited-use token, determines a balance value of the subledger that is associated with the subledger identifier, and confirms that the balance value is at least equal to the authorization value. The token management server **500** then initiates a transfer from a pooling ledger that is associated with the ledger identifier of a transfer amount that is equal to the authorization value.

[0138] An example token processing method will now be discussed in detail with reference to FIGS. **7**A, **7**B, **7**D and **7**D. In the following example, the authorization server **700** maintains a ledger ("source ledger") that is uniquely associated with the operator of the first communications device **200**. The source ledger includes a source ledger identifier, and tracks funds (monetary funds, loyalty points) that are deposited into and/or withdrawn from the source ledger.

[0139] Similarly, the authorization server **700** maintains at least one ledger ("pooling ledger") each uniquely associated with an entity that may administer the token management server **500**. Each pooling ledger includes a pooling ledger identifier, and tracks funds (monetary funds, loyalty points) that are deposited into and/or withdrawn from the pooling ledger.

[0140] The operator of the first communications device **200** intends to transfer an electronic gift (e.g. monetary funds or loyalty points) to the operator of the second communications device **300**. At least the operator of the first communications device **300** has one on more user credentials that authenticate the operator to the authorization server **700** and, therefore, the user profile database stores a copy of the user credential(s).

[0141] The operator of the second communications device **300** need not maintain an account with the financial institution or register with the token processing network **100**. However, in one implementation discussed below, the operator of the second communications device **300** has a user identifier that identifies the operator to the TSP server **600**, and the address database **612** stores the operator's user identifier in association with the device identifier of the second communications device **300**.

(i) Initiate Delivery of Limited-Use Token

[0142] At the outset of the method, the operator of the first communications device **200** may authenticate to the token processing network **100** by entering into the first communications device **200**, via the input device **202**, one on more user credentials that authenticate the operator to the authorization server **700**.

[0143] The communications device **200** may then establish an encrypted communications session (e.g. SSL, TLS) with the token management server **500**, via the wide area network **140** or the mobile communications network **150**. At step S**700**, the first communications device **200** generates an authentication request message that includes the user credential(s), and transmits the authentication request message to the token management server **500**, via the encrypted communications session.

[0144] In response to the authentication request message, the token management server **500** generates a session request message that includes the user credential(s), and transmits the session request message to the authorization server **700**, via the wide area network **140**, at step S**702**.

[0145] In response to the session request message, the authorization server **700** authenticates the user credential(s) against the user profile database. If the operator of the first communications device **200** is successfully authenticated, (i.e. the user credential(s) correspond to one of the database records in the user profile database), the authorization server **700** locates the (source) ledger identifier that is associated with the user credential(s) in the user profile database, generates a unique session token, and associates the session token with the (source) ledger identifier. In this example, the (source) ledger identifier identifies a source ledger that is maintained by the financial institution on behalf of the operator of the first communications device **200**.

[0146] The authorization server **700** then generates a session response message that includes the session token and indicates that the user credential(s) was/were successfully authenticated, and transmits the session response message to the token management server **500**, via the wide area network **140**, at step S**704**.

[0147] In response to the session response message, the token management server **500** associates the session token with the encrypted communications session, generates an authentication response message that indicates that the operator of the first communications device **200** was successfully authenticated, and transmits the authentication response message to the first communications device **200**, via the encrypted communications session, at step S**706**.

[0148] After the first communications device **200** receives the authentication response message, the first communications device **200** may display the results of the authentication response message on the display device **204**. The operator of the first communications device **200** then initiates delivery of a limited-use token to the operator of the second communication appliance **300** by entering an authorization limit value and a validation code into the first communications device **200**, via the input device **202**. The operator of the first communications device **200** may also enter, into the first communications device **200**, a destination

address (e.g. telephone number, e-mail address) that is associated with the operator of the second communication appliance **300**.

[0149] At step S**708**, the token initiation processor **220** generates a funding request message that includes the validation code and the authorization limit (and the destination address, if input to the first communications device **200**), and the first communications device **200** transmits the funding request message to the token management server **500**, via the encrypted communications session.

[0150] In response to the funding request message, the funding request processor **522** of the token management server **500** generates a source ledger authorization request message that includes the authorization limit and the session token, and requests authorization for a funds transfer (monetary amount, loyalty points) in a funding amount equal to the authorization limit. The token management server **500** then transmits the source ledger authorization request message to the authorization server **700**, via the wide area network **140**, at step S**710**.

[0151] In response to the source ledger authorization request message, the authorization server **700** uses the session token to identify the source ledger that is associated with the operator of the first communications device **200** (previously determined at step S**704**), and then determines whether source ledger has sufficient funds (monetary amount, loyalty points) to complete the funds transfer (i.e. the balance of funds in the source ledger is at least equal to the funding amount).

[0152] If the authorization server **700** determines that the source ledger has sufficient funds to complete the funds transfer, the authorization server **700** reduces the available balance value associated with the source ledger by an amount equal to funding amount, and may generate authorization code from at least a private cryptographic key of the authorization server **700**, the source ledger identifier and the funding amount. The authorization server **700** also generates a source ledger authorization response message that may include the authorization code and indicates that the funds transfer was authorized, and transmits the source ledger authorization response message to the token management server **500**, via the wide area network **140**, at step S**712**.

[0153] In response to the source ledger authorization response message, the funding request processor **522** generates a unique (eGift) reference identifier, and saves the (eGift) reference identifier in the funding database **512** in association with the validation code and the authorization limit, at step S**714**. The funding request processor **522** may also associate a status identifier with the (eGift) reference identifier, indicating that the associated electronic gift has not been claimed. The token management server **500** then provides the operator of the second communications device **300** with the (eGift) reference identifier at step S**716**, for example, by transmitting the (eGift) reference identifier to the destination address included in the funding request message.

[0154] After the token management server **500** receives one or more subledger authorization response messages, the token management server **500** may initiate completion of the funds transfer from the source ledgers by generating a clearing payload that includes one or more of the authorization codes, the associated funding amounts and the pooling ledger identifier of a pooling ledger maintained by the financial institution on behalf of the token management server **500**. The token management server **500** may transmit the clearing payload to the authorization server **700** via the payment network **160**, and the authorization server **700** may use its cryptographic key to confirm that the authorization server **700** generated the authorization codes, and may transfer the funding amounts from the source ledgers into the pooling ledger that is associated with the pooling ledger identifier.

(ii) Import Limited-Use Token

[0155] At step S**718** (the timing of which is independent of whether the (eGift) reference identifier has already been provided to the operator of the second communications device **300** and whether the funding amount has already been transferred into the pooling ledger), the operator of the first communications device **200** provides the operator of the second communications device **300** with the validation code that is associated with the (eGift) reference identifier. The operator of the first communications device **200** may provide the validation code by any suitable means, including using the validation code transmitter **222** of the first communications device **200** to generate a visual representation of the validation code and displaying the visual representation on the display **202** for capture by the second communications device **300**.

[0156] After the operator of the second communications device **300** receives both the (eGift) reference identifier and the associated validation code, the operator thereof may then request receipt of a limited-use token by invoking the token import processor **322**, via the input device **302**. The token import processor **322** may then generate a token request message that includes the (eGift) reference identifier and a credential (i.e. the associated validation code, and the unique device identifier of the second communications device **300**.

[0157] Alternately, the token import processor **322** may prompt the operator of the second communications device **300** to input a user identifier into the second communications device **300**. The operator may then enter the user identifier into the second communications device **300**, via the input device **302**, and the token import processor **322** may generate a token request message that includes the (eGift) reference identifier and a credential (i.e. the associated validation code), and the user identifier of the operator.

[0158] The communications device **300** may then establish an encrypted communications session (e.g. SSL, TLS) with the token management server **500**, via the wide area network **140** or the mobile communications network **150**. At step S**720**, the second communications device **300** transmits the token request message to the token management server **500**, via the encrypted communications session.

[0159] In response to the token request message, the token request processor **524** of the token management server **500** locates in the funding database **512** the validation code that was saved therein in association with the (eGift) reference identifier (at step s**714**). At step S**722**, the token request processor **524** validates the token request message by confirming that the (eGift) reference identifier+credential included in the token request message matches the (eGift) reference identifier+validation code saved in the funding database **512**.

[0160] If the token request processor **524** successfully validates the token request message, at step S**724** the token request processor **524** generates a new unique subledger identifier, establishes a new subledger in the subledger

database **514**, and saves the subledger identifier in the subledger database **514** in association with the new subledger identifier. The token request processor **524** also sets/initializes a balance value of the subledger equal to the authorization limit, and saves the balance value in the subledger. The token request processor **524** may also update the status identifier that is associated with the (eGift) reference identifier in the funding database **512**, indicating that the associated electronic gift has now been claimed.

[0161] At step S**726**, the token request processor **524** generates a token requisition message that includes the subledger identifier, the device identifier of the second communications device **300** (or the user identifier of the operator thereof), and the pooling ledger identifier of one of the pooling ledgers that is maintained by the financial institution on behalf of the token management server **500**. The token management server **500** then transmits the token requisition message to the TSP server **600**, via the wide area network **140**.

[0162] As will be discussed, after the TSP server **600** receives a limited-use token from the POS station **400**, the token management server **500** initiates a transfer of a "transfer amount" of funds (monetary amounts, loyalty tokens) to a merchant, from the pooling ledger that is referenced in the token requisition message. Therefore, typically the pooling ledger referenced in the token requisition message is the same pooling ledger into which the funding amount was previously transferred (from the source ledger). However, the entity associated with the token management server **500** may elect to use, for the transfer of a transfer amount, a pooling ledger that is different from the pooling ledger that was used for the transfer of the funding amount.

[0163] In response to the token requisition message, at step S**728** the token delivery processor **622** of the TSP server **600** generates a unique limited-use token, and saves the limited-use token in the token database **614** in association with the subledger identifier and the pooling ledger identifier. Preferably, the limited-use token is a unique sequence of digits that is prefixed with an Issuer Identification Number (IIN) that indicates that the limited-use token was generated by the TSP server **600** on behalf of the financial institution.

[0164] The token delivery processor **622** may then locate in the address database **612** the device identifier that is associated with the user identifier in the address database **612**. At step S**730**, the TSP server **600** may then use the device identifier (and, for example, a push notification service) to transmit the limited-use token to the intended recipient (e.g. the second communications device **300**), via the mobile communications network **150**.

[0165] In this implementation, the TSP server **600** uses the device identifier stored in the address database **612** as the destination address for the limited-use token. Therefore, depending upon the device identifier that is associated with the user identifier in the address database **612**, the TSP server **600** may transmit the limited-use token to a destination other than the second communications device **300**. However, if the token requisition message already includes a device identifier, the token delivery processor **622** may not query the address database **612** for the device identifier, and (at step S**730**) the TSP server **600** may instead use the device identifier received from the second communications device **300** as the destination address for the limited-use token.

[0166] Upon receipt of the limited-use token, the token import processor **322** may save the limited-use token in the memory **314**.

(iii) Redeem Limited-Use Token

[0167] After the second communications device **300** receives the limited-use token, the operator of the second communications device **300** may use the limited-use token to complete a transaction with a merchant.

[0168] As noted above, the POS station **400** may be implemented as a POS terminal or pin-pad device. In this situation, the operator may attend at the premises of the merchant and select a good or service that is available from the merchant. The merchant may then enter the required payment amount ("authorization amount") for the transaction into POS/pin-pad terminal **400** via the input device **402**. In response, the token processor **420** of the POS/pin-pad terminal **400** may prompt the operator for a payment token.

[0169] The operator may then initiate completion of the transaction by interfacing the second communications device **300** with the POS/pin-pad terminal **400** via the LAN interface **306**, and invoking the token redemption processor **324** on the second communications device **300** via the input device **302**. In response, the token redemption processor **324** may transmit the limited-use token to the POS/pin-pad terminal **400** via the LAN interface **306**, at step S**732**.

[0170] Alternately, the POS station **400** may be implemented as a merchant web server. In this situation, the second communications device **300** may initiate a communications session with the web server **400** via the WAN interface **308**, and the operator may use the second communications device **300** to select a good or service that is available from the web server **400**. The token processor **420** may then read the required payment amount ("authorization amount") for the transaction (e.g. from a merchant database, not shown), and may prompt the operator for a payment token.

[0171] The operator may then initiate completion of the transaction by invoking the token redemption processor **324**. In response, the token redemption processor **324** may transmit the limited-use token to the web server **400** via the WAN interface **308**, at step S**732**.

[0172] After the POS station (POS/pin-pad terminal, web server) **400** receives the limited-use token, the token processor **420** generates a token authorization request message that includes the limited-use token and the authorization value, and transmits the token authorization request message over the payment network **160**, at step S**734**. Since the limited-use token is prefixed with the IIN of the financial institution, the payment network **160** directs the token authorization request message to the authorization server **700**.

[0173] After the authorization server **700** receives the token authorization request message, the authorization server **700** determines from the IIN of the limited-use token that the TSP server **600** generated the limited-use token on behalf of the financial institution. Therefore, at step S**736**, the authorization server **700** redirects the token authorization request message to the TSP server **600**.

[0174] After the TSP server **600** receives the token authorization request message, the subledger recovery processor **624** of the TSP server **600** initiates transforming the token authorization request message into a pooled account authorization request message by locating in the token database

614 the subledger identifier that is associated with the limited-use token in the token database **614** (step S**738**), generating a token validation request message that includes the subledger identifier and the authorization value, and transmitting the validation request message to the token management server **500** via the wide area network **140** (step S**740**).

[0175] After the token management server **500** receives the token validation request message, the token authorization processor **526** of the token management server **500** validates the limited-use token by locating the subledger that is associated with the subledger identifier in the subledger database **514**, and confirming that the balance value of the subledger is at least equal to the authorization value, at step S**742**. The token authorization processor **526** then reduces the balance value by an amount equal to the authorization value.

[0176] The token authorization processor **526** then generates a token validation response message that confirms that the limited-use token was valid (i.e. the balance value of the subledger was at least equal to the authorization value). The token management server **600** transmits the token validation response message to the TSP server **600**, via the wide area network **140** (in response to the token validation request message), at step S**744**.

[0177] After the TSP server **600** receives the token validation response message, the subledger recovery processor **624** of the TSP server **600** completes transforming the token authorization request message (into a pooled account authorization request message) by locating in the token database **614** the pooling identifier that is associated with the limited-use token in the token database **614** (step S**746**), and generating a pooling account authorization request message that includes the pooling ledger identifier and the authorization value and requests authorization for a funds transfer (monetary amount, loyalty points) in a transfer amount equal to the authorization amount. At step S**748**, the TSP server **600** initiates a transfer of the transfer amount from the pooling ledger by transmitting the pooling account authorization request message to the authorization server **700**, via the wide area network **140**, in response to the token authorization request message.

[0178] In response to the pooling account authorization request message, the authorization server **700** uses the pooling account identifier to identify the pooling ledger that is associated with the pooling account identifier, and then determines whether pooling ledger has sufficient funds (monetary amount, loyalty points) to complete the funds transfer (i.e. the balance of funds in the pooling ledger is at least equal to the transfer amount), at step S**750**. If the authorization server **700** determines that the pooling ledger has sufficient funds to complete the funds transfer, the authorization server **700** reduces the available balance value associated with the pooling ledger by an amount equal to the transfer amount.

[0179] The authorization server **700** may also generate an authorization code from at least a private cryptographic key of the authorization server **700**, the pooling ledger identifier and the transfer amount. The authorization server **700** then generates a pooling ledger authorization response message that may include the authorization code and indicates that the funds transfer (from the subledger) was authorized, and transmits the pooling ledger authorization response message to the POS station **400**, via the payment network **160**, at step S**752**, in response to the token authorization request message.

[0180] However, if the subledger recovery processor **624** is unable to locate the limited-use token in the token database **614** (step S**738**), or the authorization processor **526** is unable to confirm that the balance value of the subledger is at least equal to the authorization value (at step S**742**), the subledger recovery processor **624** of the TSP server **600** generates a token authorization response message that indicates that the limited-use token was invalid or the subledger balance was insufficient to complete the transaction. The TSP server **600** then transmits the token authorization response message to the authorization server **700**, via the wide area network **140**, in response to the token authorization request message.

[0181] In response, the authorization server **700** generates a pooling ledger authorization response message that indicates that the funds transfer was not authorized, and transmits the pooling ledger authorization response message to the POS station **400**, via the payment network **160**, at step S**752**.

[0182] Independently of whether the pooling ledger authorization response message indicates that the funds transfer was authorized, the POS station **400** may display the pooling ledger authorization response message on the display device **404** (where the POS station **400** is implemented as a POS terminal or a pin-pad device).

[0183] After the POS station **400** receives one or more pooling ledger authorization response messages, the POS station **400** may initiation completion of the authorized funds transfers (from the pooling ledger) by generating a clearing payload that includes one or more of the authorization codes, the associated transfer amounts and the merchant ledger identifier of a merchant ledger maintained by the financial institution on behalf of the merchant. The POS station **400** may transmit the clearing payload to the authorization server **700** via the payment network **160**, and the authorization server **700** may use its cryptographic key to confirm that the authorization server **700** generated the authorization codes, and may transfer the transfer amounts from the pooling ledger into the merchant ledger that is associated with the merchant ledger identifier.

1. A computer server comprising:

a memory storing a token database and a plurality of computer processing instructions; and

a data processor in communication with the memory, wherein the computer processing instructions cause the data processor to:

receive from a point-of-sale station via a payment network a token authorization request including a limited-use token and an authorization value;

locate in the token database a token record storing a subledger identifier in association with the limited-use token, extract the subledger identifier from the located token record, locate in a subledger database a subledger associated with the subledger identifier, and confirm that a balance value associated with the located subledger is at least equal to the authorization value; and

initiate a transfer from a pooling ledger distinct from the subledger of a transfer amount equal to the authorization value.

2. The computer server according to claim 1, wherein:
the limited-use token is stored in the located token record in association with the subledger identifier and a ledger identifier; and
the pooling ledger is associated with the ledger identifier.

3. The computer server according to claim 2, wherein the computer processing instructions cause the data processor to initiate the transfer from the pooling ledger by:
reducing the balance value of the located subledger by the authorization value;
extracting the ledger identifier from the located token record; and
obtaining authorization for a funds transfer of the transfer amount from the pooling ledger associated with the extracted ledger identifier.

4. The computer server according to claim 1, wherein the computer processing instructions cause the data processor to, prior to receiving the token authorization request:
receive from one communications device, via one communications channel, a token request including a reference identifier and a credential;
locate in a funding database a database record associated with the reference identifier, extracting a validation code from the located database record, and confirm that the credential matches the validation code;
generate the subledger identifier, initializing the balance value of the located subledger equal to the authorization limit, and save the subledger identifier in the token record in association with the limited-use token; and
provide the one communications device with the limited-use token via another communications channel different from the one communications channel.

5. The computer server according to claim 4, wherein the computer processing instructions cause the data processor to, prior to receiving the token request:
receive from another communications device a funding request including the validation code and an authorization limit;
initiate a transfer into the pooling ledger of a funding amount equal to the authorization limit;
save the reference identifier in the located database record of the funding database in association with the validation code; and
provide the one communications device with the reference identifier.

6. The computer server according to claim 5, wherein the computer processing instructions further cause the data processor to:
receive a user identifier from the one communications device; and
initiate the transfer of the funding amount by obtaining authorization for a funds transfer of the funding amount from a source ledger associated with the user identifier.

7. The computer server according to claim 4, wherein the token request includes a device identifier, and the computer processing instructions cause the data processor to provide the one communications device with the limited-use token by:
locating in an address database a destination address associated with the device identifier; and
transmitting the limited-use token to the destination address.

8. A token processing network comprising:
a token service provider server;
a token database; and
a subledger database,
wherein the token service provider server is configured to:
receive from a point-of-sale station via a payment network a token authorization request including the limited-use token and an authorization value;
locate in the token database a token record storing a subledger identifier in association with the limited-use token, extract the subledger identifier from the located token record, locate in the subledger database a subledger associated with the subledger identifier, and confirm that a balance value associated with the located subledger is at least equal to the authorization value; and
initiate a transfer from a pooling ledger distinct from the subledger of a transfer amount equal to the authorization value.

9. The token processing network according to claim 8, wherein:
the limited-use token is stored in the located token record in association with the subledger identifier and a ledger identifier; and
the pooling ledger is associated with the ledger identifier.

10. The token processing network according to claim 9, further comprising a token management server, wherein:
the token management server is configured to reduce the balance value of the located subledger by the authorization value after the token service provider server extracts the subledger identifier; and
the token service provider server is configured to, after the token service provider server confirms the balance value, extract the ledger identifier from the located token record, and to initiate the transfer from the pooling ledger by obtaining authorization for a funds transfer of the transfer amount from the pooling ledger associated with the extracted ledger identifier.

11. The token processing network according to claim 8, further comprising a funding database and a token management server,
wherein the token management server is configured to, prior to the token service provider server receiving the token authorization request:
receive from one communications device, via one communications channel, a token request including a reference identifier and a credential;
locate in the funding database a database record associated with the reference identifier, extract a validation code from the located database record, and confirm that the credential matches the validation code; and
generate the subledger identifier, and initialize the balance value of the located subledger equal to the authorization limit, and
wherein the token service provider server is further configured to:
save the subledger identifier in the token record in association with the limited-use token; and
provide the one communications device with the limited-use token via another communications channel different from the one communications channel.

12. The token processing network according to claim 11, wherein the token management server is further configured to, prior to receiving the token request:

receive from another communications device a funding request including the validation code and an authorization limit;

initiate a transfer into the pooling ledger of a funding amount equal to the authorization limit;

save the reference identifier in the located database record of the funding database in association with the validation code; and

provide the one communications device with the reference identifier.

13. The token processing network according to claim **12**, wherein the token management server is further configured to:

receive a user identifier from the one communications device; and

initiate the transfer of the funding amount by obtaining authorization for a funds transfer of the funding amount from a source ledger associated with the user identifier.

14. A method of processing limited-use tokens, the method comprising a computer server:

receiving from a point-of-sale station via a payment network a token authorization request including a limited-use token and an authorization value;

locating in a token database a token record storing a subledger identifier in association with the limited-use token, extracting the subledger identifier from the located token record, locating in a subledger database a subledger associated with the subledger identifier, and confirming that a balance value associated with the located subledger is at least equal to the authorization value; and

initiating a transfer from a pooling ledger distinct from the subledger of a transfer amount equal to the authorization value.

15. The method according to claim **14**, wherein:

the limited-use token is stored in the located token record in association with the subledger identifier and a ledger identifier, and

the pooling ledger is associated with the ledger identifier.

16. The method according to claim **15**, wherein the initiating a transfer from a pooling ledger comprises the computer server:

reducing the balance value of the located subledger by the authorization value;

extracting the ledger identifier from the located token record; and

obtaining authorization for a funds transfer of the transfer amount from the pooling ledger associated with the extracted ledger identifier.

17. The method according to claim **14**, further comprising, prior to the receiving a token authorization request, the computer server:

receiving from one communications device, via one communications channel, a token request including a reference identifier and a credential;

locating in a funding database a database record associated with the reference identifier, extracting a validation code from the located database record, and confirming that the credential matches the validation code;

generating the subledger identifier, initializing the balance value of the located subledger equal to the authorization limit, and saving the subledger identifier in the token record in association with the limited-use token; and

providing the one communications device with the limited-use token via another communications channel different from the one communications channel.

18. The method according to claim **17**, further comprising, prior to the receiving a token request, the computer server:

receiving from another communications device a funding request including the validation code and an authorization limit;

initiating a transfer into the pooling ledger of a funding amount equal to the authorization limit;

saving the reference identifier in the located database record of the funding database in association with the validation code; and

providing the one communications device with the reference identifier.

19. The method according to claim **18**, further comprising the computer server receiving a user identifier from the one communications device, wherein the initiating a transfer of a funding amount comprises the computer server obtaining authorization for a funds transfer of the funding amount from a source ledger associated with the user identifier.

20. The method according to claim **17**, wherein the token request includes a device identifier, and the providing the one communications device with the limited-use token comprises the computer server:

locating in an address database a destination address associated with the device identifier; and

transmitting the limited-use token to the destination address.

* * * * *