(12) STANDARD PATENT (11) Application No. **AU 2016409079 B2**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
Subtoken management system for connected devices

(51) International Patent Classification(s)
H04L 29/06 (2006.01)

(21) Application No: **2016409079** (22) Date of Filing: **2016.06.03**

(87) WIPO No: **WO17/209767**

(43) Publication Date: **2017.12.07**
(44) Accepted Journal Date: **2021.07.22**

(71) Applicant(s)
Visa International Service Association

(72) Inventor(s)
Howard, Kelvan

(74) Agent / Attorney
FPA Patent Attorneys Pty Ltd, ANZ Tower 161 Castlereagh Street, Sydney, NSW, 2000, AU

(56) Related Art
US 2005/0154925 A1
US 2015/0254665 A1

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
07 December 2017 (07.12.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/209767 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/US2016/035820

(22) International Filing Date:
03 June 2016 (03.06.2016)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; P.O. Box 8999, San Francisco, California 94128-8999 (US).

(72) Inventor: **HOWARD, Kelvan**; 235 Shrader #3, San Francisco, California 94117 (US).

(74) Agent: **BOUQUET, Bert E.** et al.; Kilpatrick, Townsend & Stockton LLP, Two Embarcadero Center, 19th Floor, San Francisco, California 94111 (US).

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

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

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

(54) Title: SUBTOKEN MANAGEMENT SYSTEM FOR CONNECTED DEVICES

(57) Abstract: Described herein is a system for generating subtokens and/or sets of protocols to be provided to connected devices for use in subsequent transactions. In some embodiments, a mobile device identifies one or more connected devices via a discovery process. The mobile device may receive transaction information related to transactions to be conducted by the connected devices. The mobile device may, in some cases by communicating with a processing server, identify a parent token and/or a set of protocols related to the transaction information / connected device. The mobile device may subsequently generate a subtoken derived from the parent token based on the set of protocols. The subtoken and/or the set of protocols may be provided to a connected device, which may subsequently conduct a transaction using the subtoken and/or the set of protocols.

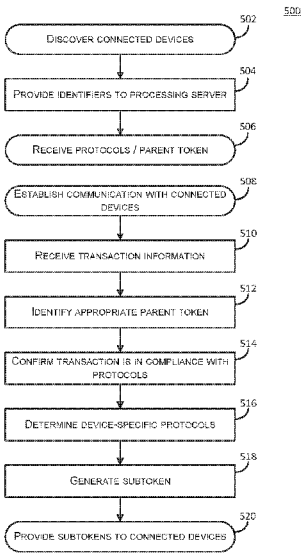

FIG. 5

WO 2017/209767 A1

SUBTOKEN MANAGEMENT SYSTEM FOR CONNECTED DEVICES

BACKGROUND

[0001] Households typically include a number of connected devices and these connected devices have needs to access resources such as goods, services, and data. For example, consumers have refrigerators for storing food, gas meters for measuring gas usage, electric meters for measuring power usage, and water meters for measuring water usage. Recently, “smart” versions of some of these connected devices have been introduced to the public. It has been contemplated that such smart connected devices could be capable of automatically requesting resources such as software updates, goods or services. However, each time a connected device initiates a transaction (usually over a wireless area network) there is a chance that details of the transaction (including payment account information) and/or sensitive credential information associated with the connected device may be intercepted and the owner of the device may be defrauded. Given the proliferation of network enabled connected devices, it is difficult to provide data security to each and every interaction between each and every connected device within system.

[0002] Embodiments of the invention address these and other problems, individually and/or collectively.

BRIEF SUMMARY

[0002a] By way of clarification and for avoidance of doubt, as used herein and except where the context requires otherwise, the term "comprise" and variations of the term, such as "comprising", "comprises" and "comprised", are not intended to exclude further additions, components, integers or steps.

[0003] Embodiments of the invention can be applied to the "Internet of things" where machines can interact with other machines without human intervention. In particular, embodiments of the invention are directed to a system in which a mobile device generates subtokens and/or a set of protocols to be provided to (or provisioned onto) one or more connected devices to be used in at least one subsequent transaction conducted by the connected devices. In some embodiments, a subtoken may be generated from a parent token stored on a mobile device, such that it is associated with an underlying account of the parent token, but is of limited

2016409079 04 Jun 2021

duration. In some embodiments, the set of protocols may dictate the conditions under which the subtoken may be used.

[0004] One embodiment of the invention is directed to a method of operating a mobile device to provide limited-use subtokens to a plurality of connected devices connected to a private network, the method comprising connecting, by a mobile device, to a private network and identifying a plurality of connected devices connected to the private network. The method further comprises receiving, from the plurality of connected devices, information related to a plurality of transactions, each transaction being requested by a respective one of the plurality of connected devices and, in response to receiving the information, for each transaction identifying a protocol set associated with the respective connected device; determining, based on the information related to the transaction, whether the transaction is compliant with one or more protocols in the protocol set; in response to determining that the transaction is compliant with the one or more protocols, generating, by the mobile device, from a parent token associated with the mobile device, a limited-use subtoken specific to a transaction type of the transaction, wherein the parent token and the limited-use subtoken reference the same account information. The method further comprising providing, by the mobile device, the limited-use subtoken and at least a portion of the identified protocol set to the connected device from which the information related to the transaction was received, the subtoken being stored in a secure memory of the connected device; wherein each of the limited-use subtokens is useable to initiate the respective transaction to be conducted by the respective connected device in accordance with the portion of the identified protocol set;.

[0005] Another embodiment of the invention is directed to a mobile device comprising one or more processors, and a memory including instructions that, when executed by the one or more processors, cause the mobile device to connect to a private network, and identify a plurality of connected devices in communication with the private network. The instructions further cause the mobile device to receive, from the plurality of

connected devices, information related to transactions to be conducted by the plurality of connected devices, each transaction being requested by a respective one of the plurality of connected devices. For each transaction, the instructions further cause the mobile device to: identify a protocol set associated with the respective connected device; determine, based on the information related to the transaction, whether the transaction is compliant with one or more protocols in the protocol set; in response to a determination that the transaction is compliant with the one or more protocols, generate, from a parent token associated with the mobile device, a limited-use subtoken specific to a transaction type of the transaction, wherein the parent token and the limited-use subtoken reference the same account information. The instructions further cause the mobile device to provide, the limited-use subtoken and at least a portion of the identified protocol set to the connected device from which the information related to the transaction was received, the subtoken being stored in a secure memory of the connected device; wherein each limited-use subtoken is useable to initiate the respective transaction to be conducted by the respective connected devices in accordance with the respective portions of the identified protocol set.

[0006] Another embodiment of the invention is directed to a connected device comprising one or more processors, and a memory including instructions that, when executed by the one or more processors, cause the connected device to connect to a private network and establish, via the private network, a communication session with a mobile device. The instructions further cause the connected device to provide, to the mobile device via the communication session, an indication of at least one transaction to be conducted in relation to a resource managed by the connected device. The instructions further cause the connected device to receive, from the mobile device via the communication session, a limited-use subtoken useable to conduct the at least one transaction and a subset of protocols, wherein the limited-use subtoken is derived from a parent token associated with the mobile device and is specific to a transaction type of the at least one transaction. The instructions further cause the connected device to store the limited-use subtoken in the secure memory, determine, based on the subset of protocols, whether to conduct the at least one transaction, and upon determining to conduct the at least one transaction, initiate, using the received limited-use subtoken, the at least one transaction.

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

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] FIG. 1 depicts an example system architecture capable of implementing at least some embodiments of the current disclosure;

[0009] FIG. 2 depicts an example mobile device configured to store and manage access credentials and provide transaction related information to connected devices in accordance with at least some embodiments;

[0010] FIG. 3 depicts an example data flow that may be implemented in accordance with at least some embodiments;

[0011] FIG. 4 depicts an illustrative example of a mobile device capable of generating subtokens and protocols to be provided to multiple connected devices in accordance with at least some embodiments;

[0012] FIG. 5 depicts a flow diagram illustrating a process for discovering one or more connected devices and subsequently providing subtokens in accordance with at least some embodiments;

[0013] FIG. 6 depicts an exemplary embodiment in which a subtoken is generated for a computer device and used to obtain software and/or software updates.

DETAILED DESCRIPTION

[0014] In the following description, various embodiments will be described. For purposes of explanation, specific configurations and details are set forth in order to provide a thorough understanding of the embodiments. However, it will also be apparent to one skilled in the art that the embodiments may be practiced without the specific details. Furthermore, well-known features may be omitted or simplified in order not to obscure the embodiment being described.

[0015] Prior to discussing the details of some embodiments of the present invention, description of some terms may be helpful in understanding the various embodiments.

[0016] An "access credential" may be any data or portion of data used to gain access to a particular resource. In some embodiments, an access credential may be a login and/or password for a user account. In some embodiments, an access credential may be include account information or a token associated with the account information, a cryptogram, a digital certificate, etc. A mobile device may store one or more access credentials associated with each connected device. In some embodiments, an access credential stored in association with a connected device may be used to conduct transactions on behalf of the connected device. In some embodiments, the mobile device may store a single access credential that may be used in each transaction initiated by the mobile device.

[0017] "Account data" may refer to any content of an account of a user conducting a transaction. In some embodiments, account data may be payment account data that may be utilized to make a purchase. In other embodiments, account data may be any content associated with a user's non-financial account. For example, account data may include electronic files, photos, videos, and documents stored by the user's account. In some embodiments, account data may be stored by an authorization computer.

[0018] "Account information" may refer to any information surrounding an account of a user. For example, account information may include account data and one or more account identifiers. In some embodiments, the account identifier may be a PAN or primary account number. The PAN may be 14, 16, or 18 digits. Account information may also include an expiration date associated with the account, as well as a service code and/or verification values (e.g., CVV, CVV2, dCVV, and dCVV2 values).

[0019] An "authorization request message" may be an electronic message that requests authorization for a transaction. In some embodiments, it is sent to a transaction processing computer and/or an issuer of a payment card to request authorization for a transaction. An authorization request message according to some embodiments may comply with ISO 8583, which is a standard for systems that exchange electronic transaction information associated with a payment made by a user using a payment device or payment account. The authorization request message may include an issuer account identifier that may be associated with a

payment device or payment account. An authorization request message may also comprise additional data elements corresponding to "identification information" including, by way of example only: a service code, a CVV (card verification value), a dCVV (dynamic card verification value), a PAN (primary account number or "account number"), a payment token, a user name, an expiration date, etc. An authorization request message may also comprise "transaction information," such as any information associated with a current transaction, such as the transaction amount, merchant identifier, merchant location, acquirer bank identification number (BIN), card acceptor ID, information identifying items being purchased, etc., as well as any other information that may be utilized in determining whether to identify and/or authorize a transaction.

[0020] An "authorization response message" may be a message that responds to an authorization request. In some cases, it may be an electronic message reply to an authorization request message generated by an issuing financial institution or a transaction processing computer. The authorization response message may include, by way of example only, one or more of the following status indicators: Approval -- transaction was approved; Decline -- transaction was not approved; or Call Center -- response pending more information, merchant must call the toll-free authorization phone number. The authorization response message may also include an authorization code, which may be a code that a credit card issuing bank returns in response to an authorization request message in an electronic message (either directly or through the transaction processing computer) to the merchant's access device (e.g. POS equipment) that indicates approval of the transaction. The code may serve as proof of authorization. As noted above, in some embodiments, a transaction processing computer may generate or forward the authorization response message to the merchant.

[0021] A "communication device" may be any electronic device that has a primary function related to communication. A communication device may be capable of establishing a communication session with another electronic device and transmitting / receiving data from that device. In some embodiments, a communication device may act as a proxy device between two or more other electronic devices by establishing communication sessions with each of the devices

and relaying information between the devices. A mobile device may be a type of communication device.

[0022] A "connected device" may be any suitable electronic device capable of communicating with, and/or interacting with other devices. A connected device may have a primary function that is unrelated to communicating with other electronic devices. For example, a connected device may be a refrigerator that, in addition to preserving food, is capable of interacting with one or more other electronic devices. In some embodiments, a connected device may be associated with a device identifier. The device identifier may be used by a service provider to determine the type of device for a particular connected device. Examples of connected devices may include gas and electric meters, refrigerators, lamps, thermostats, printers, automobiles, fire alarms, home medical devices, home alarms, motorcycles, boats, televisions, etc. A connected device need not be "connected" at all times, as the term connected is intended to refer to devices with the ability to establish a connection with another device.

[0023] A "device identifier" may include any suitable distinctive set of characters used to identify a device. An exemplary device identifier may include any suitable number or type of characters (e.g., numbers, graphics, symbols, or other information) that may uniquely represent a device. By way of example, a device identifier may be a serial number, partial serial number, or device name or nickname. In some embodiments, a device identifier may be generated, based on a trusted hardware root. Additionally, the device identifier may be a temporary identifier for a particular device, such as a network address at which the device may be found.

[0024] An "electronic device," may be any device that accomplishes its purpose electronically. An electronic device may have multiple functions. For example an electronic device may have a primary function and one or more secondary functions. A primary function may be the function that most closely aligns with the electronic device's purpose. An example of an electronic device may be a connected device.

[0025] An "issuer" may typically refer to a business entity (e.g., a bank) that maintains an account for a user that is associated with a portable communication

device such as an account enrolled in a mobile application installed on a portable communication device. An issuer may also issue account parameters associated with the account to a portable communication device. An issuer may be associated with a host system that performs some or all of the functions of the issuer on behalf of the issuer.

[0026] A "merchant" may typically be an entity that engages in transactions and can sell goods or services, or provide access to goods or services.

[0027] A "private network" may be any communication network not readily accessible by the public. In some embodiments, a private network may be secured by a password or encryption protocol. In some embodiments, a private network may be accessed by multiple electronic devices by connecting to a wireless router. By way of example, a private network may be a home network useable by the residents of the home or a business network useable by the employees of the business.

[0028] A "protocol set" may be a set of rules or configuration settings that indicates one or more actions are allowed and/or should be performed. In some cases, a protocol set may include conditions upon which those actions are to be performed. In some embodiments, a protocol set may include conditional statements, such as "if *x_condition* occurs, then perform *y_action*." In some embodiments, a protocol set may include a list of transactions that are allowed for a particular connected device and/or access credential. For example, a mobile device may identify, based on a device identifier, a type of device that the protocol set is related to. The mobile device may then create a custom protocol set for that connected device based on the device's type. For example, upon determining that a connected device is a water meter, the mobile device may create a protocol set for the water meter that only allows it to conduct transactions related to water usage. In this example, the protocol set may be stored at the mobile device in relation to the water meter (or an access credential associated with the water meter) and at least a portion of the protocol set may be provisioned onto the water meter. In some embodiments, protocols may be stored on a processing server. Upon discovery of a connected device by the mobile device, the processing server may identify the protocol set relevant to the connected device and transmit that protocol set to the mobile device.

[0029] A "processing server" may be any computing device configured to provide remote support for a mobile device. The processing server may provide any suitable service and/or processing for the mobile device. In some embodiments, the processing server may maintain an account for one or more users. The processing server may also store one or more protocols and/or user preferences related to the operation of the mobile device or service.

[0030] A "mobile device" may be any computing device capable of traveling with a user. In some embodiments, a mobile device can include any suitable computing device configured to establish communication sessions with one or more connected devices and a transaction server (either directly or via a processing server) and (in some cases) to initiate transactions with the transaction server on behalf of the connected devices. In some embodiments, the mobile device may store one or more access credentials to be used in these transactions. In some embodiments, the mobile device may be configured to store one or more protocol sets related to transactions and/or connected devices. The mobile device may be further configured to confirm that transactions are in compliance with these transaction protocols prior to initiating the transactions.

[0031] The term "provisioning" may include any preparation and/or configuring of a device to enable it to perform a function. For example, provisioning may include storing rules, protocols, and/or instructions on a device to direct the device's actions. In some embodiments, a device may be provisioned with access credentials associated with a user of the device. The access credentials may enable the device to execute transactions on the user's behalf without active input from the user.

[0032] A "server computer" may include a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The server computer may be coupled to a database and may include any hardware, software, other logic, or combination of the preceding for servicing the requests from one or more client computers. The server computer may comprise one or more computational apparatuses and may use any of a variety of computing structures,

arrangements, and compilations for servicing the requests from one or more client computers.

[0033] A “token” may be a substitute for a real credential. In some embodiments, a token may include an identifier for a payment account that is a substitute for a real credential such as primary account number (PAN). For example, a token may include a series of numeric and/or alphanumeric characters that may be used as a substitute for an original account identifier. For example, a token “4900 0000 0000 0001” may be used in place of a PAN “4147 0900 0000 1234.” In some embodiments, a token may be “format preserving” and may have a numeric format that conforms to the account identifiers used in existing payment processing networks (e.g., ISO 8583 financial transaction message format). In some embodiments, a token may be used in place of a PAN to initiate, authorize, settle or resolve a payment transaction or represent the original credential in other systems where the original credential would typically be provided. In some embodiments, a token value may be generated such that the recovery of the original PAN or other account identifier from the token value may not be computationally derived. In other embodiments, a token may be mathematically derived (e.g., with an encryption key) from the real credential. Further, in some embodiments, the token format may be configured to allow the entity receiving the token to identify it as a token and recognize the entity that issued the token. A token may be associated with a protocol set. Tokens may include parent tokens and subtokens. Although the use of payment tokens and payment subtokens are described in detail, embodiments of the invention are not limited thereto. For example, instead of subtokens that are used for payment, embodiments of the invention may include subtokens that can be used to access data.

[0034] A "parent token" can be a token which is directly derived or obtained from real credential (e.g., a PAN). For example, a parent token “4900 0000 0000 0001” may be used in place of a real PAN “4147 0900 0000 1234.”

[0035] A "subtoken" may a token that is derived or obtained from a parent token. If the subtoken is used for payment, the subtoken may be subordinate to the parent token in that funds for the subtoken may be obtained from an account associated with the parent token and/or the real credential associated with the parent

token. The subtoken may be computationally derivable from the parent token or may not be computationally derivable from the parent token. Further, the subtoken may have the same or different form or format as the parent token. For example, the subtoken and the parent token may each be format preserving and may be 16, 18, or 19 digits in length. Further, many subtokens may be associated with a single parent token in some embodiments of the invention. For example, separate subtokens may be generated from a single parent token for a plurality of connected devices, wherein each.connected device is provided with a subtoken that may only be used by that connected device.

[0036] A "transaction server" may include any computing device capable of receiving a request for a transaction and processing information related to the requested transaction. In some embodiments, the transaction server may be affiliated with an electronic marketplace or a retail entity that maintains an internet presence. A transaction server may support transactions to acquire resources (e.g., goods and/or services). In some embodiments, a user may request a transaction by visiting a website affiliated with the transaction server and selecting one or more items to purchase. The transaction server may be in communication with other devices via a network connection.

[0037] The term "verification" and its derivatives may refer to a process that utilizes information to determine whether an underlying subject is valid under a given set of circumstances. Verification may include any comparison of information to ensure some data or information is correct, valid, accurate, legitimate, and/or in good standing.

[0038] Details of some embodiments of the present invention will now be described.

[0039] FIG. 1 depicts an example system architecture capable of implementing at least some embodiments of the current disclosure. In FIG. 1, one or more connected devices 102 may be in communication with a mobile device 104. The connected devices 102 may be located within a vicinity of the mobile device 104. For example, the connected devices 102 may be within range of a short range communication means used by the mobile device 104. In some embodiments, the

range may be less than about 100, 50, 20, 10, or 5 yards. In some embodiments, the connected devices 102 may be connected to a communication network 106. For example, the connected devices 102 may each be in communication with a private communication network.

[0040] In some embodiments, the mobile device 104 may be in communication with a processing server 108 via a communication network 106. The processing server 108 and/or the mobile device 104 may also be in communication with a transaction server 110 configured to receive and process transaction requests. Upon receiving a transaction request, the transaction server 110 may generate and submit an authorization request to a transaction processing network 112 to be authorized by an authorization computer 114.

[0041] The connected device 102 may be any electronic device configured to perform at least one primary function. The connected device 102 may include one or more processors 118 capable of processing user input. The connected device 102 may also include one or more input sensors 120 for collecting input. In some embodiments, the input may include user provided input. Some non-limiting examples of input sensors 120 that may be included in a connected device include keyboards, mice, microphones, cameras, motion sensors, accelerometers, cameras, pressure sensors, thermometers, a global positioning system (GPS), etc. In some embodiments, the input may include input related to resource usage. For example, the connected device may be a water meter configured to capture input related to water usage at a particular location. In another example, the connected device may be an electricity meter configured to capture input related to electricity usage at a particular location.

[0042] In some embodiments, the connected device 102 may include a communication interface 122 configured to enable communication between the connected device 102 and another electronic device (e.g., mobile device 104, or a wireless router that manages access to communication network 106). Examples of communication interface 122 may include one or more radio frequency (RF) transceivers configured to send and receive communications using near-field communications (NFC), or other radio frequency or wireless communication protocols such as Bluetooth, Bluetooth low-energy (BLE), a wireless local area

network (e.g., WiFi), iBeacon, etc. In some embodiments, communication interface 122 may include an infrared communication device. In some embodiments, the communication interface 122 may include both long range and short range communication means. For example, the communication interface may include an antenna configured to connect to a cellular network in order to enable communication with various other components of the depicted architecture.

[0043] In some embodiments, the communication technology used by the connected device 102 and/or the mobile device 104 may depend on the type of power source used by the connected device. For example, if the device has access to a regular, external power supply (e.g., as is common for smart refrigerators and other devices such as washer/driers, garage doors, cars, etc.) it may include a WiFi interface. Alternatively, if the device relies on a battery instead of an external power supply, it may include a means for communication that consumes less power, such as low power Bluetooth interface, a ZigBee interface, a near field communication (NFC) or radio frequency (RF) interface, or any other suitable wireless access interface.

[0044] Embodiments of one or more modules on the connected device 102 may be stored and executed from its memory 124. Turning to the contents of the memory 124 in more detail, the memory 126 may include an operating system and one or more modules configured to cause the processors 118 to carry out instructions in accordance with at least some embodiments of the disclosure. For example, the memory 124 may include a transaction module 126 configured to work with the processor 118 to initiate one or more transactions related to the primary function of the connected device 102. Additionally, the memory 124 may include information related to one or more access credentials (subtoken 128).

[0045] In some embodiments, the transaction module 126 may be programmed to cause the connected device 102 to initiate a transaction on behalf of an owner and/or operator of the connected device 102. For example, the transaction module 126 may be configured to cause the connected device 102 to initiate a purchase of a resource on behalf of the user. The resource may be any good or service related to a primary function of the electronic device. For example, a water purifier may initiate a purchase order for new water filters upon determining that the

current water filters need replacement. The transaction module 126 may be programmed to cause the connected device 102 to provide one or more transaction details to the mobile device 104. For example, upon detecting that a mobile device 104 is present (e.g., the mobile device 104 may connect to a private network), the transaction module 126 may provide transaction details to the mobile device in order to receive a subtoken to be used to conduct the transaction. In some embodiments, the transaction module may be programmed to cause the connected device 102 to initiate a transaction upon determining that one or more threshold conditions have been met. Threshold conditions may be preset (e.g., programmed by the manufacturer or distributor of the connected device) or provided by a user of the connected device 102. In some embodiments, the threshold conditions may be provisioned onto the connected device 102 by the mobile device 104.

[0046] The memory 124 of connected device 102 may include a secure execution environment such as a secure memory (e.g., Smartcard based technology available in low-power devices). In some embodiments, the secure memory may include a secure element. A secure element (SE) can be a tamper-resistant platform (typically a one chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (e.g. key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities. Sensitive information (e.g., a subtoken 128 or other suitable access credential data) provisioned onto the connected device 102 may be stored in the secure memory.

[0047] In at least some embodiments of the invention, a mobile device 104 may be configured to detect local connected devices 102. For example, the mobile device 104 may be configured to perform a device discovery action that identifies all communicatively enabled electronic devices within range of the mobile device 104. By way of illustration, a mobile device 104 may detect all electronic devices that are connected to WiFi within range of the mobile device 104. In another example, the mobile device 104 may connect to a private network (e.g., a home-based or business-based network) and may identify each of the connected devices 102 that are also connected to the private network. Once detected, the mobile device 104 may receive a selection of at least one of the connected devices from a user. In

some embodiments of the disclosure, the mobile device 104 may establish a connection with the selected connected device and receive information related to the connected device (e.g., a device identifier). In some embodiments, an additional step of authenticating that a user owns the connected device may be required by the mobile device in order to establish a connection. For example, the user may be required to enter a password for the connected device or press a button located on the connected device. Information related to the connected device may be presented to a user within a graphical user interface (GUI) executed from the mobile device 104. In some embodiments, the mobile device 104 may authenticate the connected device 102 by use of a shared secret or digital signature. For example, upon encountering a new connected device 102, the mobile device 104 may, upon determining that the connected device 102 is authorized to receive a subtoken (e.g., by confirming shared ownership by the user as described above), provide an encryption key and/or passcode to the connected device 102. Upon establishing a communication session with the mobile device 104 in the future, the connected device 102 may authenticate itself by providing the passcode to the mobile device 104.

[0048] The mobile device 104 may also establish a connection with a processing server 108 that provides back end support for the mobile device 104 by maintaining and managing transaction-related activities. In some embodiments, upon selection of the connected device by the user, the mobile device 104 may transmit information related to the connected device 102 to the processing server 108. The processing server 108 may retrieve transaction processing information to be associated with the connected device and may send that transaction processing information to the mobile device 104. In this way, the transaction processing information may be provisioned onto the mobile device 104 for a particular connected device 102. The transaction processing information may include an access credential, consumer identifier, protocol information and/or any other suitable information relevant to the connected device.

[0049] The processing server 108 may be any type of computing device, including a remotely located server computer, configured to perform one or more actions on behalf of the mobile device 104. Additionally, it should be noted that in

some embodiments, the processing server 108 may be embodied by one more virtual machines implemented in a hosted computing environment. The hosted computing environment may include one or more rapidly provisioned and released computing resources, which computing resources may include computing, networking, and/or storage devices. A hosted computing environment may also be referred to as a cloud-computing environment. In some embodiments, the processing server 108 may be configured to provide information related to one or more connected devices 102 to the mobile device 104. In some embodiments, a processing server may be a mobile application server that supports a mobile application installed on, and executed from, the mobile device 104. In some embodiments, the processing server may be a server that supports mobile payment applications. For example, an e-wallet application may be installed on the mobile device 104. In this example, payment information may be maintained by the processing server.

[0050] In some examples, the communication network 106 and/or the transaction processing network 112 may include any one or a combination of many different types of networks, such as cable networks, the Internet, wireless networks, cellular networks, and other private and/or public networks. In addition, the communication network 106 and/or transaction processing network 112 may comprise multiple different networks. For example, the mobile device 104 may utilize a 3G network to communicate with a wireless router, which may then route the communication over a public network (e.g., the Internet) to the processing server 108. In some embodiments, the transaction processing network 112 may be an electronic payment network (e.g., VisaNet).

[0051] Transaction server 110 may be any computing device or plurality of computing devices configured to receive a transaction request and initiate a transaction. In some embodiments, the transaction server 110 may be associated with an electronic commerce site. For example, the transaction server may maintain a catalog of items and/or services available for purchase. The transaction server may also be associated with a utility company or other resource provider. In some embodiments, the transaction server may enable a user to pay a bill or other outstanding debt related to resource acquisition. The transaction server 110 may

also be configured to complete a transaction upon receiving an authorization response message indicating that a transaction has been approved.

[0052] In some embodiments, the transaction server 110 may be in communication with an acquirer computer. An acquirer computer may be any computing device or plurality of computing devices configured to process transaction information received from the transaction server 110 and generate an authorization request message to be transmitted to the authorization computer 114. In some embodiments, the acquirer computer may be owned and/or operated by a banking institute with which the operator of the transaction server 110 maintains an account.

[0053] Authorization computer 114 may be any computing device or plurality of computing devices configured to receive an authorization request message for a transaction, authorize or decline the transaction, and provide an authorization response message based on whether the transaction has been authorized or declined. The authorization computer 114 may determine whether to authorize or decline the transaction based on information associated with the transaction. In some embodiments, the authorization computer 114 may be an issuer of a payment account (e.g., a credit card).

[0054] For simplicity of illustration, a certain number of components are shown in FIG. 1. It is understood, however, that embodiments of the invention may include more than one of each component. In addition, some embodiments of the invention may include fewer than or greater than all of the components shown in FIG. 1. In addition, the components in FIG. 1 may communicate via any suitable communication medium (including the internet), using any suitable communications protocol.

[0055] **FIG. 2** depicts an example mobile device configured to store and manage access credentials and provide transaction related information to connected devices in accordance with at least some embodiments. The depicted mobile device may be an example mobile device 104 of FIG. 1.

[0056] The mobile device 104 may be any type of computing device capable of interacting with one or more connected devices. In some embodiments, the mobile device 104 may be a mobile phone or any other suitable portable electronic device.

In at least some embodiments, the mobile device 104 may include at least one memory 202 and one or more processing units (or processor(s)) 204. The processor(s) 204 may be implemented as appropriate in hardware, computer-executable instructions, firmware or combinations thereof. Computer-executable instruction or firmware embodiments of the processor(s) 204 may include computer-executable or machine executable instructions written in any suitable programming language to perform the various functions described.

[0057] The memory 202 may store program instructions that are loadable and executable on the processor(s) 204, as well as data generated during the execution of these program instructions. Depending on the configuration and type of mobile device 104, the memory 202 may be volatile (such as random access memory (RAM)) and/or non-volatile (such as read-only memory (ROM), flash memory, etc.). The mobile device 104 may also include additional storage 206, such as either removable storage or non-removable storage including, but not limited to, magnetic storage, optical disks, and/or tape storage. The disk drives and their associated computer-readable media may provide non-volatile storage of computer-readable instructions, data structures, program modules, and other data for the mobile device. In some embodiments, the memory 202 may include multiple different types of memory, such as static random access memory (SRAM), dynamic random access memory (DRAM) or ROM.

[0058] The memory 202 of mobile device 104 may include a secure execution environment such as a secure memory (e.g., Smartcard based technology available in low-power devices). In some embodiments, the secure memory may include a secure element. A secure element (SE) can be a tamper-resistant platform (typically a one chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (e.g. key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities. In some embodiments, a token or other access credential data may be stored in the secure execution environment.

[0059] Information provisioned by a processing server onto the mobile device 104 may be stored in the secure memory. The mobile device 104 may include secure key storage to protect data at rest and encryption keys (i.e. a shared secret).

The encryption keys could be unique-derived keys (UDKs), which can be derived from user account information and other unique information. A benefit to using UDKs is that the UDKs do not need to be transported to the devices that use them, but they can be generated by those devices using information known to those devices. The mobile device 104 may also store instructions for communicating with other devices and/or instructions for initiating a payment transaction.

[0060] Turning to the contents of the memory 202 in more detail, the memory 202 may include an operating system 208 and one or more application programs or services for implementing the features disclosed herein including at least a module for managing access credentials (e.g., real credentials, parent tokens and subtokens) and transaction protocols associated with a connected device (device management module 210) and/or a module for generating or obtaining (e.g., retrieving) subtokens in accordance with transaction data (subtoken module 212). The memory 202 may also include protocol data 214, which provides data associated with one or more transaction protocols and access credential data 216, which provides information on access credentials for one or more connected devices.

[0061] In some embodiments, the device management module 210 may, in conjunction with the processor 204, be configured to manage access credentials and transaction protocols associated with a connected device. In some embodiments, the device management module may be configured to cause the mobile device 104 to identify one or more relevant connected devices. For example, upon connecting to a private network, the mobile device may aggregate a set of identifiers for connected devices currently connected to the private network. The identifiers for the devices could include device serial numbers, device network addresses, etc. In some embodiments, the mobile device 104 may query a datastore. The query may include device identifiers (e.g., protocol data 214), and these device identifiers may be queried against a set of stored identifiers to determine if the mobile device has previously encountered the connected devices. The device management module 210 may cause the mobile device 104 to, upon detecting a new connected device, contact a processing server to receive protocol data relevant to the new connected device. For example, upon establishing a communication session between a mobile

device 104 and a private network, the mobile device 104 may detect a smart refrigerator that is also connected to the private network. The mobile device may attempt to retrieve protocol data (e.g., rules regarding what types of transactions can be conducted, what type of authentication data is needed, etc.) related to the smart refrigerator from protocol database 214. Upon determining that no protocols exist, the mobile device 104 may determine that the smart refrigerator has not previously been encountered. In this example, the device management module 210 may cause the mobile device to establish a communication session with a processing server. The mobile device may provide the processing server, via the communication session, with the device identifier for the smart refrigerator. The processing server may subsequently identify one or more protocols relevant to the smart refrigerator to be provisioned onto the mobile device 104. In some embodiments, relevant protocols may be identified based on a type or category of connected device (e.g., refrigerator), a brand of connected device, user specifications, or any other suitable information.

[0062] In some embodiments, the subtoken module 212 may, in conjunction with the processor 204, be configured to generate subtokens in accordance with transaction data and relevant protocol information. A subtoken may be derived from a parent token useable to conduct a transaction. For example, the mobile device 104 may store and manage information related to one or more tokens in access credential data 216. Upon determining that a connected device should be provided with a subtoken, the subtoken generation module may cause the processors 204 to identify an appropriate token in access credential data 216 and generate a subtoken derived from that token. An exemplary subtoken may reference the same underlying account information as the parent token from which it is derived, but may be of limited duration or use. For example, the subtoken may be single-use, in that it is invalidated immediately after use. In another example, the subtoken may be associated with an expiration date, after which the subtoken is invalidated (e.g., will not be allowed to be used by the transaction processing system). In another example, the subtoken may only be useable for a particular type of transaction or by a particular connected device. In some embodiments, the subtoken module 212 may cause the mobile device 104 to provide the subtoken to a processing server, where it

may be stored. In other embodiments, the subtoken module 212 could retrieve subtokens from external sources and need not generate them.

[0063] Once subtokens are generated or obtained by the mobile device 104, a record of the subtoken generation and/or the subtokens themselves may be transmitted to a remotely located token server so that the token server is able to approve transaction requests using the subtoken. In other embodiments, if the subtokens are mathematically derivable (e.g., using encryption keys or shared secrets), then the raw data to calculate the corresponding subtoken may be transmitted to the token server.

[0064] One or more of the device management module 210 and/or the subtoken module 212 may in conjunction with the processor(s) 118 cause the mobile device 104 to establish a communication session with a detected connected device. The mobile device may provision the connected device, via the established communication session, with one or both of a subtoken generated by the subtoken module 212 and a set of protocols relevant to the connected device. In some embodiments, the set of protocols provisioned onto the connected device may be a subset of the protocols identified by the device management module 210 as being relevant to the connected device.

[0065] The mobile device 104 may also contain communications interface(s) 218 that enable the mobile device 104 to communicate with a stored database, another computing device or server, one or more terminal devices, connected devices, and/or other electronic devices on a network. The mobile device 104 may also include input/output (I/O) device(s) and/or ports 220, such as for enabling connection with a keyboard, a mouse, a pen, a voice input device, a touch input device, a display, speakers, a printer, etc.

[0066] **FIG. 3** depicts an example data flow that may be implemented in accordance with at least some embodiments. The data flow depicted in FIG. 3, may be implemented at least by the components of the example architecture depicted in FIG. 1.

[0067] In some embodiments, a mobile device 104 may receive a request from a connected device 102 to be provided with a subtoken and/or protocol data.

For example, upon detecting that one or more predetermined conditions have been met (e.g., that an available amount of a resource has fallen below a threshold level), a connected device 102 may determine that a transaction should be conducted and may transmit a request to the mobile device 104 for a subtoken to be used in the transaction. The conditions may relate to a specific time, date, or status of the connected device. For example, if the connected device 102 is a refrigerator, then a condition may be that the refrigerator has determined that it is out of eggs or milk. It may then request a subtoken so that it may purchase more milk and eggs. In this example, the mobile device 104 may, upon receiving the request, establish a communication session with the connected device 102 to identify a type and/or quantity of resources required by the connected device 102. The mobile device 104 may also identify a type of the connected device 102 related to the request. For example, the request may include a device identifier and the mobile device 104 may query a database of device identifiers (e.g., device management data 302) to determine the identity of (or a type associated with) the connected device 102. In some embodiments, the processing server 108 may identify one or more rules for generating a subtoken associated with a particular connected device from the device management data 214. For example, rules such as constraints on use may be associated with a generated subtoken. As an illustration, if a subtoken is generated for a refrigerator to buy milk and eggs, than a constraint for that subtoken may be that it can only be used at grocery stores. In some embodiments, the mobile device 104 may display the transaction to a user of the mobile device 104 to obtain approval for the transaction. In some embodiments, the transaction may be aggregated with a number of other transactions and presented to a user for approval.

[0068] In some embodiments, the mobile device 104 may detect the connected device 102 upon connecting to a private network or entering within range of the connected device 102 (e.g., via a device discovery process). Upon detecting one or more connected devices 102, the mobile device 104 may provide instructions to the connected device 102 to cause it to check the validity of a subtoken currently stored by the connected device 102. For example, the connected device 102 may check a cryptogram associated with the subtoken to determine if it is in fact authentic and operative. In some embodiments, the mobile device 104 may, upon detecting

one or more connected devices 102, transmit device identifiers for the connected devices 102 (i.e., any indicator that may be used to identify the connected device) to a processing server 108 which maintains an account associated with a user of the mobile device 104. The processing server 108 may, based on the received identifiers, identify one or more protocols relevant to the connected devices 102 and convey those protocols to the mobile device 104. In some embodiments, the protocols may be stored by the mobile device 104 in a protocol database 216. In some embodiments, the protocol data may include user preference data. For example, the protocol data may include an indication of a user's resource preferences and/or resource replenishment preferences. As an illustration, the protocol data may indicate a preference that the user wishes to use subtokens at particular resource providers (e.g., merchants) or that the user only wishes to use those subtokens during a specified time period (e.g., the first week of each month).

[0069] In some embodiments, the mobile device 104 may receive a token (or other suitable access credential) from a token server 304. A token server 304 may be an entity, not necessarily associated with the actual payment entity, that stores and maintains relationships between tokens and actual account numbers used for payment. The mobile device 104, upon receiving connected device information and an indication that a subtoken is to be generated, may generate a subtoken from the received token information (i.e., a parent token). The subtoken may be derived from a parent token, but may be limited in at least one of duration (e.g, it may expire after a period of time or number of uses), the types of transactions that it may be used to conduct, a connected device that may utilize the subtoken (e.g., the subtoken may be associated with the device identifier), or in any other suitable way. Once a subtoken has been generated, it may be provided to the connected device 102 to complete one or more transactions. In addition, the subtoken may be provided to the token server and/or the processing server along with any relevant information (e.g., a device identifier for the connected device, expiration conditions, etc.).

[0070] In some embodiments, the connected device 102 may initiate a transaction using the generated subtoken. For example, the connected device 102 may generate a transaction request to obtain a resource that includes the subtoken, an indication of the resource, a quantity of resource to obtain, or any other suitable

transaction-related information. The connected device 102 may transmit the generated transaction request to the transaction server 110 via a communication network. The transaction server 110, upon receiving the request, may generate an authorization request to be provided to an authorization computer 114 in order to determine whether to fulfill the transaction request. The authorization request may be provided to the authorization computer 114 via a transaction processing network 112. An exemplary transaction processing network 112 may include VisaNet™. Transaction processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services. The transaction processing network may use any suitable wired or wireless network, including the Internet.

[0071] In some embodiments, the authorization request may include a subtoken or other access credential, in which case, the authorization request message may first be provided to the token server 304 to retrieve account information related to the authorization request. The token server 304 may ensure that the subtoken is valid (e.g., unexpired and authorized for use in the transaction). The token server 304 may also determine the parent token, and optionally the real credential associated with the parent token, and may return the same to the transaction processing network 112.

[0072] Once the transaction processing network 112 has determined where an authorization request message is to be routed, the transaction processing network 112 may transmit the authorization request message to the appropriate authorization computer 114. If the payment information comprises a subtoken, then the authorization request message may be routed to a token server 304, or the authorization computer 114 may obtain the parent token and/or the real credential from the token server 304. As noted above, the authorization request message may include the parent token or the real account number, and either of these may be routed to the authorization computer 114. If it includes the parent token, then the authorization computer 114 may contact the token server 304 to obtain the real account number.

[0073] Once the appropriate authorization computer 114 has received the authorization request message, it may determine if the transaction should be approved. For example, the authorization computer 114 may decline the transaction if there is a high likelihood of fraud. In another example, the authorization computer 114 may decline the transaction if the payment account has insufficient funds. Once the authorization computer 114 has decided whether to approve or decline the transaction, an authorization response message may be returned to the transaction server 110 via the transaction processing network 112. If the real credential or account number was received and used by the authorization computer 114 to authorize the transaction, then the transaction processing network 112 may contact the token server 304 to obtain the parent token and/or subtoken and may include either of these in the authorization response message that is sent back to the transaction server 110.

[0074] The transaction server 110 may, upon receiving the response, determine whether the transaction has been approved or declined. The completion of the transaction may be conducted without human intervention. For example, the transaction may be conducted without acquiring authorization from a user or otherwise requiring action on a user's behalf.

[0075] In some embodiments, the transaction server 110 may provide an indication of the status of the transaction to the processing server 108. The processing server 108 may update an account associated with a user of the connected device to reflect the transaction status. For example, the processing server 108 may add a receipt to a user's account for the requested resources. In some embodiments, the processing server 108 and/or transaction server 110 may communicate the status of the transaction to the mobile device 104.

[0076] In some embodiments, the mobile device 104 may update, upon receiving an indication of the status of the transaction, one or more protocols and/or replenishment conditions stored on the connected device 102. For example, the mobile device 104 may indicate that the resource is currently on order to prevent the connected device from re-ordering the resource. In another example, the mobile device 104 may indicate to the connected device that the subtoken is now invalid upon completion of the transaction.

[0077] It should be noted that although the mobile device 104 is depicted as being a separate device from the processing server 108, the two devices may actually be the same device. For example, the mobile device 104 may store a parent token and device protocols to be used in generating a subtoken and/or device-specific protocols.

[0078] FIG. 4 depicts an illustrative example of a mobile device capable of generating subtokens and protocols to be provided to multiple connected devices in accordance with at least some embodiments. In FIG. 4, a mobile device 104 may detect multiple connected devices 102.

[0079] In some embodiments, the mobile device 104 may identify a type or category associated with each connected device 102 based on a device identifier. This may be accomplished by the mobile device 104 itself, or it may be accomplished by providing the device identifiers to a processing server 108. In some cases, a device identifier may be advertised or otherwise published on a private network. In some cases, the mobile device 104 may connect to each connected device 102 to obtain a device identifier. For each connected device 102 (1..N), a set of master protocols and a parent token may be identified by the processing server 108 and/or the mobile device 104. For example, if a connected device is a refrigerator, then the processing server 108 may identify a set of master protocols relevant to a refrigerator. A set of master protocols may include an indication of a format in which protocols should be provided to the refrigerator, as well as an indication of functionality available from a particular connected device. In some embodiments, the set of master protocols may be provided to the processing server 108 by a manufacturer of the connected device 102. In some embodiments, a separate parent token may be provided to the mobile device 104 for each connected device. In other embodiments, the mobile device 104 may receive a single parent token to be used to generate subtokens for each connected device 102.

[0080] The mobile device 104 may cause one or more of connected devices 102 to determine whether a subtoken stored on the device is valid (e.g., not expired or otherwise invalidated). Upon detecting that one or more subtokens is no longer valid, the connected device 102 may submit a request to the mobile device 104 for a new subtoken. In some embodiments, the connected device 102 may transmit

information related to one or more transactions to be conducted by the connected device 102. For example, upon detecting that it is the first of the month, a smart gas meter may determine that a transaction should be conducted for the previous month's gas useage. In this example, the smart gas meter may provide information to the mobile device related to the previous month's gas useage with a request for a subtoken to complete the transaction.

[0081] In some embodiments, the mobile device 104 may display, or otherwise present, the transaction information to a user of the mobile device. In some embodiments, the mobile device 104 may aggregate a number of transactions provided by multiple connected devices 102. In some embodiments, the mobile device 104 may require authentication by the user before proceeding.

[0082] Upon receiving authorization from a user (in embodiments which require authorization to be provided by a user), the mobile device 104 may generate a subtoken from a parent token that the mobile device has stored. A subtoken may be any combination of characters that may be stored in relation to the parent token. A subtoken is similar to a token, but the subtoken may be associated with one or more limitations. For example, the subtoken may be associated with an expiration date, a maximum number of uses, a type of resource for which it may be used, or any other suitable limitation. Once generated, the subtoken may be provided to the processing server 108 and/or a token server. The subtoken may be provided to the token server along with an indication of the parent token, limitations, a device identifier of the connected device, or any other suitable information. In some embodiments, each connected device 102 (1..N) may be provided with a separate subtoken. In some embodiments, a single subtoken may be provided to multiple connected devices 102 (1..N).

[0083] The mobile device 104 may provide the generated subtoken to the connected device. In some cases, the connected device may be provided with a set of protocols relevant to the connected device 102. For example, the set of protocols may include rules or conditions upon which the connected device may initiate a transaction using the provided subtoken. The connected device 102 may subsequently generate a transaction request that includes the provided subtoken and an indication of the resource to be obtained.

[0084] By way of illustrative example, consider a scenario in which the connected device 102 is a smart refrigerator. In this example, the mobile device 104 may connect to a private network to which the smart refrigerator is also connected. Upon connecting to the private network, the mobile device 104 may retrieve a device identifier for the smart refrigerator. Upon providing the device identifier to a processing server, the mobile device 104 may receive a set of master protocols for the smart refrigerator as well as a parent token from the processing server. In some cases, the mobile device 104 may already have a set of protocols and/or parent token stored. The mobile device 104 may also be provided with user preferences related to transactions conducted by the smart refrigerator (e.g., an indication of a transaction server to be used, brand preference information, etc.).

[0085] Continuing with the above example, the mobile device 104 may cause the smart refrigerator to determine whether a subtoken currently stored by the refrigerator is expired or otherwise invalid. The smart refrigerator, as well as other connected devices on the private network, may provide information to the mobile device 104 for one or more transactions to be conducted. The mobile device 104 may, upon receiving the transaction information, display the transaction information to a user of the mobile device 104 for authorization.

[0086] Upon receiving authorization from a user, the mobile device 104 may generate a subtoken for the smart refrigerator. In some embodiments, the mobile device 104 may identify a parent token that can be used to conduct a transaction, and generate a subtoken from the identified parent token. Upon generating the subtoken, the subtoken may be provided to the smart refrigerator along with a set of protocols relevant to the transaction to be conducted. The mobile device 104 may also provide the subtoken to a token server with an indication that the subtoken may only be used by the refrigerator (e.g., an indication of the device identifier for the refrigerator) and an expiration date. Once the smart refrigerator has received the subtoken, it may conduct a transaction using that subtoken.

[0087] **FIG. 5** depicts a flow diagram illustrating a process for discovering one or more connected devices and subsequently providing subtokens in accordance with at least some embodiments. The first segment on FIG. 5 (502-506) depicts a discovery process for identifying one or more connected devices and receiving

information to be used in generating subtokens for those connected devices. The second segment of FIG. 5 (508-520) depicts generation of subtokens / protocols for the discovered connected devices.

[0088] Some or all of any of the processes described herein (or variations and/or combinations thereof) may be performed under the control of one or more computer systems configured with executable instructions and may be implemented as code (e.g., executable instructions, one or more computer programs or one or more applications). In accordance with at least one embodiment, the process 500 of FIG. 5 may be performed by at least the mobile device 104 depicted in FIG. 1 and FIG. 2. The code may be stored on a computer-readable storage medium, for example, in the form of a computer program including a plurality of instructions executable by one or more processors. The computer-readable storage medium may be non-transitory.

[0089] Process 500 may begin at 502, when device discovery process is initiated by the mobile device. In some embodiments, the device discovery may be initiated by activating a mechanism on the mobile device (e.g., pressing a button located on the mobile device). In some embodiments, the device discovery may be initiated via a user interface. For example, a user may be presented with connected device discovery options on a display of the user device. In some embodiments, the device discovery process may be initiated upon the mobile device connecting to a private network. The device discovery process may involve identifying one or more communicatively connected electronic devices within range of the mobile device using one or more communication means. In some embodiments, a connected device may be connected directly (i.e., hardwired) to the mobile device. In some embodiments, the mobile device may request information on security protocols and/or security certificates from the connected device. In some embodiments, a user may be required to enter a password at the connected device and/or press a button on the connected device to establish that the user is in possession of the connected device.

[0090] Upon identifying one or more potential connected devices, the mobile device may be programmed to provide device identifiers for the discovered devices to a processing server at 504. Device identifiers may be published on a private

network or they may be requested from each of the discovered connected devices by the mobile device.

[0091] Once the mobile device has provided the device identifier to the processing server, the mobile device may receive a set of protocols and/or a parent token at 506. In some embodiments, the mobile device may associate a parent token with each connected device. In some embodiments, the mobile device may maintain a single parent token associated with the mobile device to be used to generate a number of subtokens for each connected device. In some embodiments, upon discovery of a connected device, the mobile device may communicate the device identifier of the connected device to the processing server. The processing server, in turn, may generate a parent token specific to that connected device and may provide the generated parent token to the mobile device to be stored in association with the connected device.

[0092] In some embodiments, upon discovery of a connected device, the mobile device may determine that the connected device is currently associated with a subtoken (e.g., the connected device is already associated with a parent token stored on the mobile device). The mobile device may reissue a subtoken to a connected device upon determining that the subtoken currently associated with the connected device should be re-authenticated. For example, the mobile device may, upon discovery of a connected device, determine that the connected device is associated with a subtoken that is expired or is about to expire. In this example, the mobile device may generate a new subtoken from the parent token to be provisioned onto the connected device. Further in this example, the new subtoken may be associated with new expiration conditions (e.g., a new expiration date) that will prolong the subtoken. In some embodiments, the subtoken currently associated with a connected device may be extended by updating expiration conditions associated with the subtoken stored by the processing server. In some embodiments, a mobile device may automatically (e.g., without user intervention) re-authenticate subtokens associated with each connected device in a plurality of connected devices. In some embodiments, upon establishing a connection between a mobile device and a private network, a user of the mobile device may be asked to verify whether one or

more subtokens currently associated with the connected device should be re-authenticated.

[0093] In some embodiments, the processing server may also identify one or more protocol sets to be associated with the connected device. The protocol sets may be selected based on a type of the connected device, user preferences and/or settings, credit limits, or any other suitable factors. In some embodiments, the processing server may maintain a user account for the user of the connected device. The user may be provided with the capability to log into an account website maintained by the processing server in order to specific one or more user settings to be applied to the connected device. In some embodiments, the user may specify a date upon which a transaction should be initiated, a minimum or maximum currency value to be associated with transactions conducted by the connected device, conditions upon which further user authorization is required, a quantity and/or type of resource to be replenished (in some cases, a particular brand), a merchant from which the resource should be obtained, or any other suitable user preference. Each of these user preferences may be stored as protocol set data. The processing server may, upon receiving a device identifier for a connected device, identify any potentially relevant protocol sets and provide those protocol sets to the mobile device in relation to the connected device. In some embodiments, the mobile device may further communicate at least a subset of the provided protocol set to the connected device. For example, the mobile device may provide an indication of conditions upon which a transaction should be initiated to the connected device.

[0094] Once a connected device has been discovered, the mobile device may establish a communication session with the connected device at 508. In some embodiments, the communication session may be established via a private network connection. In some embodiments, the communication session may be established directly with the connected device via a wireless communication mechanism.

[0095] Upon detecting that a communication session has been established, the connected device may provider a request to conduct a transaction to the mobile device at 510. The request may include one or more of an indication of at least one resource, a transaction server, a currency amount, or any other suitable transaction-

related data. In some embodiments, the request may be encrypted using an encryption key provided to the connected device.

[0096] Upon receiving the request, the mobile device may identify an appropriate parent token to be used to generate a subtoken for the requested transaction at 512. In some embodiments, the mobile device may query a data store to identify a parent token associated with the connected device. In some embodiments, the mobile device may utilize single parent token (or set of parent tokens) for each subtoken that it generates on behalf of the identified connected devices.

[0097] In some embodiments, the mobile device may confirm that the requested transaction is in compliance with one or more relevant protocols at 514. In some embodiments, the mobile device may identify each of the relevant protocol set data and determine whether any/all conditions have been satisfied. In some embodiments, the mobile device may forward details of the potential transaction to a processing server, which may subsequently determine whether that transaction is in compliance with relevant protocol set data.

[0098] In some embodiments, the mobile device may identify a set of device-specific protocols to be provided to the connected device at 516. The set of protocols may include an indication of resources preferred by a user, a brand of the resource, a transaction server from which the resource should be obtained, conditions upon which a transaction for the resource may be conducted, or any other suitable resource-related information. The protocols may be device-specific protocols, in that a set of protocols provided to each connected device is unique to the connected device to which it is provided. In some embodiments, the device-specific protocols may include information related to a subtoken provided to the connected device (e.g., an expiration date of the subtoken, usage limitations, a maximum currency threshold, etc.).

[0099] Upon determining that the transaction is in compliance with relevant protocols, the mobile device may generate a subtoken at 518. A subtoken may be associated with an account underlying the parent token, but may be subject to limitations that the parent token is not necessarily subject to. In some embodiments,

the limitations may be based on transaction information provided to the mobile device. For example, if a water meter provides transaction information to the mobile device indicating that the previous month's water useage should be paid for, then a subtoken generated by the mobile device may be redeemable only by a water utility company and only within the next 15 days. In another example, a mobile device may receive transaction information from a smart refrigerator indicating a type of food that the refrigerator needs to replenish. In this example, the mobile device may determine, based on user preferences indicated in the set of protocols, that the refrigerator should order the food only from a particular merchant. The mobile device may also determine that the user prefers a particular brand of that type of food. The subtoken generated by the mobile device may be useable only at the specified merchant and only for a specified maximum amount. In addition, the mobile device may provide a set of device-specific protocols to the refrigerator to indicate that the user-preferred brand should be ordered.

[0100] In some embodiments, the mobile device may provide the generated subtoken and/or a set of device-specific protocols to a connected device at 520. The connected device may subsequently conduct one or more transactions using the generated subtoken and device-specific protocols.

[0101] **FIG. 6** depicts an exemplary embodiment in which a subtoken is generated for a computer device and used to obtain software and/or software updates. As depicted in FIG. 6, a user indicate an intent to use the computer device 602 (e.g., the user may attempt to log into the computer device 602). In some embodiments, the user may submit a request to provide the computer device with a specific application or upgrade. The computer device 602 may be an example connected device 102 of FIG. 1. The computer device 602 may, upon receiving an indication that the user wishes to interact with it, establish a communication session with the user's mobile device 104. The computer device 602 may transmit, via the established communication session, a device identifier identifying the computer device 602 to the mobile device 104.

[0102] Upon receiving the device identifier from the computer device 102, the mobile device may determine if a request associated with the computer device 102 should be allowed. In some embodiments, the mobile device may confirm with the

user that he or she wishes to interact with the computer device 602. Upon determining that the user does wish to interact with the computer, the mobile device may generate a subtoken useable by the computer device 602 to access user-specific data and/or software. The mobile device 104 may transmit the subtoken to the computer device 602. In some embodiments, the mobile device 104 may also transmit the subtoken to a processing server 108 that supports an application on the mobile device 104.

[0103] In some embodiments, the requested user interaction may be to use one or more software applications associated with the user. The computer device 602, upon receiving the subtoken, may generate a request for one or more software applications and/or software upgrades to a transaction server 110. The transaction server 110 may confirm the validity of the subtoken with an authorization computer 114 and/or a processing computer 108.

[0104] Upon confirming the validity of the subtoken, the transaction server 110 may access profile data 604 associated with the user of the mobile device 104. The profile data 604 may indicate one or more applications stored within an application database 606 that the user has a license to use. (e.g., that the user has rights to). In some embodiments, the subtoken may be associated with a license, such that the receipt of the subtoken results in licensing information being added to the profile of the user. In some embodiments, the subtoken may be a limited-use token, such that it may only be redeemed at a specified number of computing devices 602. Upon identifying one or more applications that the user is authorized to execute, the transaction server 110 may determine whether an application requested by the computer device 602 is among the identified applications. If it is not, then the transaction server 110 may decline the transaction. If the requested application is among those authorized to be used by the user, then the computer device 602 may be given a location of the application in the application data 606 so that the requested application may be downloaded by the computer device.

[0105] In some embodiments, the computer device 602 may be provided with, or used to access, one or more applications from the application data 606. In some embodiments, the computer device 602 may be imaged with a user profile for the user upon verification of the subtoken. For example, a number of applications that

the user is authorized to access may be made available to the computer device 602 upon the user's login. In some embodiments, the transaction server 110 may be a virtual computing instance (e.g., a cloud computing environment) associated with the user. The computer device 602 may connect to the virtual computing instance upon verification of the subtoken, such that the virtual computing instance is displayed by the computing device 602.

[0106] By way of illustrative example, a user may attempt to log into the computer device 602. Upon receiving the login attempt, the computer device 602 may initiate a communication with the user's mobile device. The user may be asked, by the mobile device 104, to verify that he or she is attempting to access the computer device 602. Upon receiving verification from the user, the mobile device 104 may generate a subtoken and provide it to the computer device 602. The computer device 602 may, in turn, transmit the subtoken to the transaction server 110. Upon receiving the subtoken, the transaction server 110 may access a virtual computing instance associated with the user such that the user is able to access one or more applications installed on and executed by the transaction server 110 from the computer device 602.

[0107] In another example, the user may have an account with a transaction server 110 that maintains a digital library associated with the user. In this example, the user may access the computer device 602 and request download of a particular software application. In this example, the computer device 602 may initiate a communication with the mobile device 104. The mobile device 104 may communication with the transaction server 110 via the processing server 108 to determine what software licenses the mobile device 104 is associated with. The mobile device 104 may be provided with a list or selection of software applications that may be installed on the computer device 602. In this example, the user may select one or more applications from the list and a subtoken may be generated based on this selection. The subtoken may be provided to the computer device 602, which may subsequently redeem the subtoken with the transaction server 110. In this example, the selected software applications may be provided to the computer device 602.

[0108] A computer system can include a plurality of the same components or subsystems, e.g., connected together by external interface or by an internal interface. In some embodiments, computer systems, subsystem, or apparatuses can communicate over a network. In such instances, one computer can be considered a client and another computer a server, where each can be part of a same computer system. A client and a server can each include multiple systems, subsystems, or components.

[0109] Embodiments of the invention provide for a number of technical advantages. For example, embodiments of the invention enable connected devices to conduct transactions using subtokens of limited duration. In these embodiments, the subtoken may be invalidated shortly after being used in a transaction, preventing their use by an unauthorized party, even if the subtoken was intercepted in a transaction request. In addition, subtoken information acquired from a connected device that was disposed of may not be used to defraud a previous owner of the connected device, as the token would automatically expire. Additionally, a subtoken may be valid for a specified period of time in which a user of a mobile device may be present. For example, if a user intends to stay in a hotel room for one week, then connected devices in his or her hotel room may be provided with a subtoken and protocols that will automatically expire at the end of the stay. During the stay, the connected devices would conduct transactions in accordance with the user's preferences. The use of subtokens in different connected devices thus increases transaction security, since the validity and policies specifically associated with the use of those subtokens is confined to the functions that the connected devices are intended to perform. In addition, since the subtokens are subordinate to the parent token, all transactions can be recorded against an account associated with a single parent token, thus making it easier for a user to administer. Lastly, because a parent token and subtokens are used, even the unauthorized use of one or more of the subtokens results in limited exposure since those subtokens can only be used in limited circumstances and under specific conditions.

[0110] It should be understood that any of the embodiments of the present invention can be implemented in the form of control logic using hardware (e.g. an application specific integrated circuit or field programmable gate array) and/or using

computer software with a generally programmable processor in a modular or integrated manner. As used herein, a processor includes a single-core processor, multi-core processor on a same integrated chip, or multiple processing units on a single circuit board or networked. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement embodiments of the present invention using hardware and a combination of hardware and software.

[0111] Any of the software components or functions described in this application may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C, C++, C#, Objective-C, Swift, or scripting language such as Perl or Python using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions or commands on a computer readable medium for storage and/or transmission, suitable media include random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a compact disk (CD) or DVD (digital versatile disk), flash memory, and the like. The computer readable medium may be any combination of such storage or transmission devices.

[0112] Such programs may also be encoded and transmitted using carrier signals adapted for transmission via wired, optical, and/or wireless networks conforming to a variety of protocols, including the Internet. As such, a computer readable medium according to an embodiment of the present invention may be created using a data signal encoded with such programs. Computer readable media encoded with the program code may be packaged with a compatible device or provided separately from other devices (e.g., via Internet download). Any such computer readable medium may reside on or within a single computer product (e.g. a hard drive, a CD, or an entire computer system), and may be present on or within different computer products within a system or network. A computer system may include a monitor, printer, or other suitable display for providing any of the results mentioned herein to a user.

[0113] The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon

review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents. For example, although the described embodiments mention the use of subtokens for purchase transactions, subtokens can also be used to access data in remote systems. For example, different connected devices may request software upgrades from a remote computer, but may need to have valid tokens before the upgrades can be obtained.

[0114] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0115] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0116] All patents, patent applications, publications, and descriptions mentioned above are herein incorporated by reference in their entirety for all purposes. None is admitted to be prior art.

2016409079 04 Jun 2021

WHAT IS CLAIMED IS:

1. A method of operating a mobile device to provide limited-use subtokens to a plurality of connected devices connected to a private network, the method comprising:

connecting, by a mobile device, to a private network;

identifying, by the mobile device, a plurality of connected devices connected to the private network;

receiving, from the plurality of connected devices, information related to a plurality of transactions, each transaction being requested by a respective one of the plurality of connected devices;

in response to receiving the information, for each transaction:

identifying a protocol set associated with the respective connected device;

determining, based on the information related to the transaction, whether the transaction is compliant with one or more protocols in the protocol set;

in response to determining that the transaction is compliant with the one or more protocols, generating, by the mobile device, from a parent token associated with the mobile device, a limited-use subtoken specific to a transaction type of the transaction, wherein the parent token and the limited-use subtoken reference the same account information; and

providing, by the mobile device, the limited-use subtoken and at least a portion of the identified protocol set to the connected device from which the information related to the transaction was received, the subtoken being stored in a secure memory of the connected device;

wherein each of the limited-use subtokens is useable to initiate the respective transaction to be conducted by the respective connected device in accordance with the portion of the identified protocol set.

2. The method of claim 1 further comprising:

providing management rules to each of the connected devices associated with the transactions, the management rules comprising instructions for initiating at least one transaction of the transactions.

2016409079 04 Jun 2021

3. The method of claim 1 wherein the information related to the transactions requested by the plurality of connected devices comprises an aggregated list of transactions to be conducted by the plurality of connected devices.

4. The method of claim 1 wherein each limited-use subtoken is of limited duration.

5. The method of claim 1 further comprising:

authenticating, by the mobile device, each of the plurality of connected devices before providing the limited-use subtoken to the connected device.

6. A mobile device comprising:

one or more processors; and

a memory including instructions that, when executed by the one or more processors, cause the mobile device to:

connect to a private network;

identify a plurality of connected devices in communication with the private network;

receive, from the plurality of connected devices, information related to transactions to be conducted by the plurality of connected devices, each transaction being requested by a respective one of the plurality of connected devices;

and for each transaction:

identify a protocol set associated with the respective connected device;

determine, based on the information related to the transaction, whether the transaction is compliant with one or more protocols in the protocol set;

in response to a determination that the transaction is compliant with the one or more protocols, generate, from a parent token associated with the mobile device, a limited-use subtoken specific to a transaction type of the transaction, wherein the parent token and the limited-use subtoken reference the same account information; and

provide, the limited-use subtoken and at least a portion of the identified protocol set to the connected device from which the information

2016409079 04 Jun 2021

related to the transaction was received, the subtoken being stored in a secure memory of the connected device;

wherein each limited-use subtoken is useable to initiate the respective

transaction to be conducted by the respective connected devices in accordance with the respective portions of the identified protocol set.

7. The mobile device of claim 6, wherein the transactions to be conducted by the plurality of connected devices are related to replenishment resources managed by the plurality of connected devices.

8. The mobile device of claim 6, wherein the instructions further cause the mobile device to convey the subtoken to a server computer along with information related to the at least one transaction.

9. The mobile device of claim 6, wherein the limited-use subtoken derived from the parent token is associated with one or more limitations.

10. The mobile device of claim 9, wherein the one or more limitations are associated with the limited-use subtoken based on a type of the connected device to which it is provided.

11. The mobile device of claim 9, wherein the limitations comprise one or more of an expiration date, a maximum number of uses, or a type of resource for which it may be used.

12. The mobile device of claim 6, wherein the mobile device is a mobile phone.

13. The mobile device of claim 6, wherein providing the limited-use subtoken derived from the parent token to each connected device of the plurality of connected devices comprises re-authenticating an existing limited-use subtoken for at least one connected device of the plurality of connected devices.

14. A connected device comprising:

one or more processors; and

2016409079 04 Jun 2021

a memory including instructions that, when executed by the one or more processors, cause the connected device to:

connect to a private network;

establish, via the private network, a communication session with a mobile device;

provide, to the mobile device via the communication session, an indication of at least one transaction to be conducted in relation to a resource managed by the connected device;

receive, from the mobile device via the communication session, a limited-use subtoken useable to conduct the at least one transaction and a subset of protocols, wherein the limited-use subtoken is derived from a parent token associated with the mobile device and is specific to a transaction type of the at least one transaction;

store the limited-use subtoken in the secure memory;

determine, based on the subset of protocols, whether to conduct the at least one transaction; and

upon determining to conduct the at least one transaction,

initiate, using the received limited-use subtoken, the at least one transaction.

15. The connected device of claim 14, wherein the connected device initiates the at least one transaction by generating a transaction request that includes an indication of the resource and the limited-use subtoken.

16. The connected device of claim 15, wherein the instructions further cause the connected device to transmit the generated transaction request to a provider of the resource.

17. The connected device of claim 14, wherein the limited-use subtoken is configured to be useable only by the connected device.

18. The connected device of claim 14, wherein the connected device is a car or a washing machine.

19. The connected device of claim 18, wherein the set of protocols includes an indication of a limitation associated with the limited-use subtoken.

20. The connected device of claim 19, wherein the limited-use subtoken is used to obtain a software upgrade for the connected device.

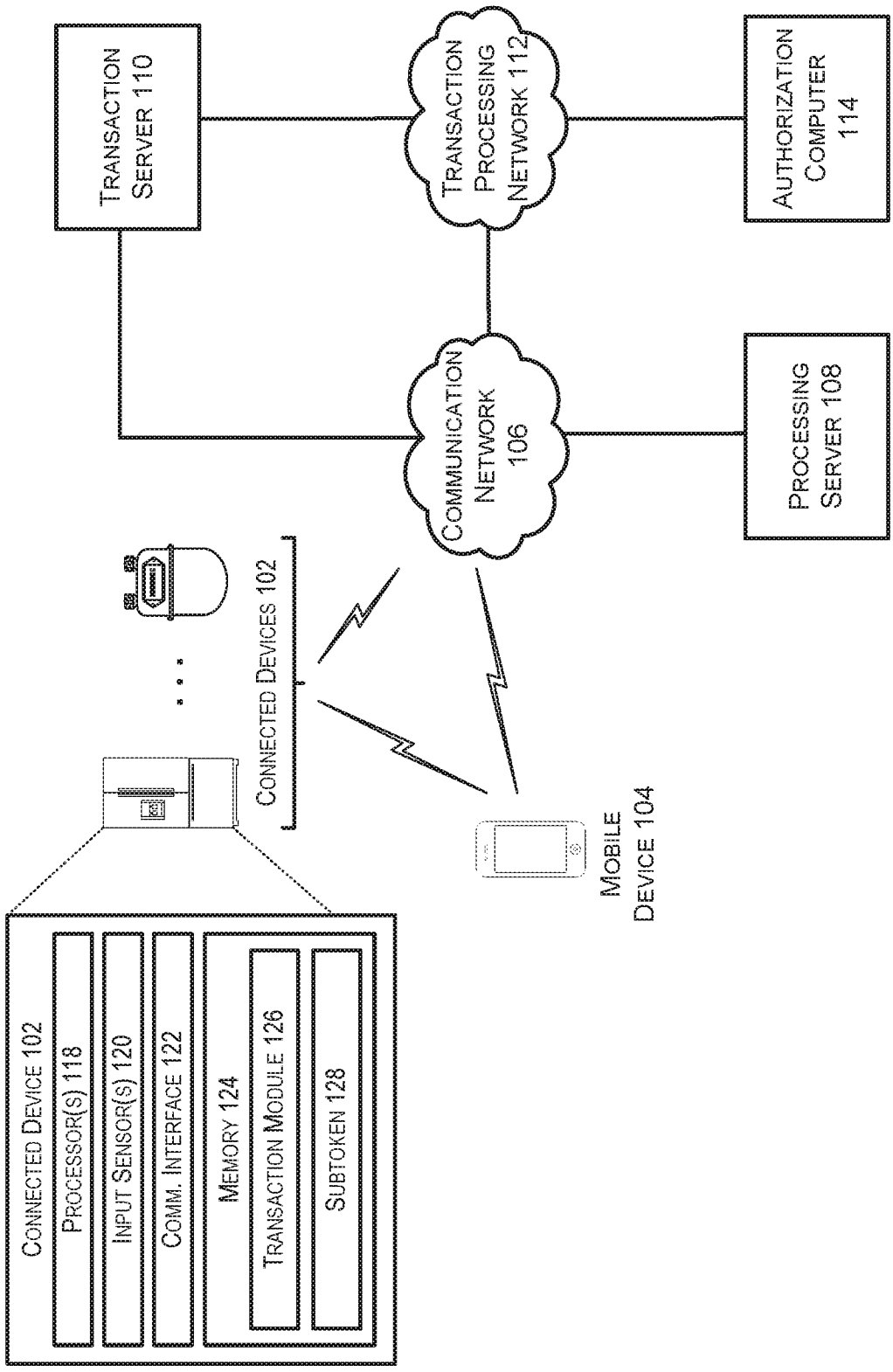
TRANSACTION SERVER 110
TRANSACTION PROCESSING NETWORK 112
AUTHORIZATION COMPUTER 114
COMMUNICATION NETWORK 106
PROCESSING SERVER 108
CONNECTED DEVICES 102
MOBILE DEVICE 104
CONNECTED DEVICE 102
PROCESSOR(S) 118
INPUT SENSOR(S) 120
COMM. INTERFACE 122
MEMORY 124
TRANSACTION MODULE 126
SUBTOKEN 128

FIG. 1

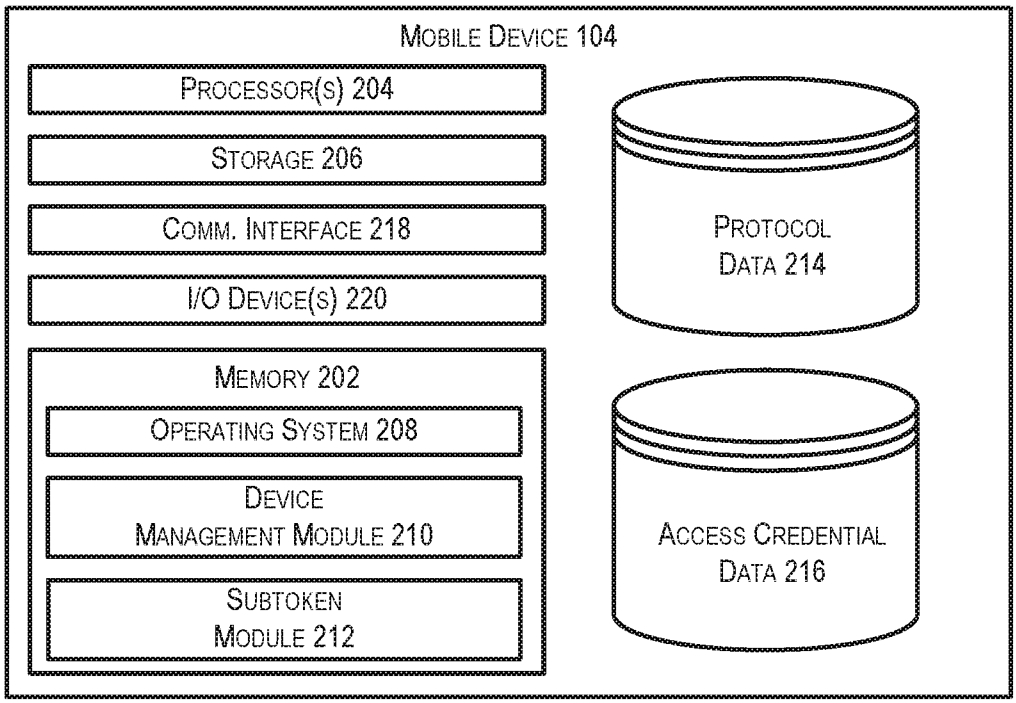
MOBILE DEVICE 104
PROCESSOR(S) 204
STORAGE 206
COMM. INTERFACE 218
I/O DEVICE(S) 220
MEMORY 202
OPERATING SYSTEM 208
DEVICE MANAGEMENT MODULE 210
SUBTOKEN MODULE 212
PROTOCOL DATA 214
ACCESS CREDENTIAL DATA 216

FIG. 2

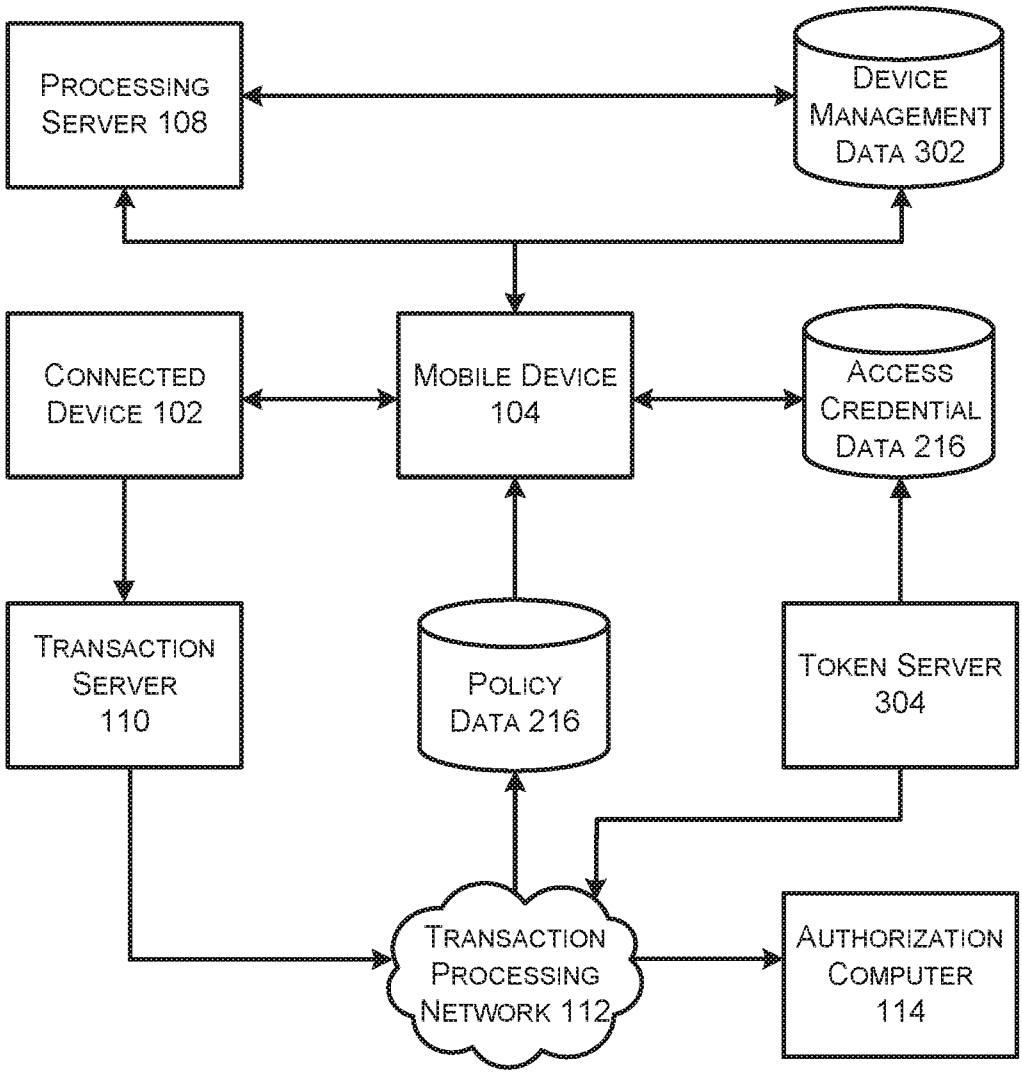
PROCESSING SERVER 108
DEVICE MANAGEMENT DATA 302
CONNECTED DEVICE 102
MOBILE DEVICE 104
ACCESS CREDENTIAL DATA 216
TRANSACTION SERVER 110
POLICY DATA 216
TOKEN SERVER 304
TRANSACTION PROCESSING NETWORK 112
AUTHORIZATION COMPUTER 114

FIG. 3

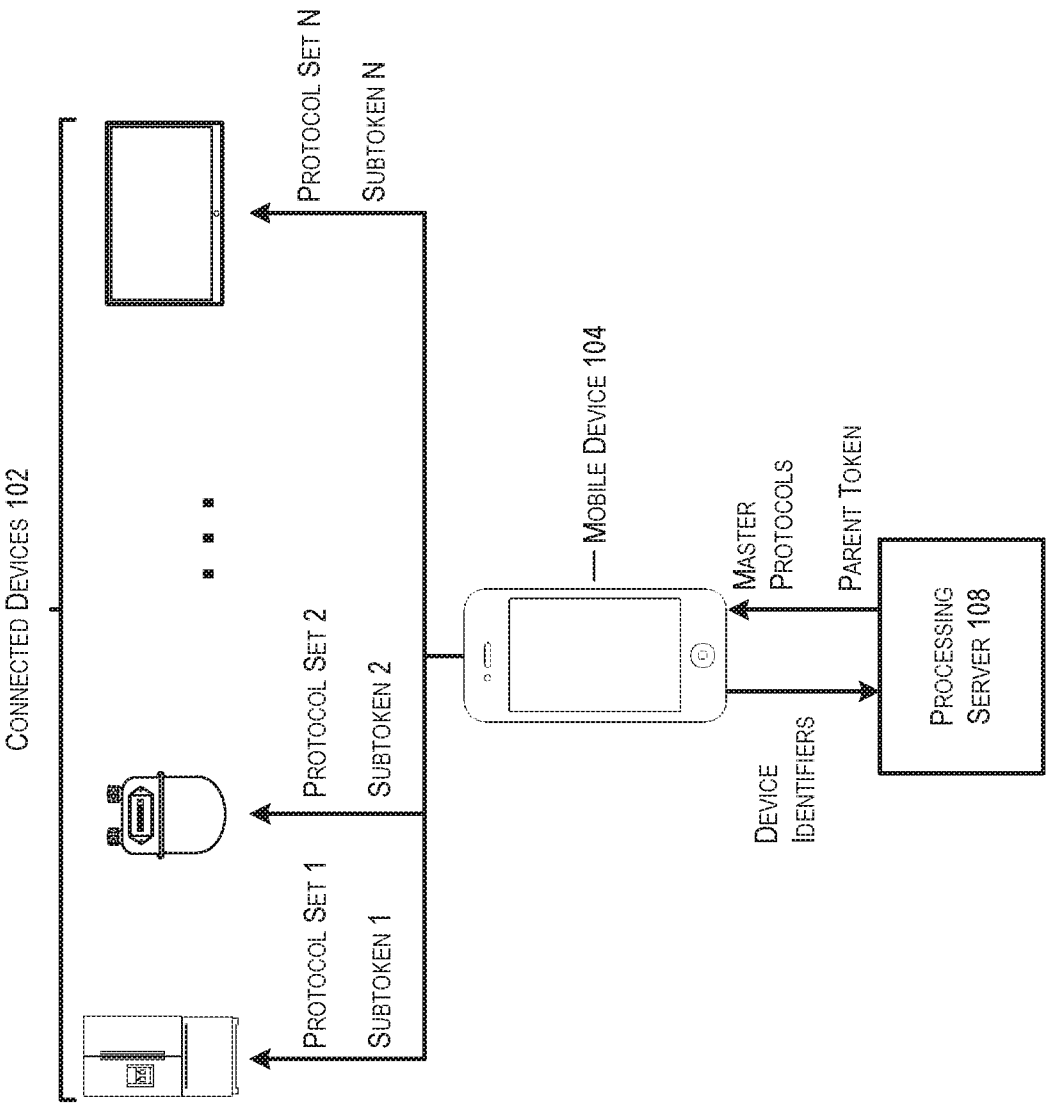
CONNECTED DEVICES 102
PROTOCOL SET 1
SUBTOKEN 1
PROTOCOL SET 2
SUBTOKEN 2
PROTOCOL SET N
SUBTOKEN N
MOBILE DEVICE 104
MASTER PROTOCOLS
PARENT TOKEN
DEVICE IDENTIFIERS
PROCESSING SERVER 108

FIG. 4

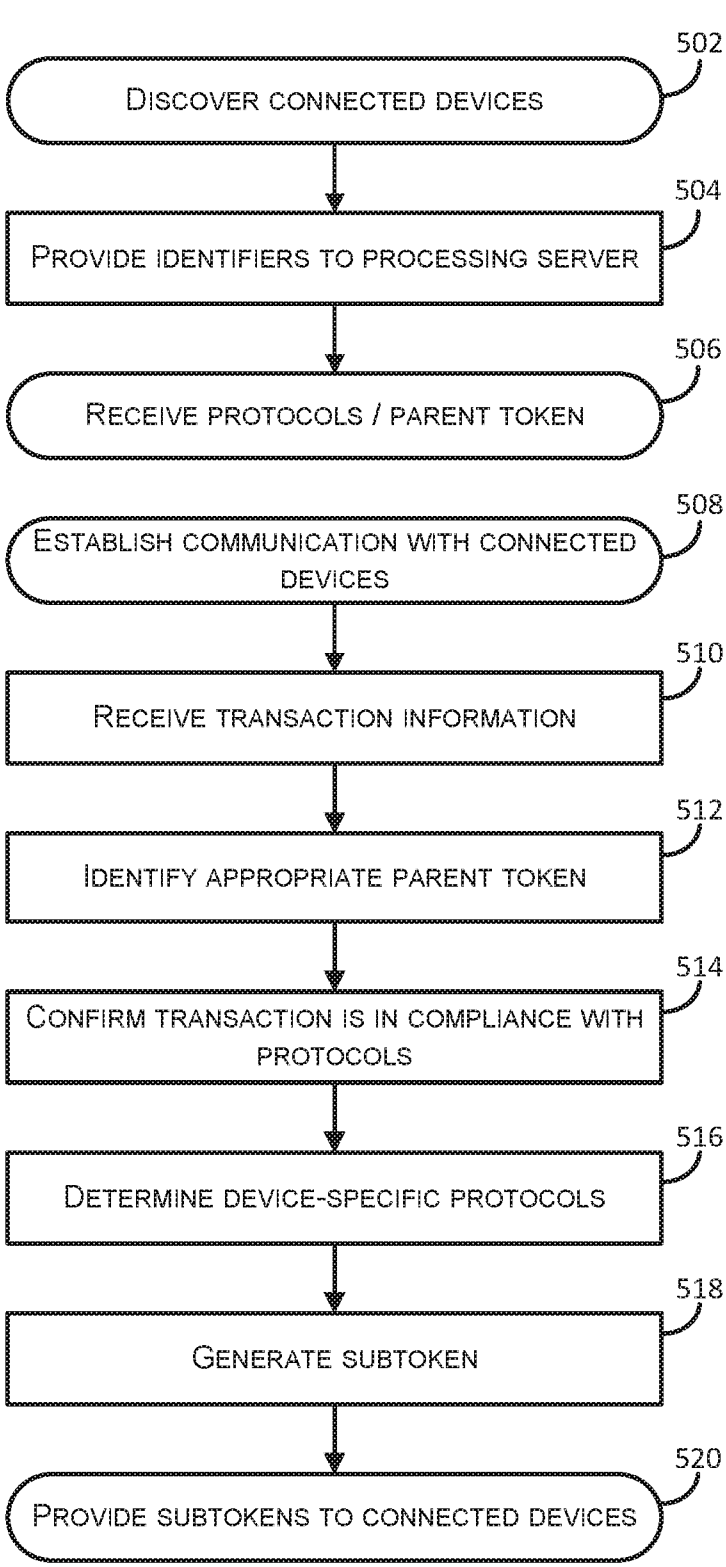
500
502
DISCOVER CONNECTED DEVICES
504
PROVIDE IDENTIFIERS TO PROCESSING SERVER
506
RECEIVE PROTOCOLS / PARENT TOKEN
508
ESTABLISH COMMUNICATION WITH CONNECTED DEVICES
510
RECEIVE TRANSACTION INFORMATION
512
IDENTIFY APPROPRIATE PARENT TOKEN
514
CONFIRM TRANSACTION IS IN COMPLIANCE WITH PROTOCOLS
516
DETERMINE DEVICE-SPECIFIC PROTOCOLS
518
GENERATE SUBTOKEN
520
PROVIDE SUBTOKENS TO CONNECTED DEVICES

FIG. 5

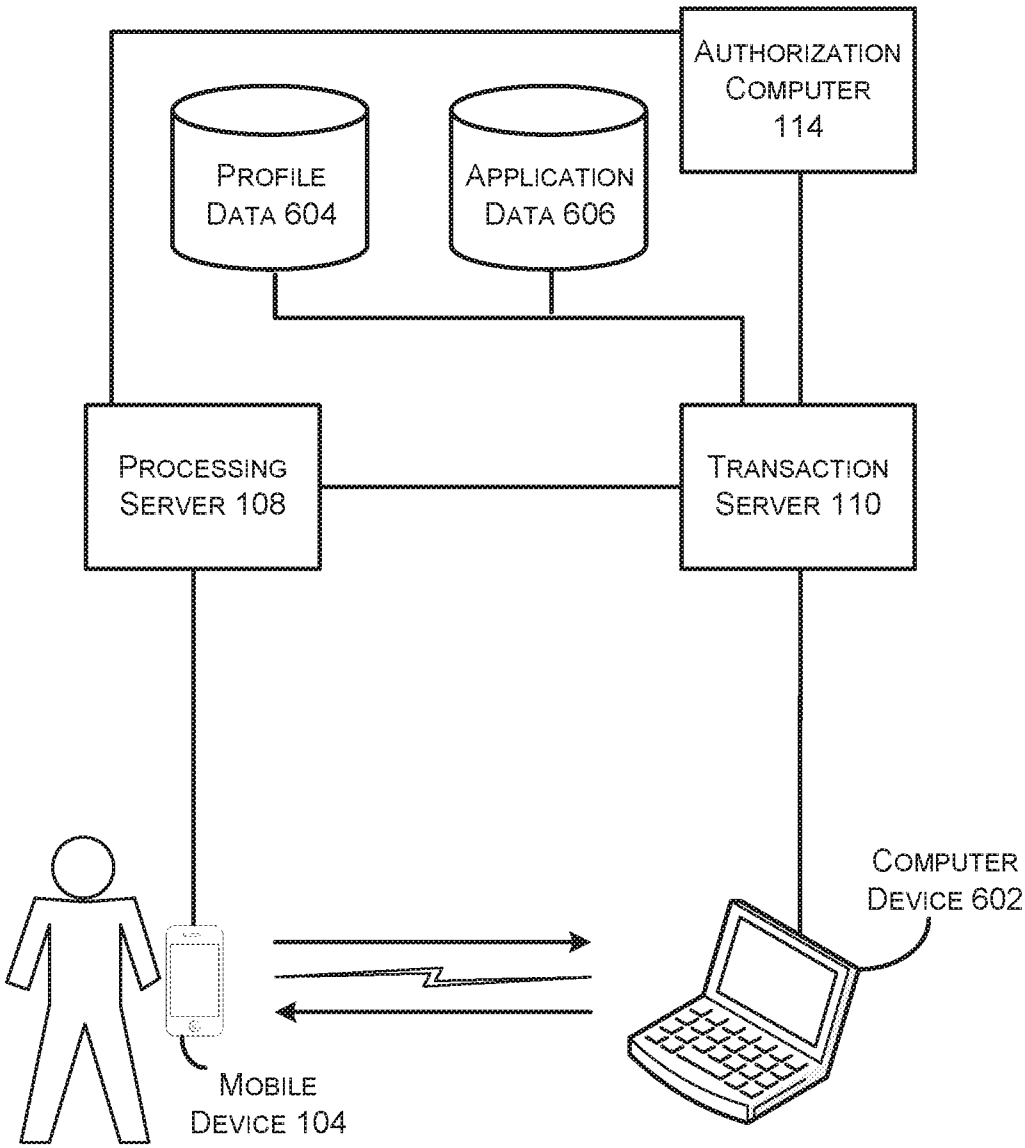
AUTHORIZATION COMPUTER 114
PROFILE DATA 604
APPLICATION DATA 606
PROCESSING SERVER 108
TRANSACTION SERVER 110
COMPUTER DEVICE 602
MOBILE DEVICE 104

FIG. 6