US 20230145489A1

(19) **United States**
(12) **Patent Application Publication**
Prakash et al.

(10) **Pub. No.: US 2023/0145489 A1**
(43) **Pub. Date: May 11, 2023**

(54) **PROVISIONING PLATFORM FOR MACHINE-TO-MACHINE DEVICES**

(71) Applicant: **Visa International Service Association**, San Francisco, CA (US)

(72) Inventors: **Gyan Prakash**, Foster City, CA (US); **Ajit Gaddam**, Sunnyvale, CA (US); **Selim Aissi**, Dublin, CA (US)

(73) Assignee: **Visa International Service Association**, San Francisco, CA (US)

(21) Appl. No.: **18/152,025**

(22) Filed: **Jan. 9, 2023**

Related U.S. Application Data

(62) Division of application No. 14/955,716, filed on Dec. 1, 2015, now Pat. No. 11,580,519.

(60) Provisional application No. 62/091,097, filed on Dec. 12, 2014.

Publication Classification

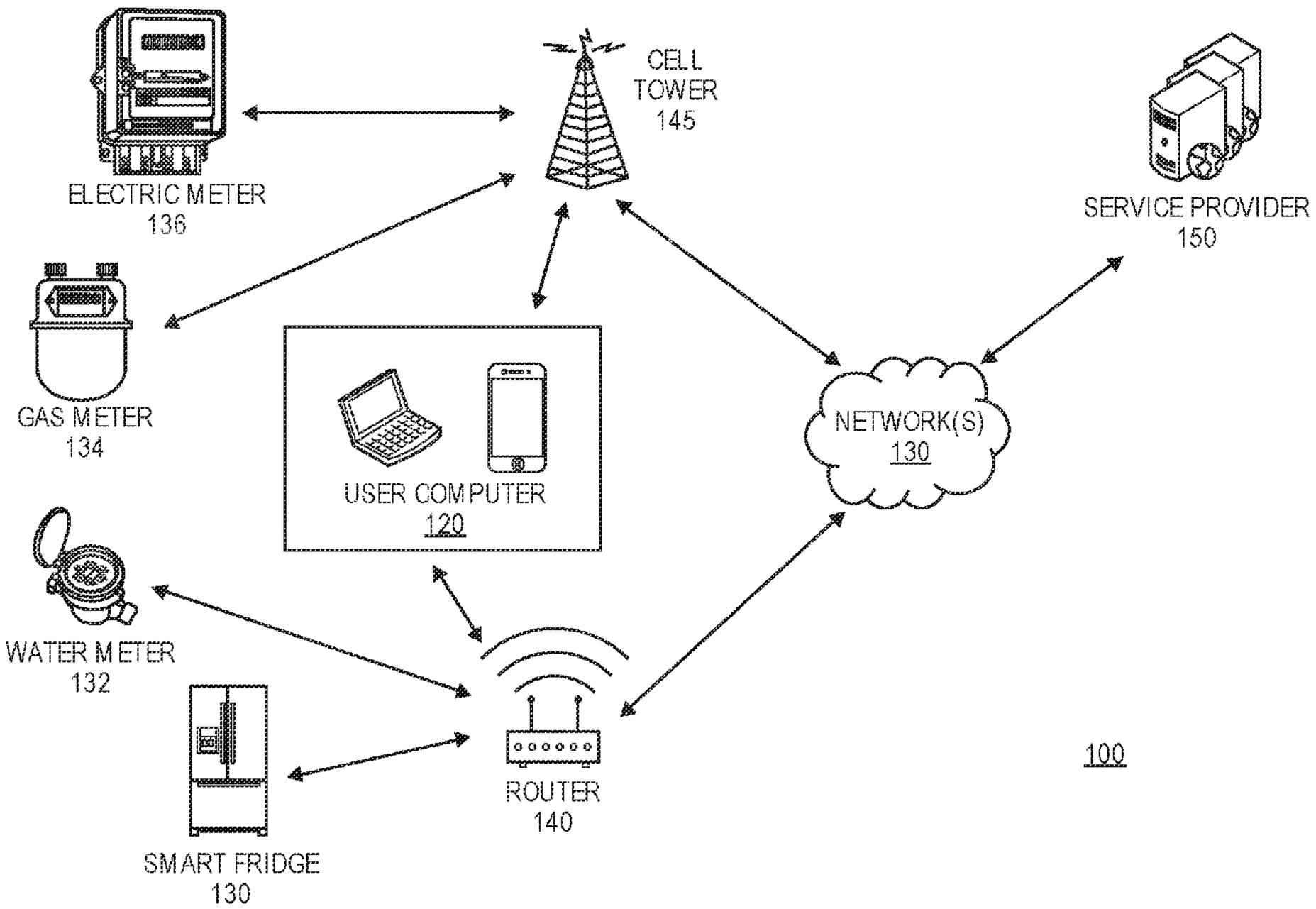
(51) **Int. Cl.**

G06Q 20/32	(2006.01)
H04L 9/40	(2006.01)
H04W 4/70	(2006.01)
G01D 4/00	(2006.01)
G06F 21/44	(2006.01)

(52) **U.S. Cl.**
CPC ***G06Q 20/3226*** (2013.01); ***G01D 4/004*** (2013.01); ***G06F 21/44*** (2013.01); ***H04L 63/102*** (2013.01); ***H04L 63/0876*** (2013.01); ***H04W 4/70*** (2018.02); *H04W 8/26* (2013.01)

(57) **ABSTRACT**

Techniques described herein include a platform and process for provisioning user information onto a machine-to-machine device in order to enable the machine-to-machine device to conduct transactions utilizing the user information. In some embodiments, a user device is used to relay information between a machine-to-machine device and a provisioning service provider computer. In some embodiments, a machine-to-machine device is connected to the provisioning service provider computer via a network connection. Upon receiving a request to provision the machine-to-machine device, the service provider computer may identify the device from a device identifier. The service provider computer may generate an access credential or token for the machine-to-machine device. The access credential, token, and/or one or more policies may be provisioned onto the machine-to-machine device.



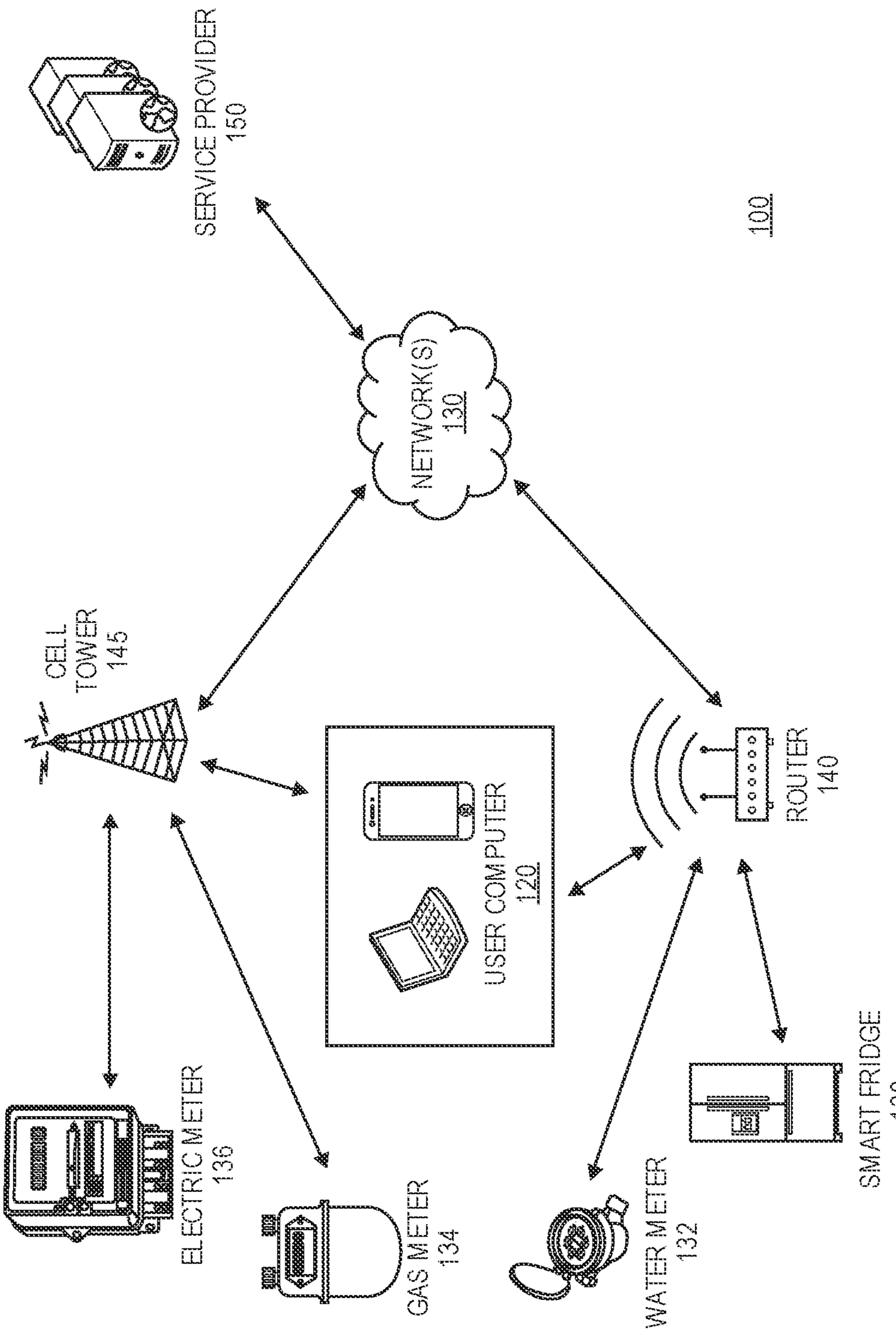

100
SERVICE PROVIDER
150
NETWORK(S)
130
CELL
TOWER
145
USER COMPUTER
120
ROUTER
140
ELECTRIC METER
136
GAS METER
134
WATER METER
132
SMART FRIDGE
130

FIG. 1

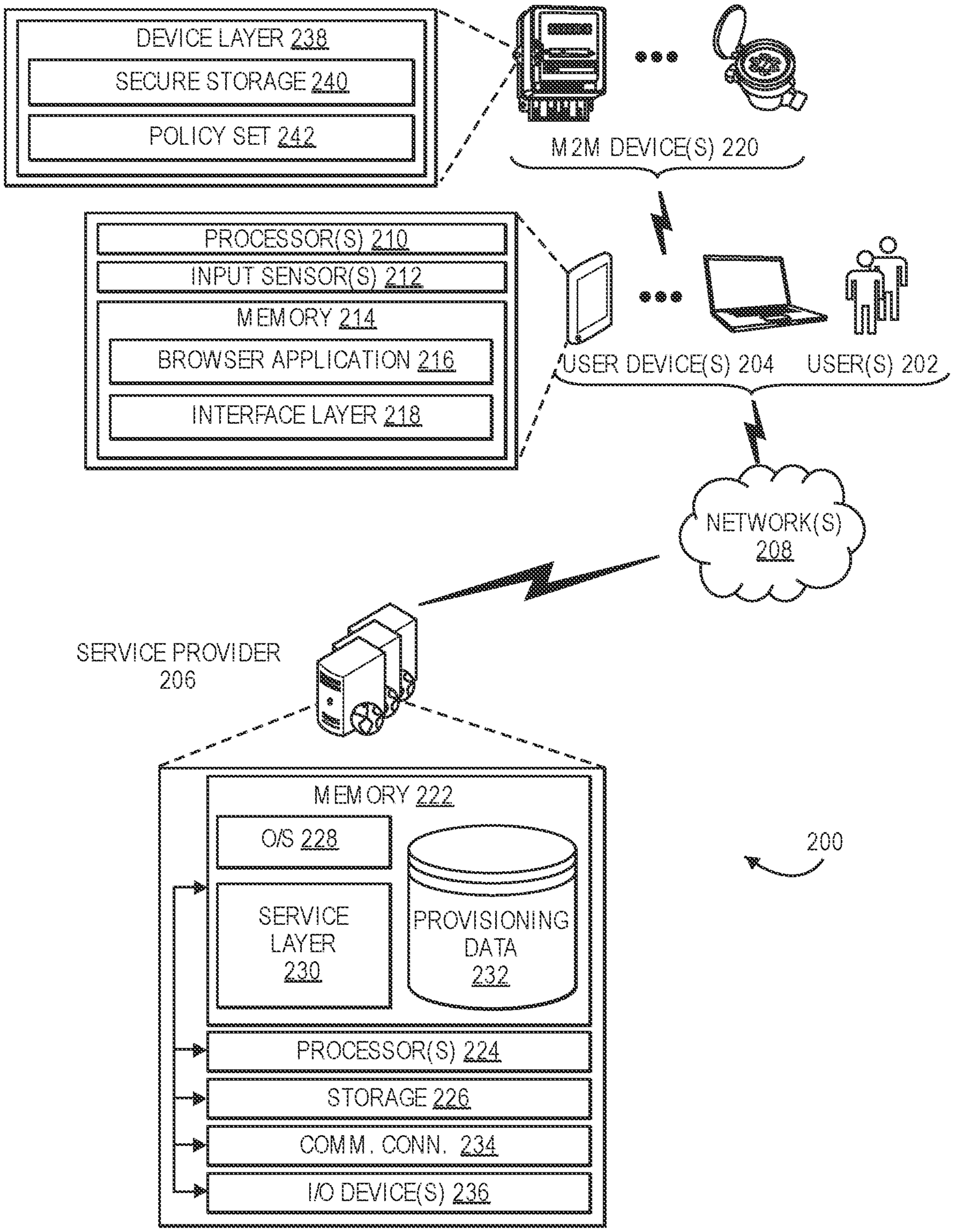

DEVICE LAYER 238
SECURE STORAGE 240
POLICY SET 242
M2M DEVICE(S) 220
PROCESSOR(S) 210
INPUT SENSOR(S) 212
MEMORY 214
BROWSER APPLICATION 216
INTERFACE LAYER 218
USER DEVICE(S) 204
USER(S) 202
NETWORK(S) 208
SERVICE PROVIDER 206
MEMORY 222
O/S 228
SERVICE LAYER 230
PROVISIONING DATA 232
PROCESSOR(S) 224
STORAGE 226
COMM. CONN. 234
I/O DEVICE(S) 236
200

FIG. 2

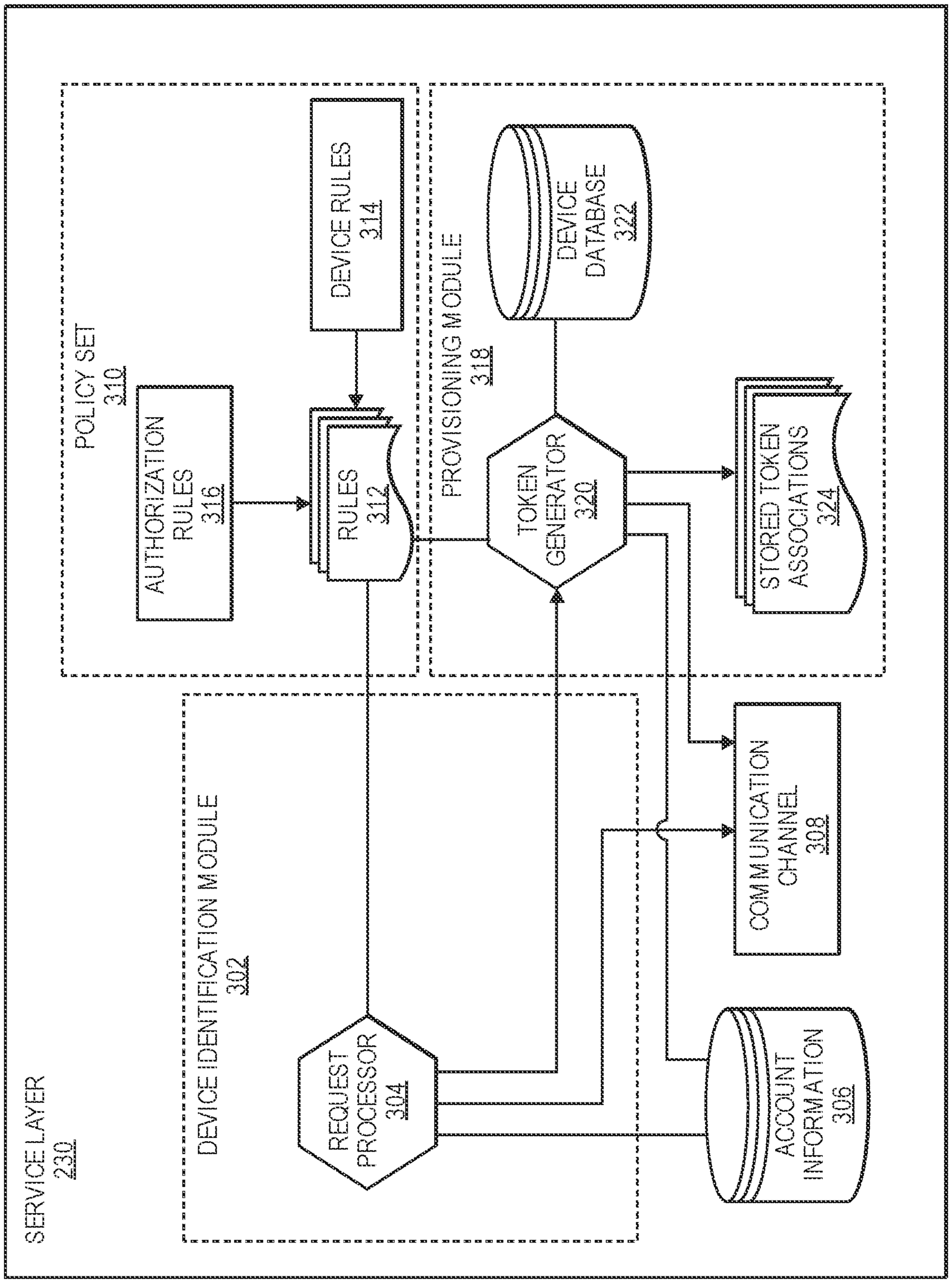

SERVICE LAYER
230
DEVICE IDENTIFICATION MODULE
302
REQUEST PROCESSOR
304
ACCOUNT INFORMATION
306
COMMUNICATION CHANNEL
308
POLICY SET
310
AUTHORIZATION RULES
316
DEVICE RULES
314
RULES
312
PROVISIONING MODULE
318
TOKEN GENERATOR
320
DEVICE DATABASE
322
STORED TOKEN ASSOCIATIONS
324

FIG. 3

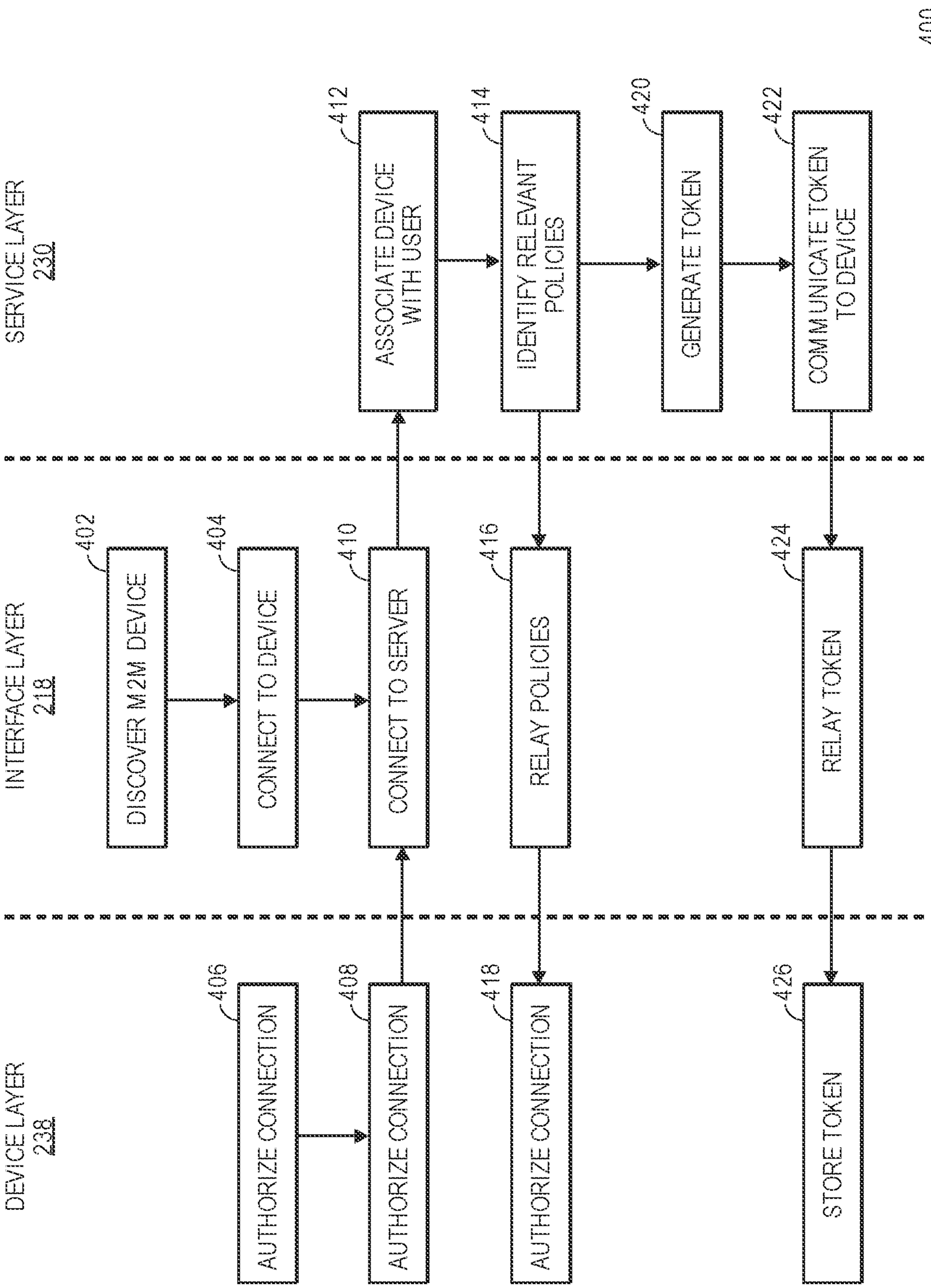

400
SERVICE LAYER
230
INTERFACE LAYER
218
DEVICE LAYER
238
DISCOVER M2M DEVICE
402
CONNECT TO DEVICE
404
AUTHORIZE CONNECTION
406
AUTHORIZE CONNECTION
408
CONNECT TO SERVER
410
RELAY POLICIES
416
AUTHORIZE CONNECTION
418
RELAY TOKEN
424
STORE TOKEN
426
ASSOCIATE DEVICE WITH USER
412
IDENTIFY RELEVANT POLICIES
414
GENERATE TOKEN
420
COMMUNICATE TOKEN TO DEVICE
422

FIG. 4

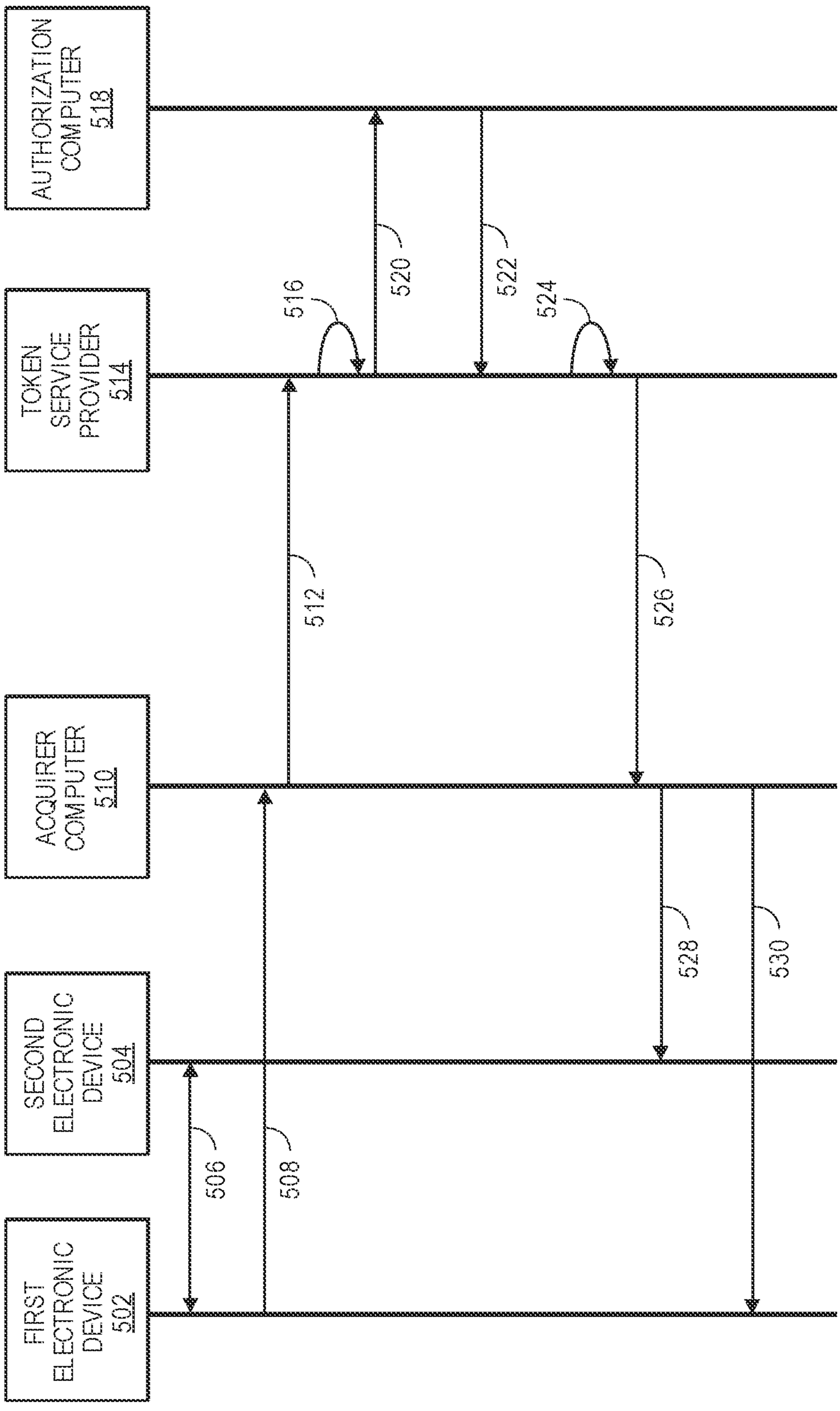

AUTHORIZATION COMPUTER 518
TOKEN SERVICE PROVIDER 514
ACQUIRER COMPUTER 510
SECOND ELECTRONIC DEVICE 504
FIRST ELECTRONIC DEVICE 502
506
508
512
516
520
522
524
526
528
530

FIG. 5

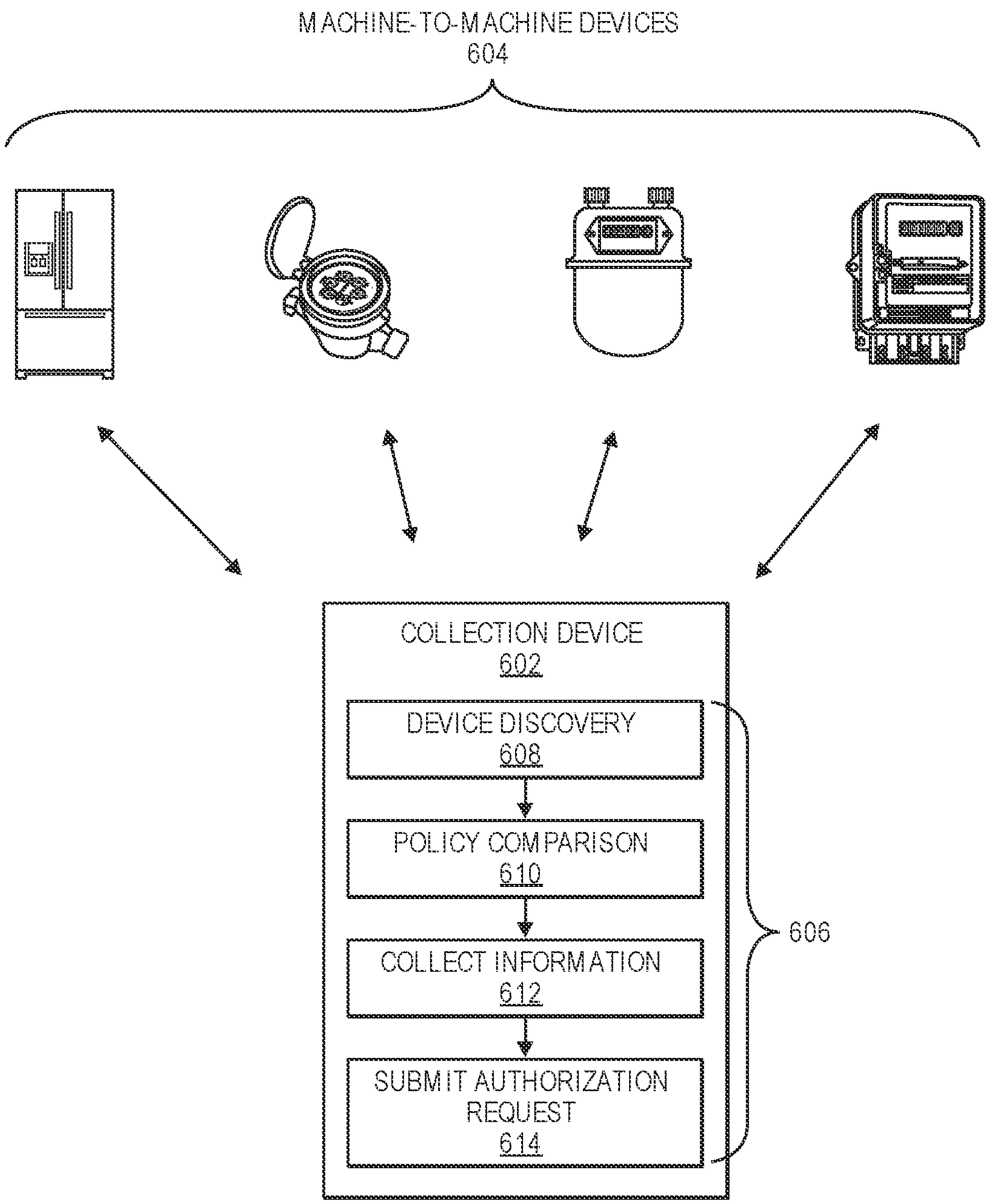

MACHINE-TO-MACHINE DEVICES
604
COLLECTION DEVICE
602
DEVICE DISCOVERY
608
POLICY COMPARISON
610
COLLECT INFORMATION
612
SUBMIT AUTHORIZATION REQUEST
614
606

FIG. 6

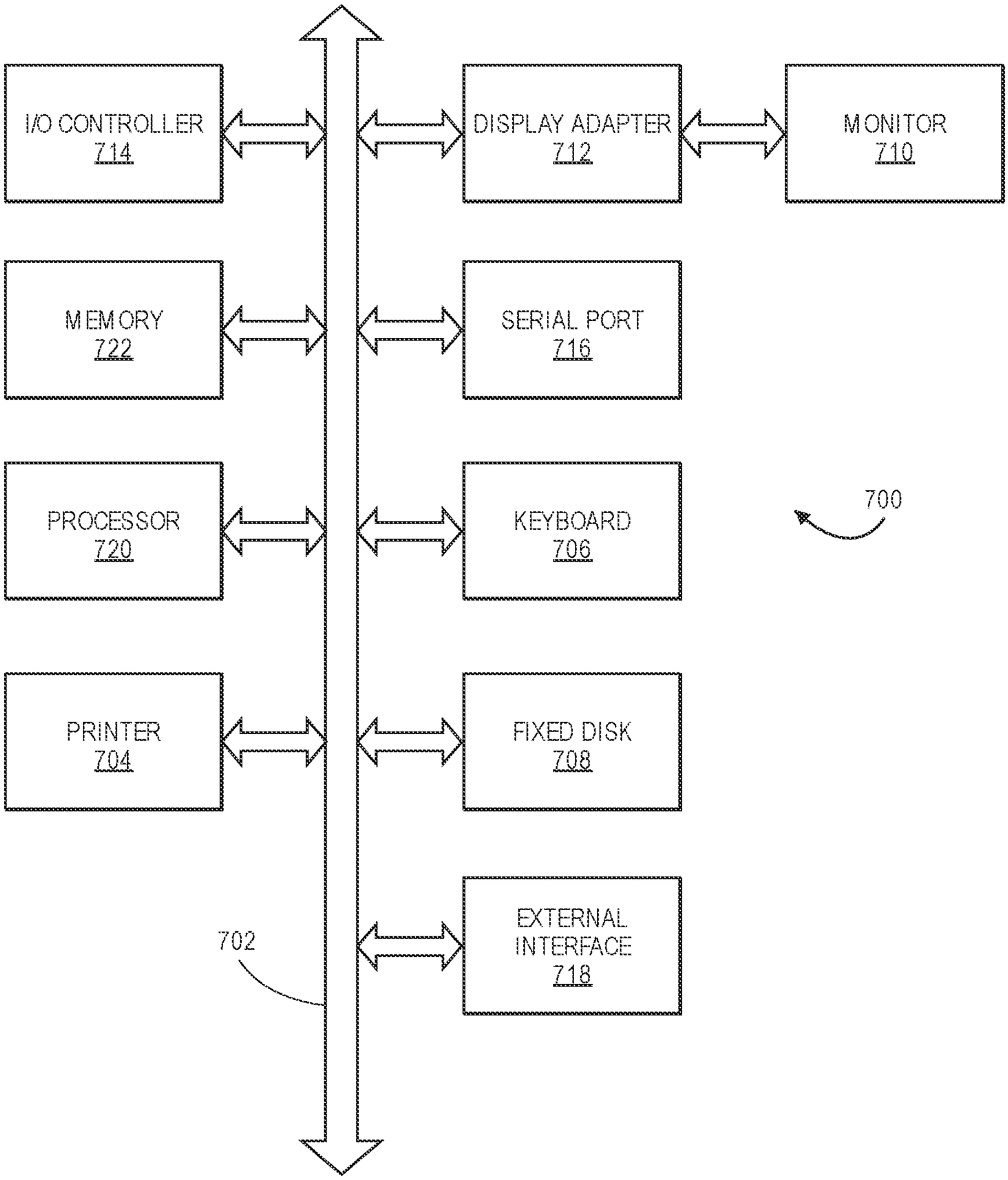

I/O CONTROLLER
714
DISPLAY ADAPTER
712
MONITOR
710
MEMORY
722
SERIAL PORT
716
PROCESSOR
720
KEYBOARD
706
700
PRINTER
704
FIXED DISK
708
EXTERNAL
INTERFACE
718
702

FIG. 7

PROVISIONING PLATFORM FOR MACHINE-TO-MACHINE DEVICES

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application is a continuation of U.S. Pat. Application No. 14/955,716, filed Dec. 1, 2015, which claims the benefit of U.S. Provisional Application No. 62/091,097, filed Dec. 12, 2015, all of which are herein incorporated by reference in their entirety for all purposes.

BACKGROUND

[0002] Households typically include a number of appliances associated with goods and services that are purchased by users on a regular basis. 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. Consumers are often inconvenienced by regular paper bills associated with the goods and services. More convenient ways to provide and/or obtain resources for appliances are needed.

[0003] Embodiments of the present invention address these problems and other problems, individually and collectively.

BRIEF SUMMARY

[0004] Embodiments of the invention can be applied to the "Internet of things" where machines can interact with other machines without human intervention. In embodiments of the invention, machines can be provisioned with access credentials such as payment account numbers or payment tokens associated with payment account numbers. Such access credentials can be used by those machines to obtain (e.g., purchase) resources that are associated with those machines.

[0005] One embodiment of the invention is directed to a method of receiving, at a provisioning server computer, a device identifier associated with a machine-to-machine device and consumer information. The provisioning server computer may then bind the device identifier to the consumer information. The provisioning server computer may then provision the consumer information onto the machine-to-machine device.

[0006] Another embodiment of the invention is directed to a method. The method comprises receiving, at a service provider computer from a user device, a request to provision a first electronic device including a device identifier associated with the first electronic device. The first electronic device is configured to interact with at least one second electronic device independent of human interaction. The method also includes determining, by the service provider computer, based at least in part on the user device, access credentials. The method also includes identifying, by the service provider computer, based at least in part on the access credentials and the device identifier, a policy set relevant to the first electronic device; determining, by the service provider computer, from the access credentials, at least one access credential to be associated with the device identifier, and then providing, by the service provider computer, the at least one access credential to the first electronic device, the at least one access credential to be stored on the first electronic device and used to interact with the at least one second electronic device.

[0007] Another embodiment of the inventon is directed to an electronic device comprising an input sensor configured to detect consumption of a resource, a processor, and a memory. The memory may include instructions that, when executed with the processor, cause the system to: receive, from a service provider computer, an access token and a policy; initiate a transaction in accordance with the policy by: establishing a communication session with an electronic device that manages the resource; requesting access to the resource based at least in part on the consumption of the resource detected by the input sensor; and providing the access token to the electronic device.

[0008] Another embodment of the invention is directed to a method comprising storing, by a first electronic device; an access credential in a secure memory in the first electronic device. The method also includes determining, by the first electronic device and without human intervention, that a resource associated with the first electronic device needs to be obtained. Then, in response to determining that the resource needs to be obtained, the method includes transmitting the access credential to a second electronic device, the second electronic device operated by a resource provider. The resource provider thereafter conducts a transaction using the access credential and then provides the resource to the first electronic device without human intervention.

[0009] Further details regarding embodiments of the invention can be found in the Detailed Description and the Figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] FIG. **1** depicts an example system comprising a number of components in accordance with at least some embodiments;

[0011] FIG. **2** depicts an illustrative example of a system or architecture in which techniques for provisioning a device with user-specific information may be implemented;

[0012] FIG. **3** depicts an illustrative example service layer data flow in accordance with at least some embodiments;

[0013] FIG. **4** depicts a flow diagram illustrating an example technique for provisioning a device with relevant information in accordance with at least some embodiments;

[0014] FIG. **5** depicts a flow diagram illustrating a payment processing technique in accordance with at least some embodiments;

[0015] FIG. **6** depicts the use of a collection device to interact with a provisioned machine-to-machine device in accordance with at least some embodiments; and

[0016] FIG. **7** depicts aspects of elements that may be present in a computer device and/or system configured to implement a method and/or process in accordance with some embodiments of the present invention.

DETAILED DESCRIPTION

[0017] 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 sim-

plified in order not to obscure the embodiment being described.

[0018] Techniques described herein include a system and platform for provisioning consumer information onto a machine-to-machine device so that it may provide consumer information upon request. Also described is a platform in which transactions may be performed automatically by a machine-to-machine device using provisioned consumer information. Prior to discussing specific embodiments of the invention, some terms may be described in detail.

[0019] A "service provider computer" may be a computer that is associated with a service provider. The service provider may provide any suitable service. For example, the service provider may be a merchant, a utility company, a payment processing network, a wallet provider, a merchant, an authentication cloud, an acquirer, or an issuer.

[0020] A "user device" may be a device that is operated by a user. Examples of user devices may include a mobile phone, a smart phone, a personal digital assistant (PDA), a laptop computer, a desktop computer, a server computer, a vehicle such as an automobile, a thin-client device, a tablet PC, etc. Additionally, user devices may be any type of wearable technology device, such as a watch, earpiece, glasses, etc. The user device may include one or more processors capable of processing user input. The user device may also include one or more input sensors for receiving user input. As is known in the art, there are a variety of input sensors capable of detecting user input, such as accelerometers, cameras, microphones, etc. The user input obtained by the input sensors may be from a variety of data input types, including, but not limited to, audio data, visual data, or biometric data. The user device may comprise any electronic device that may be operated by a user, which may also provide remote communication capabilities to a network. Examples of remote communication capabilities include using a mobile phone (wireless) network, wireless data network (e.g., 3G, 4G or similar networks), Wi-Fi, Wi-Max, or any other communication medium that may provide access to a network such as the Internet or a private network.

[0021] 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 or instructions on a device to direct the device's actions. In some embodiments, a device may be provisioned with payment information associated with a user of the device. The payment information may enable the device to execute transactions on the user's behalf without active input from the user.

[0022] 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.

[0023] 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.

[0024] "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.

[0025] "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).

[0026] A "policy 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, conditions upon which those actions are to be performed. In some embodiments, a policy set may include conditional statements, such as "if x_condition occurs, then perform y_action." In some embodiments, a policy set may include a list of transactions that are allowed for a particular electronic device or payment instrument. For example, a service provider may identify, based on a device identifier, a type of device that the policy set is related to. The service provider may then create a custom policy set for that device based on the device's type. For example, upon determining that a device is a water meter, the service provider may create a policy set for the water meter that only allows it to conduct transactions related to water usage. In this example, the policy set may be stored at the service provider in relation to the water meter (or a payment instrument associated with the water meter) and at least a portion of the policy set may be provisioned onto the water meter.

[0027] 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 machine-to-machine device.

[0028] A "machine-to-machine device" may be any suitable electronic device capable of communicating with, and/or interacting with other devices. A machine-to-machine device may have a primary function that is unrelated to communicating with other electronic devices. For example, a machine-to-machine 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 machine-to-machine 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 machine-to-machine device. Examples of machine-to-machine devices may include gas and electric meters, refrigerators, lamps, thermostats, printers, automobiles, fire alarms, home medical devices, home alarms, motorcycles, boats, televisions, etc.

[0029] A "payment instrument" may be any device or data used for making payments. The payment instrument may be intangible (e.g., a software module or software application) or it may be a physical object. As examples of physical objects, the payment instrument may comprise a substrate such as a paper or plastic card, and information that is printed, embossed, encoded, or otherwise included at or near a surface of an object. A physical object may also be a hardware object, which may include circuitry (e.g., permanent voltage values). An intangible payment instrument may relate to non-permanent data stored in the memory of a hardware device. A payment instrument may be associated with a value such as a monetary value, a discount, or store credit, and a payment instrument may be associated with an entity such as a bank, a merchant, a payment processing network, or a person. A payment instrument may be used to make a payment transaction.

[0030] A "token" may include an identifier for a payment account that is a substitute for an account identifier, such as a 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. 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 policy set.

[0031] In some embodiments, a set of payment tokens may be generated based upon a single user account. This might be useful if all payments made using those tokens are to be tied to and paid from the same account. For example, a user may have a credit card account number. Separate tokens (e.g., account number substitutes) may be generated for the different devices in the user's home. For instance, if the user has a washing machine, refrigerator, and a thermostat, then three different tokens may be generated and tied to the single credit card number. When transactions are conducted by these devices, all of the charges may be made to the single credit card account number.

[0032] 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.

[0033] 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.

[0034] 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.

[0035] In at least some embodiments of the invention, a user device may be utilized to detect local machine-to-machine devices. For example, the user device may be configured to perform a device discovery action that identifies all communicatively enabled electronic devices within range of the user device. By way of illustration, a user device may detect all electronic devices that are connected to WiFi within range of the user device. Once detected, the user device may receive a selection of at least one of the machine-to-machine devices from a user of the user device. In some embodiments of the disclosure, the user device may establish a connection with the selected machine-to-machine device and receive information related to the machine-to-machine device. In some embodiments, an additional step of authenticating that a user owns the machine-to-machine device may be required by the machine-to-machine device in order to establish a connection. For

example, the user may be required to enter a password for the machine-to-machine device or press a button located on the machine-to-machine device. Information related to the machine-to-machine device may be presented by the user device within a graphical user interface executed from the user device. The user device may also establish a connection with a service provider computer that maintains and executes provisioning activities. In some embodiments, upon selection of the machine-to-machine device by the user, the service provider computer may send consumer information to the user device, which may subsequently be relayed by the user device to the machine-to-machine device. In this way, the consumer information may be provisioned onto the machine-to-machine device. The consumer information may include an access credential, consumer identifier, and/or policy set information.

[0036] In at least some embodiments, a user may connect to a service provider computer without first connecting to a machine-to-machine device. The user may provide, via the graphical user interface executed on the user device, a device identifier, such as a device name or device location (e.g., an Internet Protocol address), to the service provider computer. In some embodiments, the user may also provide consumer information (such as payment information) to be provisioned onto the device. In some embodiments, the consumer information may be stored at the service provider computer in relation to an account associated with the user. Once a device identifier has been provided to the service provider computer, the service provider computer may locate the device using one or more network connections and provision the device. In some cases, the user may also provide authentication information for the machine-to-machine device to the service provider. For example, the user may provide the service provider computer with a password to access the machine-to-machine device.

[0037] Once a machine-to-machine device has been provisioned with consumer information, the machine-to-machine device may perform one or more transactions using the consumer information. For example, an electronic device may send a request to the machine-to-machine device for some piece of consumer data. The machine-to-machine device may then consult a policy set regarding distribution of the piece of consumer data. If the distribution of the consumer data is identified by the policy set as being allowed, then the machine-to-machine device may respond to the received request with the consumer information. In another example, the machine-to-machine device may advertise the identity of the consumer as the machine-to-machine device's owner.

[0038] FIG. **1** depicts an example system **100** comprising a number of components in accordance with at least some embodiments. A user device **120**, a service provider computer **150**, and one or more machine-to-machine devices (e.g., smart refrigerator **130**, water meter **132**, gas meter **134**, and electric meter **136**) may all be in direct or indirect communication with one another via a network connection **130**, a wireless router **140**, a cell tower **145**, or any other suitable means of communication.

[0039] As noted above, a machine-to-machine device may be any device capable of communicating with, and/or interacting with other devices. Each machine-to-machine device may be configured to perform one or more functions unrelated to the device's ability to interact. For example, the smart refrigerator **130** (one example of the M2M or machine-to-machine device) may comprise both refrigeration and computing capabilities. Although the smart refrigerator **130** is primarily utilized as a means of storing and refrigerating food, it has secondary functions that allow it to communicate with other devices, making it a machine-to-machine device. The machine-to-machine device may include a device identifier, which may be provided by a manufacturer of the machine-to-machine device. The device identifier may serve as a communication address for the machine-to-machine device, and it may be a secure device identifier based on a trusted hardware root of trust (so that integrity/confidentiality can be protected). In some embodiments, the manufacturer may be a trusted issuer of confidentially protected device identifiers.

[0040] The machine-to-machine device 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.

[0041] Information provisioned by the service provider computer **150** onto the machine-to-machine device may be stored in the secure memory. The machine-to-machine device 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. The machine-to-machine device may also store instructions for communicating with other devices and/or instructions for initiating a payment transaction.

[0042] In some embodiments, the machine-to-machine device may be able to communicate wirelessly with the wireless router **140**, the user device **120**, and/or the cell tower **145** (e.g., via Wifi, Bluetooth (classic and BLE or Bluetooth Low Energy), IR, GSM, etc.). Also, the machine-to-machine device may be able to access the Internet via the wireless router **140**, the user device **120**, and/or the cell tower **145** in order to communicate with the service provider computer **150**. For example, in the absence of direct connectivity (e.g., WWAN, GSM), the machine-to-machine device may connect with local devices (e.g., wireless router **140**, user device **120** which can act as a hotspot, etc.) and rely on the devices for Internet connectivity and communication. Accordingly, the machine-to-machine device may be remotely accessible by other devices, and further it may include a user interface for management purposes (such as card activation and provisioning of information).

[0043] In some embodiments, the communication technology used by the machine-to-machine device may depend on the type of power source used by the machine-to-machine device. For example, if the machine-to-machine 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 machine-to-machine 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] In some embodiments, the machine-to-machine device may instead be any other device that provides a household function. As noted above, FIG. **1** includes several devices such as a smart refrigerator **130**, a water meter **132**, a gas meter **134**, and an electric meter **136**. However, further examples of a household device include a television, lamp, fire alarm, home medical device, home alarm, washer/drier, garage door, car, and any other suitable device.

[0045] The service provider computer **150** may be configured to provision information onto the machine-to-machine device. In some embodiments, the information being provisioned onto the machine-to-machine device by the service provider computer **150** may be payment information. In some embodiments, the service provider computer **150** may be associated with an issuer of a payment instrument, a payment processing network associated with the payment instrument, a trusted third party, a digital wallet provider, a token server computer, and/or any other suitable entity.

[0046] FIG. **2** depicts an illustrative example of a system or architecture **200** in which techniques for provisioning a device with user-specific information may be implemented. In architecture **200**, one or more consumers and/or users **202** may utilize user devices **204**. In some examples, the user devices **204** may be in communication with a service provider **206** via the network(s) **208**, or via other network connections.

[0047] Each user device **204** may include one or more processors **210** capable of processing user input. The user device **204** may also include one or more input sensors **212** for receiving user input. As is known in the art, there are a variety of input sensors **212** capable of detecting user input, such as accelerometers, cameras, microphones, etc. The user input obtained by the input sensors may be from a variety of data input types, including, but not limited to, audio data, visual data, or biometric data. Embodiments of the application on the user device **204** may be stored and executed from its memory **214**.

[0048] Turning to the contents of the memory **214** in more detail, the memory **214** may include a browser application **216**. The memory **214** may also include an interface layer **218** that is capable of enabling user interaction with the service provider and/or a machine-to-machine (M2M) device **220**. Although sample architecture **200** depicts an interface layer **218** as being included in the contents of the memory **214** of the user device **204**, some embodiments may not include an interface layer **218** in memory **214** of the user device **204**. In those embodiments in which the interface layer **218** is not included in memory **214**, input received by the input sensors **212** may instead be processed by the service provider **206**. This will be described in detail below.

[0049] In some embodiments, the interface layer **218** may be configured to enable user interaction with the service provider **206** and/or one or more machine-to-machine devices **220**. For example, the interface layer **218** may be configured to allow a user to initiate a device discover process. In this process, the user device **204** may identify a number of machine-to-machine devices **220** within its vicinity. A number of device discovery techniques are known in the art for performing such a device discovery. Once the user device **204** has identified one or more machine-to-machine devices **220**, the user may be given the ability to interact with the discovered devices. In some embodiments, the user may be required to authenticate that he or she has physical access to the device prior to being given the ability to interact with the machine-to-machine devices **220**. For example, the user may be required to press a button on the device, input a password, or perform any other suitable authentication technique. In some embodiments, the interface layer **218** may allow the user device **204** to communicate with both the service provider **206** and the machine-to-machine devices **220** simultaneously. In some embodiments, the service provider may provision the machine-to-machine devices **220** with information using the connection established between the machine-to-machine devices **220** and the user device **204** and the connection established between the user device **204** and the service provider **206**. In some embodiments, the interface layer **218** may allow a user to provision at least some information to the machine-to-machine devices **220** directly.

[0050] In some examples, the network(s) **208** 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. While the illustrated example represents the users **202** accessing the service provider **206** via browser application **216** over the network(s) **208**, the described techniques may equally apply in instances where the users **202** interact with a service provider **206** via the user device **204** over a landline phone, via a kiosk, or in any other manner. It is also noted that the described techniques may apply in other client/server arrangements (e.g., set-top boxes, etc.), as well as in non-client/server arrangements (e.g., locally stored applications, peer to-peer systems, etc.).

[0051] As described briefly above, the browser application **216** may allow the users **202** to interact with a service provider computer **206**, such as to store, access, and/or manage data, develop and/or deploy computer applications, and/or interact with web content. The one or more service provider computers **206**, perhaps arranged in a cluster of servers or as a server farm, may be configured to host a website (or combination of websites) viewable via the user device **204** or a web browser accessible by a user device **204** via the browser application **216**. Although depicted in memory of the user device **204** in this example, in some embodiments the browser application **216** may be hosted at a server. For example, the user device **204** may be a thin client device capable of accessing a browser application **216** remotely. The browser application **216** may be capable of handling requests from many users **202** and serving, in response, various user interfaces that can be rendered at the user device **204** such as, but not limited to, a web site. The browser application **216** may be any type of application or interface that supports user interaction with a website, including those with user interaction, such as social networking sites, electronic retailers, informational sites, blog sites, search engine sites, news and entertainment sites, and so forth. As discussed above, the described techniques can similarly be implemented outside of the browser application **216**, such as with other applications running on the user device **204**. In some embodiments, the browser application **216** may be the interface layer **218**.

[0052] In one illustrative configuration, the service provider computer **206** may include at least one memory **222** and one or more processing units (or processor(s)) **222**. The processor(s) **222** may be implemented as appropriate in hardware, computer-executable instructions, firmware or combinations thereof. Computer-executable instructions or

firmware implementations of the processor(s) **222** may include computer-executable or machine executable instructions written in any suitable programming language to perform the various functions described.

[0053] The memory **222** may store program instructions that are loadable and executable on the processor(s) **222**, as well as data generated during the execution of these programs. Depending on the configuration and type of service provider computer **206**, the memory **222** may be volatile (such as random access memory (RAM)) and/or non-volatile (such as read-only memory (ROM), flash memory, etc.). The service provider computer **206** may also include additional storage **226**, 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 computing devices. In some implementations, the memory **222** may include multiple different types of memory, such as static random access memory (SRAM), dynamic random access memory (DRAM) or ROM. Turning to the contents of the memory **222** in more detail, the memory **222** may include an operating system **228** and one or more application programs or services for implementing the features disclosed herein including at least a module for generating payment tokens and/or provisioning information (e.g., payment tokens and payment rules) onto a machine-to-machine device **220** (service layer **230**). The memory **222** may also include provisioning data **232**, which provides provisioning rules for each device as well as token information. In some embodiments, the provisioning data **232** may be stored in a database.

[0054] The memory **222** and the additional storage **226**, both removable and non-removable, are examples of computer-readable storage media. For example, computer-readable storage media may include volatile or non-volatile, removable or non-removable media implemented in any method or technology for storage of information such as computer-readable instructions, data structures, program modules or other data. As used herein, modules may refer to programming modules executed by computing systems (e.g., processors) that are part of the user device **204** or the service provider **206**. The service provider computer **206** may also contain communications connection(s) **234** that allow the service provider computer **206** to communicate with a stored database, another computing device or server, user terminals, and/or other devices on the network(s) **208**. The service provider computer **206** may also include input/output (I/O) device(s) and/or ports **236**, 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.

[0055] Turning to the contents of the memory **222** in more detail, the memory **222** may include an operating system **228**, a database containing provisioning data **232** and the one or more application programs or services for implementing the features disclosed herein, including a service layer **230**.

[0056] In some embodiments, the service layer **230** may be configured to receive data from the interface layer **218** and provision the machine-to-machine device **220**. In a first illustrative example, a user **202** may send, via the user device **204** and a connection over network **208**, an instruction to the service layer **230** to associate a particular machine-to-machine device **220** with the user. In this example, the user may provide a device identifier associated with the machine-to-machine device **220** to the service layer **230**. The user may also provide an indication of a payment instrument with which to associate the machine-to-machine device **220**. In this example, the service layer **230** may utilize network connection **208** to identify a machine-to-machine device **220** matching the device identifier. Once identified, the service layer **230** may provision the device with information related to the user or the user's account with the service provider. In a second illustrative example, the user **202** may connect to, via a user device **204** and a connection over network **208**, the machine-to-machine device **220** and the service layer **230** simultaneously. In this example, the service layer **230** may provision the machine-to-machine device **220** with information using the connection between the service provider and the user device and the connection between the user device and the machine-to-machine device **220**.

[0057] Provisioning data **230** may be predetermined or it may be dynamically generated. For example, the service provider computer **206** may generate a payment token upon receiving a request to provision a particular device. In this example, the generated token may be stored at the service provider in provisioning data **230** as well as being provisioned to the machine-to-machine device **220**. In addition, a rule set may be generated that is specific to a user and a device. For example, the user may elect a particular brand of dish detergent that he or she prefers. In this example, the user may also elect to provision a smart dishwasher. The service provider may then generate a payment token for the dishwasher to use that is associated with a payment device owned by the user, as well as a set of rules to be associated with the payment token. The rules may indicate that the payment token may only be used to purchase dish detergent, and may even indicate that the payment token may only be used to purchase the specified brand of dish detergent.

[0058] A machine-to-machine device **220** may be any device capable of communicating with, and/or interacting with other devices, but is configured to perform a primary function unrelated to communicating with other devices. In some embodiments, the machine-to-machine device **220** may be a device used to monitor resource consumption. For example, the machine-to-machine device **220** may include a number of input sensors capable of detecting an amount of resource being consumed. By way of illustration, the machine-to-machine device **220** may be a water meter, gas meter, electricity meter, or other utility monitoring device. In some embodiments, the machine-to-machine device **220** may be a device configured to dispense a product or perform a service. For example, the machine-to-machine device **220** may be a vending machine or a clothing washing machine.

[0059] A machine-to-machine device **220** may include memory and one or more processors for storing and executing programmatic instructions. The machine-to-machine device **220** may include a device layer **238** configured to enable interaction between the service layer **230** of the service provider **206** and the programmatic instructions stored on the machine-to-machine device **220**. The device layer **238** 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 machine-

to-machine device **220** may also include a secure storage **240** (e.g., secure key storage) and one or more policy sets **242**. Policy set **242** may include instructions for communicating with other devices, rules indicating what transactions are allowed, instructions for initiating a payment transaction and/or any other suitable information. The policy set may also include a set of conditional instructions for determining an action to be taken by the machine-to-machine device **220** and under what conditions the action should be taken. By way of illustrative example, a machine-to-machine device **220** may be provisioned with payment token information, a policy restricting use of the provided payment token, and a policy conditioning a payment upon an event. In this example, the machine-to-machine device **220** would, upon detection of the event, execute a payment transaction in accordance with the restrictive use policy.

[0060] FIG. **3** depicts an illustrative example service layer data flow in accordance with at least some embodiments. In FIG. **3**, service layer **230** is depicted as being an example service layer **230** of FIG. **2**. Service layer **230** may include a device identification module **302** configured to identify a machine-to-machine device to be provisioned and establish a communication session with the device. In the device identification module **302**, a request processor **304** may receive a request from a user device to provision a machine-to-machine device. The request processor **304** may have access to account information database **306**. Account information database **306** may include various user information related to a user account. For example, the account information database **306** may include a user's demographic information, payment information, device information, or any other suitable user-related information.

[0061] Device identification module **302** may also establish a communication session with a machine-to-machine device via one or more communication channels **308**. In some embodiments, the user device may be in direct communication with the machine-to-machine device to be provisioned. The service provider computer may identify the machine-to-machine device and may establish a communication session with the machine-to-machine device via the user device. In some embodiments, the service provider computer may receive a device identifier, such as a device name or device location (e.g., an Internet Protocol address) from the user device. The service provider may identify the machine-to-machine device on a network based at least in part on the provided device identifier. In some embodiments, the service provider computer may ascertain the type of machine-to-machine device upon, or prior to, establishing a connection with the device. For example, a service provider may determine that the machine-to-machine device is a water meter based on the device identifier supplied to it.

[0062] In accordance with at least some embodiments, the service layer **230** may include a policy set **310**. Policy set **310** may include rules **312** that comprise at least one or more of device rules **314** and authorization rules **316**. Device rules **314** may include rules related to transactions that are authorized for a particular device. For example, a device rule related to a water meter may indicate that the device is only able to perform transactions related to water usage. In another example, a device rule associated with a smart refrigerator may indicate that the refrigerator is only able to perform transactions related to acquisition of food. In some embodiments, the device rules **314** may include an indication of what electronic devices and/or merchants that device is able to interact with. In some embodiments, the device rules may be rules that are provisioned onto a machine-to-machine device itself.

[0063] Authorization rules **316** may include indications of what is authorized for a particular device or payment instrument. In some cases, the authorization rules may be based on user indicated preferences. For example, the user may create an authorization rule to associate the use of a particular payment instrument with a machine-to-machine device. In this example, even if the device is provisioned with multiple tokens associated with multiple payment instruments, only a transaction associated with the particular payment instrument will be authorized. The authorization rules may also include rules related to authorization of transactions. For example, the authorization rules may indicate that a payment for water usage made by a water meter should only be authorized once every two months. In this example, if the service provider computer receives a request to complete a transaction a second time in a two-month period, the service provider may decline the request according to the authorization rules **316**. In some embodiments, the authorization rules **316** may include an indication that a particular transaction type (e.g., transactions for more than a threshold value, transactions with a particular vendor, or any other suitable transaction type) must be approved by the user. In this scenario, the user may be contacted via the user device for approval. For example, the service provider computer may send a short messaging service (SMS) message to the user device requesting authorization for the transaction. In this example, the transaction may be authorized upon receiving a response from the user device indicating that the transaction is authorized.

[0064] A service layer **230** may include a provisioning module **318** configured to generate configuration information and send it to the machine-to-machine device to be stored thereon. In some embodiments, the provisioning module **318** may include a token generator **320** configured to generate an access credential to be stored on the machine-to-machine device. In some embodiments, the provisioning module **318** may include a device database **322** for storing device information. In device database **322**, a device identifier provided by a user may be associated with that user. In addition, device database **322** may include a type of device associated with each device identifier. In some embodiments, the device database **322** may include rules for generating a token that is device specific. In some embodiments, a relationship may be stored with regard to a token generated and the machine-to-machine device on which it is provisioned.

[0065] Token generator **320** may generate a token configured to allow access to one or more aspects of a user's account with the service provider. For example, a token may be generated for a particular machine-to-machine device in order to allow it to use payment information in transactions that it performs without exposing the actual payment information to a third party. In this example, the token may be provided to a third party by the machine-to-machine device in response to receiving a request to make a payment. The third party may subsequently present the token to the service provider to gain authorization for the release of funds related to the transaction. The service provider may determine whether the token received from the third party is authentic, whether the transaction is in compliance with policies associated with the originating

machine-to-machine device, whether the funds for a payment instrument associated with the token are sufficient, and/or any other suitable prerequisites for authorization have been met. Token generator **320** may be responsible for the ongoing operation and maintenance of a token vault storing the generated tokens and a mapping between the tokens and account information and/or payment information associated with the tokens. The token generator may be responsible for token generation and issuance, as well as application of security and controls to the generated tokens. The token generator **320** may register a user device that requests a token and provision the generated token onto the user device and/or a machine-to-machine device.

[0066] In some embodiments, multiple tokens may be generated for a single payment instrument. The token generator **320** may access the device database **322** to identify any device specific token generation rules. In some embodiments, a token may be generated such that the source of the token may be ascertained. In other words, a token may be generated for a machine-to-machine device such that the device (or type of device) may be easily identified from the format or characters of the token. By way of illustration, a token created for a water meter device may begin with the characters WAT. This may allow for a service provider to immediately decline a transaction for water usage in which a provided payment token does not begin with the characters WAT. In some embodiments, the payment instrument information may not be ascertainable from the token. For example, the token may be generated based on a random number. The relationship between these tokens and the machine-to-machine device that they are provisioned on may be stored in device database **322**. In some embodiments, the token may include information for a payment instrument that has been encrypted. For example, a token may be generated by encrypting a device identifier and user account number with an encryption key. In some embodiments, the encryption key may be based on the type of machine-to-machine device for which the token is being generated.

[0067] In embodiments of the invention, tokens may also be generated at any suitable interval. For example, in some embodiments, tokens may be generated and provisioned onto machine-to-machine devices only once, for every transaction, or for each set of a predetermined number of transactions. In some embodiments, a cryptogram may be accompany each token when a payment transaction is attempted by a machine-to-machine device that stores the token. The cryptogram may be generated by an encryption key (e.g., a limited use key) that is stored on the machine-to-machine device with the token.

[0068] The provisioning module **318** may be configured to provide the generated token and one or more rules **312** to the machine-to-machine device, to be used in future transactions via the communication channel **308**. In some embodiments, the provisioning module **318** may store a relationship between the token and the machine-to-machine device in a separate data store **324**. Subsequently, the service provider may receive a request to authorize a transaction from a third party. The request may include information related to the transaction and the payment token. In some cases, the request may also include the device identifier for the machine-to-machine device that provided the token. In the described scenario, the service provider may check to make sure that the token is associated with the device identifier. Upon determining that the relationship exists, the service provider may determine whether the transaction is in compliance with any rules associated with the device identifier before authorizing the transaction.

[0069] In some cases, a dynamic card verification value (dCVV) can be used. The dCVV may be generated based on a counter that changes after every transaction. For example, a machine-to-machine device and the service provider may independently track the number of transactions performed by the machine-to-machine device. When the machine-to-machine device initiates a transaction, a dCVV may be generated based on the tracked number of transactions. In some embodiments, the dCVV may be generated based on a time at which the transaction is initiated. The rules for generating a dCVV may be provided in a policy set that is provisioned onto the machine-to-machine device.

[0070] FIG. **4** depicts a process flow diagram illustrating an example technique for provisioning a device with relevant information in accordance with at least some embodiments. The process **400** is illustrated as a logical flow diagram, each operation of which represents a sequence of operations that can be implemented in hardware, computer instructions, or a combination thereof. In the context of computer instructions, the operations represent computer-executable instructions stored on one or more computer-readable storage media that, when executed by one or more processors, perform the recited operations. Generally, computer-executable instructions include routines, programs, objects, components, data structures, and the like that perform particular functions or implement particular data types. The order in which the operations are described is not intended to be construed as a limitation, and any number of the described operations can be omitted or combined in any order and/or in parallel to implement this process and any other processes described herein.

[0071] In accordance with one embodiment, the process **400** of FIG. **4** may be performed by at least the one or more computer systems of the interface layer **218**, the service layer **230**, and the device layer **238** shown in 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.

[0072] Process **400** may begin at **402**, when a number of devices are discovered by an interface layer **218** of a user device via a discovery process. In some embodiments, the interface layer **218** may be implemented on one or more of the user computers **120** depicted in FIG. **1**. In this process, multiple machine-to-machine devices having wireless connectivity may be identified as being within the vicinity of the user device. The interface layer **218** may then request a connection to a device layer **238** of a selected machine-to-machine device at **404**. In some embodiments, the user device may connect to a machine-to-machine device using the same wireless capability that it used to discover the device. In some embodiments, a user device may utilize an alternative means of connecting to a machine-to-machine device. For example, the user device may connect to a machine-to-machine device via an infrared connection or it may be connected physically via a cable.

[0073] In some cases, the device layer **238** (which, in some embodiments may be implemented in one or more of the machine-to-machine devices **130**, **132**, **134**, and **136** depicted in FIG. **1**) may require that the user provide addi-

tional assurance that the user is the owner of the selected machine-to-machine device before allowing the connection at **406**. For example, the device layer **238** may require that the user enter a password or press a button physically located on the machine-to-machine device to demonstrate physical possession of the machine-to-machine device. Once the user is confirmed as having authorization to access the machine-to-machine device, the device layer **238** may allow the interface layer **218** of the user device to establish a connection at **408**.

[0074] The interface layer **218** may also establish a connection to the service layer **230** of a service provider computer at **410**. In some embodiments, the service layer **230** may be implemented on the service provider **150** depicted in FIG. **1**. The service layer **230** may subsequently identify the user and the machine-to-machine device to be provisioned in order to register the machine-to-machine device as being associated with the user. The service layer **230** may determine the identity of the user in a number of ways. In one example, the user may be required to log into an account maintained at the service provider computer. The account may include details indicating the user's identity. In another example, the service provider may determine an identity of the user based on receiving, in the connection request, an identifier related to the user device (e.g., an Internet Protocol address, a telephone number, a serial number, etc.). The machine-to-machine device may be identified from a device identifier relayed from the device layer **238** to the service layer **230** via the interface layer **218**. In some cases, the user device may already have been registered with the service provider. The registration information for the device may then be used to identify the user. In other cases, the service provider may utilize a lookup service, such as an Internet Protocol address lookup or caller identification. Once the user's identity and the device identifier have been determined, the service layer may create an association between the two at **412**. For example, the service layer **230** may store information in a database that indicates the device identifier is associated with the user.

[0075] Once the machine-to-machine device has been associated with the user, the service layer **230** may identify one or more policies relevant to the machine-to-machine device at **414**. One or more policies may be configured by a user via interface layer **218**. For example, the user may indicate a maximum purchase amount over a period of time (e.g., one week) for the machine-to-machine device. It may also indicate what types of goods or services may be purchased by the machine-to-machine device. In another example, the user may be notified when certain transactions are made or when one or more transactions involves a purchase exceeding a predetermined threshold. In some embodiments, a policy may only permit the machine-to-machine device to conduct transactions for certain resource types (e.g., digital or physical), for a certain amount, with certain merchants, and/or at certain times. For example, a smart refrigerator may only be allowed to purchase groceries. Further, the smart refrigerator may only be allowed to purchase groceries previously specified by the user, groceries that are currently inside the refrigerator, groceries that are running low, and/or groceries from stores located in a certain region. Some policies may specify when to alert the user about transactions and other events. For example, a message (e.g., email, SMS, phone call, etc.) may be sent to the user device any time the machine-to-machine device makes a purchase or pays a bill. In some embodiments, a transaction may not be allowed to take place unless the user indicates approval of the transaction (e.g., by replying to the message above).

[0076] In some embodiments, the user may only be informed if a transaction is attempted that relates to an amount that exceeds or is below a determined threshold. Additionally, a policy may specify what devices (such as the user device) can access the device layer **238** and change settings/policies on the device layer **238**.

[0077] In some embodiments, a policy may also provide an encryption mechanism. For example, the service provider may maintain an encryption key pairing with respect to a device type. In this example, the service provider may provision the device with one key of the key pairing to be used by the device to encrypt transaction information. Further, access mechanisms and a password may be configured, and policies can be set regarding expired payment information (e.g., how to obtain new payment information).

[0078] In some embodiments, at least some of the policies identified as being relevant at **414** may be provisioned onto the machine-to-machine device. To do this, the policies may be transmitted to the interface layer **218** of the user device and further relayed to the device layer **238** by the user device at **416**. The device layer **238** may subsequently store the received policies in a memory of the machine-to-machine device at **418**. If the machine-to-machine device receives a request to complete a transaction, it may consult the stored policy information to determine if the transaction is authorized.

[0079] In some embodiments, the service provider computer may generate a token or other access credential to be associated with the machine-to-machine device at **420**. In some embodiments, when the service provider issues a token for a primary account number or payment instrument associated with an account, the account holder (user) may be asked to participate in the identification and verification process during token generation. For example, the user may be asked to provide identification information to ensure that the token is being generated for an account rightfully owned by the user. By way of illustration, the user may be asked to log into an account associated with the user by providing a username and password. In some embodiments, the user may already be associated with account information to be used in generating the token. For example, information stored in a user's account, such as payment information or a primary account number, may be used to generate the token. In some embodiments, the user may provide information to the service provider with which to generate a token. For example, the user may provide, via the interface layer **218**, a credit card number to be associated with the generated token. In some embodiments, tokens that are generated by the service layer **230** may be accompanied by a token expiration date. The token expiration date may meet the format of a primary account number expiration date and may be the same date or different date than that of the actual primary account number. In various embodiments, tokens that are generated in response to a token request from the user device are only valid for transactions related to the primary function of the device for which the token has been issued. In some embodiments, the service provider may generate a token assurance level to be provisioned onto a machine-to-machine device with the token. One technique for doing this is described in U.S. Pat. Application number

14/514,290, to Powell et al., which is herein incorporated by reference.

[0080] Once the token or other access credential has been generated, it may be provisioned onto the machine-to-machine device at **422**. To do this, the access credential may be transmitted to the interface layer **218** of the user device and further relayed to the device layer **238** by the user device at **424**. The device layer **238** may subsequently store the received access credential in a memory of the machine-to-machine device at **426**. Once fully provisioned with the access credential and any relevant policies, the machine-to-machine device may initiate, or respond to a request for, a transaction with at least one other electronic device.

[0081] Although the above description provides that the interface layer **218** may be present on a user device separate from the machine-to-machine device, it should be noted that, in at least some embodiments, the interface layer **218** may reside on the machine-to-machine device itself. For example, a machine-to-machine device may include a display and one or more input devices configured to receive user input. In these embodiments, the user may request provisioning of the machine-to-machine device as described in the current specification from the machine-to-machine device.

[0082] In some embodiments, the service provider may receive an indication that the access credentials associated with a user's account have changed or are otherwise not valid. For example, the service provider may determine that the user's payment information has expired. In these cases, the user may be required to provide new payment information. For example, the user may be required to update his or her account with a new credit card number. Upon determining that the payment information has been updated, the service provider may generate a second access credential to be associated with the new payment information. For example, upon receiving updated credit card information, the service provider may generate a second token to be associated with the new credit card information. In some embodiments, the second access credential may be provisioned onto the machine-to-machine device without further user interaction. For example, upon generation of a new access credential to be associated with a machine-to-machine device, the service provider may execute **422** -**426** of the process **400** in order to provision the new access credential onto the machine-to-machine device.

[0083] FIG. **5** depicts a flow diagram illustrating an automated payment process in accordance with some embodiments of the invention. In FIG. **5**, a first electronic device **502**, which may be a machine-to-machine device, determines that a transaction should be conducted with respect to a resource (e.g., that a resource needs to be obtained). This determination may be made without human intervention. For example, the first electronic device may utilize a set of rules that dictate under what circumstances the resource should be obtained. The first electronic device may establish a communication session with a second electronic device **504** owned/operated by a resource manager at **506**. For purposes of illustration, the first electronic device **502** may be a smart refrigerator, while the second electronic device **504** may be a server computer that is operated by a merchant such as a grocery store.

[0084] In a first example, the first electronic device may include a policy that indicates a payment for resource usage should be made on the first of each month. In this example, the first electronic device, upon determining that a date/time condition in the policies has been met, may initiate contact with the second electronic device to request a transaction. In a second example, the first electronic device **502** may establish a communication session with the second electronic device **504** upon detecting the presence of the second electronic device. The first electronic device may communicate, via the communication session, an amount of a resource that it requires. The second electronic device may consult a rate chart and/or an item catalog to determine an appropriate reimbursement for the requested amount of the resource. In some embodiments, the second electronic device may also provide a shipping cost to the first electronic device. If the transaction details (amount of the resource, proposed reimbursement, shipping costs, etc.) are in compliance with policies stored on the first electronic device, then a transaction authorization request may be initiated from either the first electronic device or the second electronic device.

[0085] For purposes of illustration, the first electronic device **502** may be a smart refrigerator, while the second electronic device **504** may be a server computer that is operated by a merchant such as a grocery store. The first electronic device may determine (through internal sensors) that it is low on eggs and milk. Upon this determination, the first electronic device may contact the second electronic device operated by a grocery store. When contacting the grocery store, the first electronic device **502** may provide a payment token to the second electronic device **504**, and the grocery store may conduct the payment transaction as further explained below. After the payment process has concluded, the grocery store may then automatically send the milk and eggs to the household that has the first electronic device. All of this may be performed without any user intervention.

[0086] In some embodiments, the transaction authorization request message may be initiated by the first electronic device **502** by sending the transaction details and payment information to an acquirer computer **508** at **510**. The acquirer computer **508** receives the transaction details and payment information and determines an appropriate payment entity to route an authorization request message to. In some embodiments, the format and/or characters of the payment information may be used to indicate the payment entity. For example, a payment information number beginning with 4012 may be associated with a payment processing network such as Visanet. In some embodiments, the acquirer computer may determine that the payment information is associated with a token. Token information may be maintained by token service provider. A token service provider 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 token service provider may operate one or more computers, as well as the service layer **230** depicted in FIGS. **2** - **4**.

[0087] Once the acquirer computer **510** has determined where an authorization request is to be routed, the acquirer computer may transmit the authorization request message to the appropriate payment entity at **512**. If the payment information comprises a token, then the authorization request message may be routed to a token service provider **514** at **512**. The token service provider may be provided in a transaction processing network. An exemplary transaction processing network may include VisaNet™. Transaction pro-

cessing 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.

[0088] The token service provider **514** may query a token vault (a data store configured to store associations between tokens and actual payment information) to retrieve actual payment account information details. In this way, the token service provider **514** de-tokenizes the payment token to obtain an actual primary account number or PAN at **516**. In some embodiments, the token service provider **514** may perform one or more mathematical calculations to identify actual payment account information from the token, or it may simply retrieve the actual payment account information. The token service provider **514** may then forward the authorization request message, along with the actual payment account information, to the authorization computer **518** operated by the payment entity (which may be an issuer) at **520**. In some embodiments, the authorization request message may also include the token so that the authorization entity is able to associate the token with the authorization request.

[0089] The authorization computer **518** receives the authorization request message at **520** and determines if the transaction should be authorized. For example, the authorization computer may decline the transaction if there is a high likelihood of fraud. In another example, the authorization computer may decline the transaction if the payment account has insufficient funds. Once the authorization computer has decided whether to approve or decline the transaction, an authorization response message may be sent to the token service provider at **522**.

[0090] The token service provider **514**, upon receiving the authorization response message, may re-tokenize the message at **524** by querying the token vault to identify the token from the actual payment account information included in the authorization response message. The token service provider may then remove any actual payment account information out of the response and replace it with the token payment information. The authorization response message comprising the payment token may then be provided to the acquirer computer at **526**.

[0091] The acquirer computer may, upon receiving the response, determine whether the transaction has been approved or declined. In either case, the authorization response message may be provided to the second electronic device at **528** and/or the first electronic device at **530**. If the transaction has been authorized, the first electronic device may complete the transaction with the second electronic device. 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.

[0092] At some later point in time, a clearing and settlement process between the acquirer computer **510** and the authorization computer **518** may occur, and funds may be transferred from the authorization computer to the acquirer computer.

[0093] It should be noted that although the second electronic device is depicted as being a separate device from the acquirer computer, the two devices may be the same device. For example, the first electronic device may contact the acquirer computer directly to request an amount of a resource. Additionally, the token service provider and authorization computer may be maintained by the same entity. For example, both the token service provider and the authorization computer may be maintained and operated by a credit card issuer. In some embodiments, the payment information may not be tokenized (though it might still be encrypted). In these embodiments, one skilled in the art would recognize that figure references **508**, **514**, and **524** are not necessary to the disclosure. Additionally, the acquirer computer may communicate with the authorization computer directly.

[0094] FIG. **6** depicts the use of a collection device to interact with a provisioned machine-to-machine device in accordance with at least some embodiments. In some embodiments, a machine-to-machine device may be connected to a network. Machine-to-machine devices that are connected to a network may contact a resource manager directly in order to conduct a transaction. For example, an electric meter in communication with a server operated by the local utility company may contact the server directly to make a payment for electricity usage in accordance with at least some embodiments. However, if the machine-to-machine device is not connected to a network, then a transaction needs to be conducted in a different manner. One such technique is illustrated by FIG. **6**, in which a collection device **602** may enter the proximity of one or more machine-to-machine devices **604**. The collection device **602** may be any electronic device operated by, or with authority from, a resource manager. For example, the collection device **602** may be a meter reader configured to communicate with an electric meter to collect electricity usage information on behalf of a local utility company. In some embodiments, the collection device may be in communication with a backend server or other electronic device. For example, a collection device may have a connection to a wireless network (e.g., 3G, 4G or similar networks) to a server hosted by the resource manager.

[0095] The collection device **602** may be configured to perform one or more steps of a collection process **606**. In this example, the collection device **602**, upon entering a geographic location or in response to a request by a user of the collection device, may attempt to discover local machine-to-machine devices at **608**. Once discovered, the collection device may initiate a rule comparison. In some embodiments, the collection device **602** may send a discovered machine-to-machine device an indication of a type of transaction to be performed. The machine-to-machine device **604** may then compare the transaction type to a stored policy to determine whether the transaction type is one that the machine-to-machine device is authorized to perform. If the machine-to-machine device **604** is authorized to perform the transaction, then it may transmit a response to the collection device **602**. In some embodiments, the machine-to-machine device **604** may publish a type of transaction that it is authorized to perform. For example, the electric meter mentioned above may publish that it is able to pay for electricity usage. In this example, a meter reader (collection device **602**) may detect the electric meter (machine-to-machine device **604**) and identify that it is capable of performing transactions related to electricity usage. In this example, the meter reader may compare the published transaction

type to a policy stored on the meter reader to determine that a transaction should be performed at **610**.

[0096] Once the machine-to-machine device **604** and the collection device **602** have determined that a transaction is authorized, the two electronic devices may conduct a transaction. This may involve the collection device collecting transaction information from the machine-to-machine device at **612**. The collection device **602** may collect resource information from the machine-to-machine device. For example, the collection device may collect information related to an amount of resource used or an amount of resource needed. Either the collection device **602** or the machine-to-machine device **604** may then calculate an appropriate reimbursement for the resource. If the transaction is in compliance with the policies stored on the machine-to-machine device **604**, then the collection device **602** may collect an access credential or payment information from the machine-to-machine device at **612**. In some embodiments, the collection device **602** may send credential information to the machine-to-machine device **604** to validate that the collection device **602** is authorized to collect the payment information.

[0097] Upon receiving the credential information from the machine-to-machine device, the collection device may contact the service provider or an authorization server to request release of a payment in accordance with the transaction at **614**. (e.g., in a manner similar to or different than the flow in FIG. **5**). The service provider may authorize the payment upon validating the payment information or access credential and ensuring that the transaction is in compliance with policies stored at the service provider. In some embodiments, the collection device **602** may not have communication access to the service provider. The collection device **602** may store the transaction information until it is able to request authorization for the transaction. It should be noted that although the collection device **602** is described as requesting authorization for a transaction, the collection device **602** may provide the transaction information to a server maintained by the resource manager, and the resource manager may contact the service provider to get authorization for the transaction.

[0098] By way of illustration, an example machine-to-machine device may be a refrigerator that is authorized to purchase groceries. In this example, the machine-to-machine device may have stored in memory a grocery list (a list of items that are to be purchased) as well as one or more policies. At least some of the policies may indicate a maximum amount that may be spent on a particular item. In this example, a mobile grocery vendor may enter the vicinity of the refrigerator and, using a collection device, determine that the refrigerator is in need of the one or more items from the grocery list. The refrigerator may provide the grocery list to the collection device and the collection device may consult an item catalog to determine prices for each of the items on the list. The collection device may then provide the determined prices to the refrigerator. In some embodiments, the refrigerator may subsequently determine whether the price for each grocery item involved in the transaction is in compliance with the policies, and remove any grocery item from the transaction that is not. In some embodiments, a policy may indicate a maximum amount to spend on a total order. Upon determining that the transaction is in compliance with the policies, the transaction is completed. The mobile grocery vendor may leave the requested groceries on the doorstep of the house containing the refrigerator. The collection device collects payment information from the refrigerator and sends an authorization request to the service provider to gain access to payment information.

[0099] In some embodiments, a token may be generated for a particular type of machine-to-machine device without having been provided a device identifier. The token may be stored on a user device for future use. For example, a user may request generation of a token related to parking meters. In this example, the service provider computer may generate a token to be stored on the user device that is associated with the user's payment information and will allow parking meters to conduct transactions. The user may subsequently utilize the user device to perform a transaction with a parking meter. For example, the user may utilize the user device to interact with a parking meter and request parking. The user device may then provision the payment token onto the parking meter. In this example, the parking meter may be configured to detect the presence of a vehicle and may continue to toll the provided payment token for as long as the vehicle is present. In another example, the user may elect a timeframe from the parking meter for which to be billed.

[0100] In accordance with at least some embodiments, a machine-to-machine device may maintain a "tab" or balance for a particular user. For example, in a scenario in which a vending machine with wireless capabilities (a machine-to-machine device) is placed outside of network coverage, the vending machine may be configured to collect tokens from one or more user devices in exchange for vended products. In this scenario, the user device may, in response to receiving a request for payment, provide the vending machine with a pre-generated token. The vending machine may check the format and/or content of the provided token in order to assess whether the token is likely to be valid. If the vending machine determines that the token is likely valid, then it may store the token in relation to a balance owed for the user device and dispense a requested good. A collection agent may enter the proximity of the vending machine with a collection device at a subsequent time, at which point the vending machine may provide any stored payment tokens and balances to the collection device. In some embodiments, the collection device may contact the service provider for authorization of the previously conducted transactions upon re-entering network coverage. After transmitting the information to the collection device, the vending machine may continue to maintain the token, but with a zeroed balance, or it may delete the payment token and balance.

[0101] Some machine-to-machine devices may be associated with a single user and some machine-to-machine devices may be associated with multiple users. For example, a machine-to-machine device may include provisioned information related to multiple users that consume a single resource. In this example, the machine-to-machine device may enter into a transaction related to the resource for each user either individually or within a single transaction. By way of illustration, a household may consist of three roommates that each split utility payments equally. In this illustration, the water meter may be provisioned with payment instrument information for each of the three roommates. Upon receiving a request to make a payment for water usage, the water meter may present each of the three payment instruments to each be charged for a third of the water usage. In this illustration, payment instrument infor-

mation for each of the three roommates may be stored on the machine-to-machine device and the service provider computer may store an indication that all three roommates are associated with the water meter.

[0102] Additionally, a machine-to-machine device may be provisioned temporarily. By way of illustration, consider a scenario in which a user rents a vehicle. The vehicle may be provisioned with the user's payment information for the duration of the rental. The rental vehicle may be a machine-to-machine device in that as the rental vehicle passes a toll booth, the vehicle may be configured to interact with an electronic device within the toll booth to pay a fee for using the road. In this scenario, the toll may be charged directly to the user's payment information instead of to the vehicle rental company. Upon the return of the vehicle to the rental company, the provisioned payment information may be removed from the vehicle. This limits risk of nonpayment for the vehicle rental company and prevents the user from paying toll fees that have been marked up by the vehicle rental company.

[0103] In accordance with at least some embodiments, the system, apparatus, methods, processes and/or operations for event processing may be wholly or partially implemented in the form of a set of instructions executed by one or more programmed computer processors such as a central processing unit (CPU) or microprocessor. Such processors may be incorporated in an apparatus, server, client or other computing device operated by, or in communication with, other components of the system. As an example, FIG. **7** depicts aspects of elements that may be present in a computer device and/or system **700** configured to implement a method and/or process in accordance with some embodiments of the present invention. The subsystems shown in FIG. **7** are interconnected via a system bus **702**. Additional subsystems such as a printer **704**, a keyboard **706**, a fixed disk **708**, a monitor **710**, which is coupled to a display adapter **712**. Peripherals and input/output (I/O) devices, which couple to an I/O controller **714**, can be connected to the computer system by any number of means known in the art, such as a serial port **716**. For example, the serial port **716** or an external interface **718** can be utilized to connect the computer device **700** to further devices and/or systems not shown in FIG. **7** including a wide area network such as the Internet, a mouse input device, and/or a scanner. The interconnection via the system bus **702** allows one or more processors **720** to communicate with each subsystem and to control the execution of instructions that may be stored in a system memory **722** and/or the fixed disk **708**, as well as the exchange of information between subsystems. The system memory **722** and/or the fixed disk **708** may embody a tangible computer-readable medium.

[0104] Embodiments of the invention provide for a number of technical advantages. Embodiments of the invention allow for different machines to conduct access transactions (e.g., payment transactions) with other machines without human intervention. Also, because tokens are used instead of real account credentials, the processing between devices is secure.

[0105] It should be understood that the present invention as described above can be implemented in the form of control logic using computer software in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement the present invention using hardware and a combination of hardware and software.

[0106] Any of the software components, processes or functions described in this application may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0107] All references, including publications, patent applications, and patents, cited herein are hereby incorporated by reference to the same extent as if each reference were individually and specifically indicated to be incorporated by reference and/or were set forth in its entirety herein.

[0108] Different arrangements of the components depicted in the drawings or described above, as well as components and steps not shown or described are possible. Similarly, some features and sub-combinations are useful and may be employed without reference to other features and sub-combinations. Embodiments of the invention have been described for illustrative and not restrictive purposes, and alternative embodiments will become apparent to readers of this patent. Accordingly, the present invention is not limited to the embodiments described above or depicted in the drawings, and various embodiments and modifications can be made without departing from the scope of the claims below.

[0109] For example, although the specific examples described above relate to payment, it is understood that other types of transactions can be conducted and that embodiments of the invention are not limited to payment transactions. For example, a first device may seek to access data on a second device, and may request authorization in a similar manner to that described above with respect to payment transactions.

What is claimed is:

1. An electronic device comprising:

an input sensor configured to detect consumption of a resource;

a processor; and

a memory including instructions that, when executed with the processor, cause the system to at least:

receive, from a service provider computer, an access token and a policy;

initiate a transaction in accordance with the policy by:

establishing a communication session with a second electronic device that manages the resource;

requesting access to the resource based at least in part on the consumption of the resource detected by the input sensor; and

providing the access token to the second electronic device.

2. The electronic device of claim **1**, wherein the access token is stored in a secure memory of the electronic device.

3. The electronic device of claim **1**, wherein a primary function of the electronic device is to monitor consumption of the resource.

4. The electronic device of claim **1**, wherein the policy restricts the transaction to a purchase of the resource.

5. The electronic device of claim **1**, wherein the policy indicates at least one condition upon which a transaction is to be initiated.

6. The method of claim **5**, wherein the one condition includes liming the transaction to transactions associated with a type of the electronic device.

7. The method of claim **5**, wherein the one condition includes a data or time condition associated with the transaction.

8. A method comprising;

storing, by a first electronic device; an access credential in a secure memory in the first electronic device;

determining, by the first electronic device and without human intervention, that a resource associated with the first electronic device needs to be obtained;

in response to determining that the resource needs to be obtained, transmitting the access credential to a second electronic device, the second electronic device operated by a resource provider, wherein the resource provider thereafter conducts a transaction using the access credential and then provides the resource to the first electronic device without human intervention.

9. The method of claim **8**, wherein the access credential is a token.

10. The method of claim **8**, wherein the access token is stored in a secure memory of the electronic device.

11. The method of claim **8**, wherein a primary function of the electronic device is to monitor consumption of the resource.

12. The method of claim **8**, further comprising receiving, from a service provider computer, a policy.

13. The method of claim **12**, wherein the policy restricts the transaction to a purchase of the resource.

14. The method of claim **12**, wherein the policy indicates at least one condition upon which a transaction it to be initiated.

15. The method of claim **14**, wherein the one condition includes liming the transaction to transactions associated with a type of the electronic device.

16. The method of claim **14**, wherein the one condition includes a data or time condition associated with the transaction.

17. The method of claim **12**, wherein the service provider computer previously determined the access credential based on a user device associated with the first electronic device.

18. A first electronic device comprising:

a processor; and

a computer readable medium comprising code, executable by the processor, for implementing a method comprising

storing an access credential in a secure memory in the first electronic device;

determining, without human intervention, that a resource associated with the first electronic device needs to be obtained;

in response to determining that the resource needs to be obtained, transmitting the access credential to a second electronic device, the second electronic device operated by a resource provider, wherein the resource provider thereafter conducts a transaction using the access credential and then provides the resource to the first electronic device without human intervention.

* * * * *