

(51) International Patent Classification:
H04L 9/40 (2022.01)

(21) International Application Number:
PCT/US2024/031520

(22) International Filing Date:
30 May 2024 (30.05.2024)

(25) Filing Language:
English

(26) Publication Language:
English

(30) Priority Data:
18/332,079 09 June 2023 (09.06.2023) US

(71) Applicant: MICROSOFT TECHNOLOGY LICENSING, LLC [US/US]; One Microsoft Way, Redmond, Washington 98052-6399 (US).

(72) Inventors: RAY, Mayukh; Microsoft Technology Licensing, LLC, One Microsoft Way, Redmond, Washing-

ton 98052-6399 (US). LOWE, Alistair James; Microsoft Technology Licensing, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US).

(74) Agent: CHATTERJEE, Aaron C. et al.; Microsoft Technology Licensing, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US).

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

(54) Title: DEVICE AUTHORIZATION USING A DIRECTORY SYSTEM

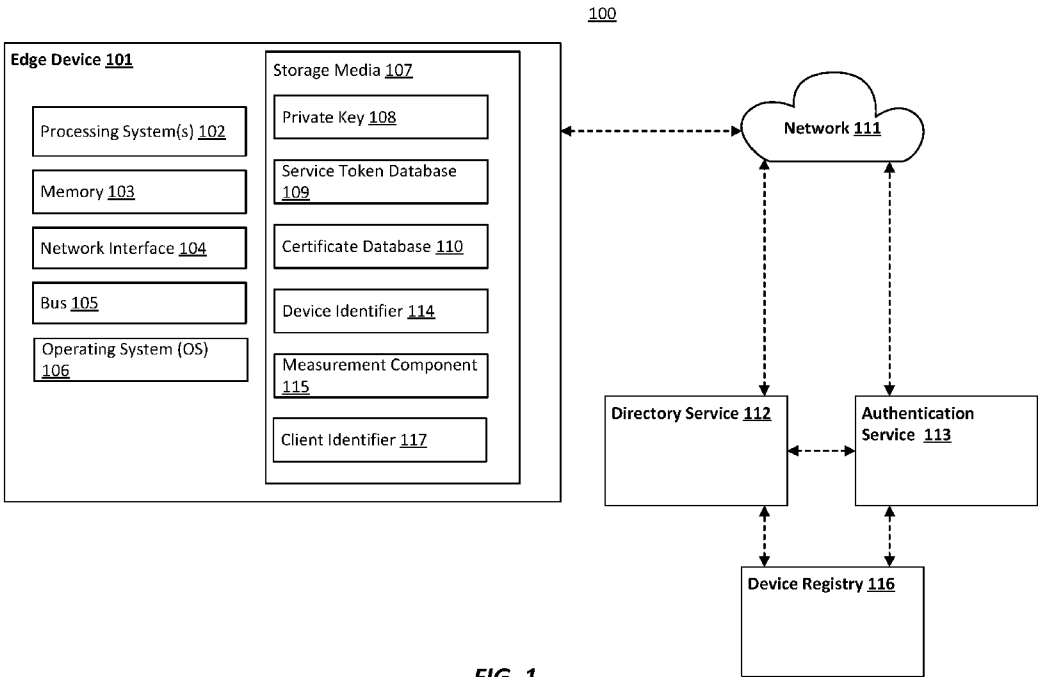


FIG. 1

(57) Abstract: Methods and systems are described which obtain a service token at an edge device. Embodiments obtain a device certificate from an authentication service based on a private key which is associated with a public key. The public key is further associated with a device identifier for the edge device at a directory service. Embodiments send a request for a service token to an authentication service from a directory service based on the private key where the directory service has identified the public key for the edge device. Other embodiments extract the device identifier from the device certificate and send a request for a service token to the directory service, where the request includes the device certificate and the device identifier. Embodiments receive the service token from the directory service and use the service token to access a service.

TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS,
ZA, ZM, ZW.

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

Declarations under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

- *with international search report (Art. 21(3))*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

DEVICE AUTHORIZATION USING A DIRECTORY SYSTEM**BACKGROUND**

[0001] Internet of Things devices have the ability to connect to platforms to access services. These devices can connect to services based on certificates possessed by those devices.

[0002] The subject matter claimed herein is not limited to embodiments that solve any disadvantages or that operate only in environments such as those described above. Rather, this background is only provided to illustrate one example technology area where some embodiments described herein may be practiced.

BRIEF SUMMARY

[0003] In some aspects, the techniques described herein relate to a method for obtaining a service token at an edge device, implemented at a computer system that includes a processor, including: based on a private key at the edge device, obtaining a device certificate from an authentication service, wherein the private key is associated with a public key, the public key being associated with a device identifier for the edge device at a directory service; based on the private key, sending a request for a service token to the authentication service from a directory service, wherein the directory service has identified the public key for the edge device; receiving the service token from the authentication service; and using the service token to access a service.

[0004] In some aspects, the techniques described herein relate to a method for obtaining a service token at an edge device, implemented at a computer system that includes a processor, including: based on a private key at the edge device, obtaining a device certificate from an authentication service, wherein the private key is associated with a public key, the public key being associated with a device identifier for the edge device at a directory service; extracting the device identifier from the device certificate; sending a request for a service token to the directory service, wherein the request includes the device certificate and the device identifier; receiving the service token from the directory service based on the directory service identifying the public key for the edge device; and using the service token to access a service.

[0005] In some aspects, the techniques described herein relate to a computer system including: a processing system; and a computer storage media that stores computer-executable instructions that are executable by the processing system to at least: based on a private key at the edge device, obtain a device certificate from an authentication service, wherein the private key is associated with a public key, the public key being associated with a device identifier for the edge device at a directory service; derive a device identifier from the device certificate; send a request for a service token to the directory service, wherein the request includes the device certificate and the device identifier; receive the service token from the directory service based on the directory service

identifying the public key for the edge device; and use the service token to access a service.

[0006] This summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used as an aid in determining the scope of the claimed subject matter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] In order to describe the manner in which the advantages and features of the systems and methods described herein can be obtained, a more particular description of the embodiments briefly described above will be rendered by reference to specific embodiments thereof which are illustrated in the appended drawings. Understanding that these drawings depict only typical embodiments of the systems and methods described herein, and are not therefore to be considered to be limiting of their scope, certain systems and methods will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

[0008] Figure 1 illustrates an example computer architecture that facilitates an edge device obtaining a service token;

[0009] Figure 2 illustrates an example computer architecture of a directory service and an authentication service;

[0010] Figure 3 illustrates a flow chart of an example method for obtaining a service token from an authentication service; and

[0011] Figure 4 illustrates a flow chart of an example method for obtaining a service token from a directory service.

DETAILED DESCRIPTION

[0012] Edge devices, such as Internet of Things devices, are capable of connecting to online services by utilizing authentication and attestation, resulting in the use of services provided by online service providers. For example, after an edge device boots up, it connects to an online service, such as a cloud service. Based on information provided by the edge device to the cloud service, such as a certificate, the cloud service determines whether the edge device is valid. However, in some instances, a counterfeit device may be authenticated using a counterfeit certificate. In these cases, the counterfeit device could fraudulently access the cloud service. Therefore, there is an ongoing need to provide secure device service tokens to authentic devices allowing the authentic devices to access the online services while avoiding providing counterfeit devices access to online services.

[0013] The embodiments described herein are directed to securely provisioning an edge device with a service token, which allows the edge device to securely access an online service provided by an online application platform. For example, an edge device may use a service token to request

access to an online service found on an application platform such as AZURE SPHERE from MICROSOFT CORPORATION of Redmond, Washington. In embodiments, to access an online service, the edge device initially sends measurement data to a directory service. The directory service uses this measurement information to determine if the edge device is authentic or not. If the edge device is determined by the directory service to be authentic, the edge device is permitted to obtain a device certificate from an authentication service. The authentication service sends the device certificate to the edge device based on a private key stored in the edge device and a public key. The public key is associated with the edge device and is stored in the directory service. In one example, the public key is associated with the edge device at the directory service using a unique device identifier of the edge device. Once the edge device obtains the device certificate from the authentication service, the edge device uses the device certificate to request a service token for accessing an online service.

[0014] By securely obtaining service tokens at edge devices via the use of device certificates that are issued to the edge devices in the manner disclosed, the disclosed embodiments provide authentic devices access to online services while preventing counterfeit devices from accessing the online services.

[0015] Figure 1 illustrates an example of a computer architecture 100 that facilitates obtaining a service token at an edge device. In Figure 1, the computer architecture 100 includes an edge device 101 comprising processing system(s) 102 (e.g., a single processor or a plurality of processors), memory 103 (e.g., system or main memory), operating system (OS) 106, storage media 107 (e.g., a single computer-readable storage medium, or a plurality of computer-readable storage media), all interconnected by a bus 105. In embodiments, edge device 101 also includes a network interface 104 (e.g., one or more network interface cards) for forming local or wide-area network connections via network 111. Lastly, computer architecture 100 also includes a directory service 112 (e.g., AZURE ACTIVE DIRECTORY from MICROSOFT CORPORATION of Redmond, Washington; OKTA WORKFORCE IDENTITY from OKTA INCORPORATED of San Francisco, California), an authentication service 113, and a device registry 116, which are interconnected to one another and the edge device 101 via the network 111.

[0016] The storage media 107 is illustrated as storing data. In some embodiments, the data includes a private key 108 (from an asymmetric public/private key pair) associated with the edge device 101. In embodiments, the private key 108 is stored on the edge device 101 during manufacturing of the edge device 101. In some embodiments, a public key 207 (see Figure 2) that corresponds to private key 108 is also stored on the edge device 101 during manufacturing of the edge device 101.

[0017] The storage media 107 is also illustrated as storing a service token database 109 and a

certificate database 110. In embodiments, the service token database 109 stores one or more service tokens obtained by the edge device, while the certificate database 110 stores one or more certificates obtained by the edge device 101. In embodiments, the edge device 101 obtains certificate(s) from the authentication service 113 and stores those certificate(s) in the certificate database 110. In some embodiments, the edge device 101 receives service token(s) from the authentication service 113 and stores those service token(s) in the service token database 109. In other embodiments, the edge device 101 receives service token(s) from the directory service 112 and stores those service token(s) in the service token database 109.

[0018] In embodiments, storage media 107 also stores a device identifier 114, which is unique to edge device 101 and a client identifier 117, which is unique to the client with which the edge device 101 is associated. In embodiments, the device identifier 114 is extracted from a device certificate stored in the certificate database 110. The device identifier 114 may be extracted, in some embodiments, by the OS 106 of the edge device 101.

[0019] In embodiments, the edge device 101 obtains a device certificate based on using a measurement component 115 to measure a state of the edge device 101 and sends that measurement to the directory service 112. In embodiments, the measured edge device state includes information about the OS 106 (e.g., a version of the OS 106), information about other software operating at the edge device 101, information about a bootup state of the edge device 101, and the like.

[0020] Figure 2 illustrates another example of the computer architecture 100 of Figure 1, with details regarding the directory service 112, the authentication service 113, and the device registry 116. As shown in Figure 2, in embodiments, the directory service 112 comprises processing system(s) 202 (e.g., a single processor or a plurality of processors), memory 203 (e.g., system or main memory), storage media 206 (e.g., a single computer-readable storage medium, or a plurality of computer-readable storage media), all interconnected by a bus 205. In embodiments, the directory service 112 also includes a network interface 204 (e.g., one or more network interface cards) for forming local or wide-area network connections via the network 111 (see Figure 1). Similarly, in embodiments, the authentication service 113 comprises processing system(s) 214 (e.g., a single processor or a plurality of processors), memory 215 (e.g., system or main memory), storage media 218 (e.g., a single computer-readable storage medium, or a plurality of computer-readable storage media), all interconnected by a bus 217. In embodiments, the authentication service 113 also includes a network interface 216 (e.g., one or more network interface cards) for forming local or wide-area network connections via the network 111 (see Figure 1).

[0021] Referring to directory service 112, storage media 206 is illustrated as storing computer-executable instructions implementing a template component 208, a device identifier component

209, a service token component 211, and a mapping component 212. Additionally, the storage media 206 is illustrated as storing data such as a device object 210 associated with the edge device 101.

[0022] The device registry 116 is illustrated as storing data such as a public key 207, which cryptographically corresponds to the private key 108 of the edge device 101, and a device object 219 associated with the edge device 101. In embodiments, the device object 219 associates the public key 207 with the device identifier 114 of the edge device 101. In some embodiments, the directory service 112 obtains public key 207 from the device registry 116 or from the edge device 101 directly (e.g., during provisioning of edge device 101 within computer architecture 100) or from a manufacturer of edge device 101.

[0023] The authentication service 113 is also referred to as the device attestation and authentication service. In some embodiments, the authentication service 113 performs both authentication tasks as well as attestation tasks. The storage media 218 is illustrated as storing computer-executable instructions implementing at least a certificate component 221 and a service token component 222. Storage media 218 is also illustrated as storing data such as a device mapping 220. In embodiments, the authentication service 113 uses the certificate component 221 to generate a device certificate for the edge device 101. In embodiments, the generated device certificate is based on the public key 207, such that the generated device certificate is usable by edge device 101 based on its possession of private key 108. In an embodiment, authentication service 113 obtains the public key 207 from one or more of the edge device 101, the device registry 116, or the directory service 112. In embodiments, authentication service 113 generates the device certificate based on receiving confirmation from the directory service 112 that the public key 207 of edge device 101 corresponds to the device identifier 114 of the edge device 101 (e.g., based on device object 210).

[0024] In embodiments, the directory service 112 associates the public key 207 stored in the device registry 116 with a device identifier 114 stored in the storage media 206. In embodiments, the device identifier component 209 creates the device identifier 114 for the edge device 101. While a variety of device identifier types can be used, in embodiments, the device identifier component 209 generates a globally-unique identifier (GUID) (e.g. a 128-bit or a 256-bit GUID). In embodiments, the device identifier component 209 stores the created device identifier 114 in the device certificate created by the certificate component 221 at the authentication service 113. In embodiments, this enables the edge device 101 to obtain the device identifier 114 by extracting the device identifier 114 from the device certificate (e.g., using the OS 106 of the edge device 101). In embodiments, a template component 208 creates a device template that specifies the general parameters of edge device 101, such as manufacturer, model, OS, and the like.

[0025] Embodiments create device object 210 associated with the edge device 101 and store that device object 210 in the storage media 206 of the directory service 112. Embodiments also create device object 219 associated with the edge device 101 and store that device object 219 in the device registry 116. A mapping component 212 at the directory service 112 maps the device object 210 and the device object 219 and stores that mapping in a device mapping 220 at the authentication service 113. In embodiments, the mapping component 212 maps the device identifier 114 with a device certificate and sends the device mapping 220 to the authentication service 113. The authentication service 113, in turn, stores the device mapping 220 in the storage media 218.

[0026] In some embodiments, the edge device 101 sends a request to the authentication service 113 for a service token that is used to access an online service. In these embodiments, the request is based on the device certificate generated by the authentication service 113. Once the authentication service 113 receives the request for the service token, the service token component 222 creates the service token and sends the service token to the edge device 101. The edge device 101 receives the service token and stores the service token in the service token database 109. The edge device 101 then uses the service token stored in the service token database 109 to access an online service (e.g., an AZURE SPHERE application).

[0027] Embodiments are now described in connection with Figures 3 and 4, which illustrate flow charts of example methods 300 and 400 for obtaining a service token at an edge device. In embodiments, instructions for implementing methods 300 and 400 are encoded as computer-executable instructions (e.g., device identifier component 209, service token component 211, and certificate component 221) stored on a computer storage media (e.g., storage media 107, 206, and 218) that are executable by a processing system (e.g., processing system(s) 102, 202, and 214) to cause a computer system (e.g., edge device 101, directory service 112, authentication service 113) to perform the method.

[0028] The following discussion now refers to a number of methods and method acts. Although the method acts may be discussed in certain orders, or may be illustrated in a flow chart as occurring in a particular order, no particular ordering is required unless specifically stated, or required because an act is dependent on another act being completed prior to the act being performed.

[0029] Referring to Figure 3, method 300 illustrates an embodiment in which the edge device 101 obtains a service token from the directory service 112 directly. In some embodiments, method 300 comprises act 301 of sending a measurement of edge device state. In some embodiments, act 301 comprises sending a measurement of edge device state to a directory service. For example, the measurement component 115 at the edge device 101 measures edge device state of the edge device

101. In embodiments, the measured edge device state includes information about the OS 106 of the edge device 101 (e.g., OS version information), information about other software operating at the edge device 101, information about a bootup state of the edge device 101, and the like. In embodiments, the edge device 101 sends this measurement of the edge device state to the directory service 112. In embodiments, the directory service 112 uses this measurement to determine whether the edge device 101 is an authentic device or a counterfeit device.

[0030] Method 300 also comprises an act 302 of obtaining a device certificate. In some embodiments, act 302 comprises, based on the possession of a private key at the edge device, obtaining a device certificate from an authentication service. For example, the edge device 101 obtains a device certificate from authentication service 113 and stores that certificate in the certificate database 110. In embodiments, the authentication service 113 uses the certificate component 221 to generate the device certificate for the edge device 101.

[0031] In embodiments, the private key is associated with the public key, and the public key is associated with a device identifier for the edge device at the device registry. For example, the private key 108 and the public key 207 form an asymmetric cryptographic key pair that was created during the manufacturing of edge device 101. In embodiments, the private key 108 (and, potentially, public key 207) is stored on the edge device 101 during manufacturing of the edge device 101. In embodiments, the directory service 112 receives the public key 207 (e.g., from the edge device 101, from a manufacturer of edge device 101), and the directory service 112 creates the device identifier 114 for the edge device 101 (device identifier component 209). The directory service 112 further maps the identity of the edge device 101 with the public key 207 using the mapping component 212. The mapping component also maps the device object 210 with a device object 219 stored in the device registry 116 and sends a device mapping 220 to the authentication service 113.

[0032] Method 300 also comprises act 303 of sending a request for a service token to an authentication service from a directory service. In some embodiments, act 303 comprises, based on the private key, sending a request for a service token to the authentication service from a directory service, wherein the directory service has identified the public key for the edge device.

[0033] Method 300 also comprises act 304 of receiving the service token. In some embodiments, act 304 comprises receiving the service token from the authentication service. In embodiments, the service token component 222 creates the service token after receiving a request and sends the service token to the edge device 101. The edge device 101 then stores the service token in the service token database 109.

[0034] Method 300 also comprises act 305 of using the service token. In some embodiments, act 304 comprises using the service token to access a service. In embodiments, once the edge device

101 has stored the service token in the service token database 109, the edge device 101 uses the service token to access services (e.g., applications found in AZURE SPHERE or similar application platforms).

[0035] Referring to Figure 4, method 400 illustrates an embodiment in which the edge device 101 obtains a service token from the directory service 112 via the authentication service 113. In 5 embodiments, method 400 comprises act 401 of sending a measurement of edge device state. In some embodiments, act 401 comprises sending a measurement of edge device state to the directory service. For example, the measurement component 115 at the edge device 101 measures the edge device state the edge device 101. The measured edge device state includes information about the 10 OS 106 of the edge device 101 (e.g., OS version information), information about other software operating at the edge device 101, information about a bootup state of the edge device 101, and the like. In embodiments, the edge device 101 sends this measurement of the edge device state to the directory service 112. In embodiments, the directory service 112 uses this measurement to determine whether the edge device 101 is an authentic device or a counterfeit device.

[0036] Method 400 also comprises an act 402 of obtaining a device certificate. In some 15 embodiments, act 402 comprises, based on a private key at the edge device, obtaining a device certificate from an authentication service. For example, the edge device 101 obtains a device certificate from authentication service 113 and stores that certificate in the certificate database 110. In embodiments, the authentication service 113 uses the certificate component 221 to 20 generate the device certificate for the edge device 101.

[0037] In embodiments, the private key is associated with the public key, and the public key is associated with a device identifier for the edge device at the directory service. For example, the private key 108 and the public key 207 form an asymmetric cryptographic key pair that was created during the manufacturing of edge device 101. In embodiments, the private key 108 (and, 25 potentially, public key 207) is stored on the edge device 101 during manufacturing of the edge device 101. In embodiments, the directory service 112 receives the public key 207 (e.g., from the edge device 101, from a manufacturer of edge device 101), and the directory service 112 creates the device identifier 114 for the edge device 101 (device identifier component 209). The directory service 112 further maps the identity of the edge device 101 with the public key 207 using the 30 mapping component 212. The mapping component also maps the device object 210 with a device object 219 stored in the device registry 116 and sends a device mapping 220 to the authentication service 113.

[0038] Method 400 also comprises act 403 of extracting a device identifier from the device certificate. In some embodiments, act 403 comprises extracting the device identifier from the 35 device certificate. In embodiments, the device identifier 114 is stored in the device certificate

using the device identifier component 209. The edge device 101 receives this device certificate and stores the certificate in the certificate database 110. The edge device 101 then extracts the device identifier 114 from the device certificate (e.g., using the OS 106 of the edge device 101). The edge device 101 stores the device identifier 114 in the storage media 107.

5 **[0039]** Method 400 also comprises act 404 of sending a request for a service token to the directory service. In some embodiments, act 404 comprises sending a request for a service token to the directory service where the request includes the device certificate and the device identifier. In some embodiments, the request includes the client identifier as well as the device certificate and the device identifier.

10 **[0040]** Method 400 also comprises act 405 of receiving the service token. In some embodiments, act 405 comprises receiving the service token from the directory service based on the directory service identifying the public key for the edge device. In embodiments, the directory service 112 receives the request from the edge device 101 for a service token and identifies the public key 207, which corresponds to the edge device 101. The service token component 211 creates the
15 service token and sends the service token to the edge device. The edge device 101 stores the service token in the service token database 109.

[0041] Method 400 also comprises act 406 of using the service token. In some embodiments, act 406 comprises using the service token to access a service. In embodiments, once the edge device 101 has stored the service token in the service token database 109, the edge device 101 may use
20 the service token to access services (e.g., applications found in AZURE SPHERE or similar application platforms).

[0042] Embodiments of the disclosure may comprise or utilize a special-purpose or general-purpose computer system (e.g., edge device 101, directory service 112, and authentication service 113) that includes computer hardware, such as, for example, a processing system (e.g., processing
25 system(s) 102, 202, and 214) and system memory (e.g., memory 103, 203, and 215), as discussed in greater detail below. Embodiments within the scope of the present disclosure also include physical and other computer-readable media for carrying or storing computer-executable instructions and/or data structures. Such computer-readable media can be any available media that can be accessed by a general-purpose or special-purpose computer system. Computer-readable
30 media that store computer-executable instructions and/or data structures are computer storage media (e.g., storage media 107, 206, and 218). Computer-readable media that carry computer-executable instructions and/or data structures are transmission media. Thus, by way of example, embodiments of the disclosure can comprise at least two distinctly different kinds of computer-readable media: computer storage media and transmission media.

35 **[0043]** Computer storage media are physical storage media that store computer-executable

instructions and/or data structures. Physical storage media include computer hardware, such as random access memory (RAM), read-only memory (ROM), electrically erasable programmable ROM (EEPROM), solid state drives (SSDs), flash memory, phase-change memory (PCM), optical disk storage, magnetic disk storage or other magnetic storage devices, or any other hardware storage device(s) which can be used to store program code in the form of computer-executable instructions or data structures, which can be accessed and executed by a general-purpose or special-purpose computer system to implement the disclosed functionality.

[0044] Transmission media can include a network and/or data links that can be used to carry program code in the form of computer-executable instructions or data structures and which can be accessed by a general-purpose or special-purpose computer system. A “network” is defined as one or more data links that enable the transport of electronic data between computer systems and/or modules and/or other electronic devices. When information is transferred or provided over a network or another communications connection (either hardwired, wireless, or a combination of hardwired or wireless) to a computer system, the computer system may view the connection as transmission media. Combinations of the above should also be included within the scope of computer-readable media.

[0045] Further, upon reaching various computer system components, program code in the form of computer-executable instructions or data structures can be transferred automatically from transmission media to computer storage media (or vice versa). For example, computer-executable instructions or data structures received over a network or data link can be buffered in RAM within a network interface module (e.g., network interface 104), and then eventually transferred to computer system RAM and/or to less volatile computer storage media at a computer system. Thus, it should be understood that computer storage media can be included in computer system components that also (or even primarily) utilize transmission media.

[0046] Computer-executable instructions comprise, for example, instructions and data which, when executed at one or more processors, cause a general-purpose computer system, special-purpose computer system, or special-purpose processing device to perform a certain function or group of functions. Computer-executable instructions may be, for example, binaries, intermediate format instructions such as assembly language, or even source code.

[0047] It will be appreciated that the disclosed systems and methods may be practiced in network computing environments with many types of computer system configurations, including, personal computers, desktop computers, laptop computers, message processors, hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, mobile telephones, PDAs, tablets, pagers, routers, switches, and the like. Embodiments of the disclosure may also be practiced in distributed system

environments where local and remote computer systems, which are linked (either by hardwired data links, wireless data links, or by a combination of hardwired and wireless data links) through a network, both perform tasks. As such, in a distributed system environment, a computer system may include a plurality of constituent computer systems. In a distributed system environment, program modules may be located in both local and remote memory storage devices.

[0048] It will also be appreciated that the embodiments of the disclosure may be practiced in a cloud computing environment. Cloud computing environments may be distributed, although this is not required. When distributed, cloud computing environments may be distributed internationally within an organization and/or have components possessed across multiple organizations. In this description and the following claims, “cloud computing” is defined as a model for enabling on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services). A cloud computing model can be composed of various characteristics, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service, and so forth. A cloud computing model may also come in the form of various service models such as, for example, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The cloud computing model may also be deployed using different deployment models such as private cloud, community cloud, public cloud, hybrid cloud, and so forth.

[0049] Some embodiments, such as a cloud computing environment, may comprise a system that includes one or more hosts that are each capable of running one or more virtual machines. During operation, virtual machines emulate an operational computing system, supporting an OS and perhaps one or more other applications as well. In some embodiments, each host includes a hypervisor that emulates virtual resources for the virtual machines using physical resources that are abstracted from the view of the virtual machines. The hypervisor also provides proper isolation between the virtual machines. Thus, from the perspective of any given virtual machine, the hypervisor provides the illusion that the virtual machine is interfacing with a physical resource, even though the virtual machine only interfaces with the appearance (e.g., a virtual resource) of a physical resource. Examples of physical resources including processing capacity, memory, disk space, network bandwidth, media drives, and so forth.

[0050] Although the subject matter has been described in language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the described features or acts described above, or the order of the acts described above. Rather, the described features and acts are disclosed as example forms of implementing the claims.

[0051] The present disclosure may be embodied in other specific forms without departing from

its essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

[0052] When introducing elements in the appended claims, the articles “a,” “an,” “the,” and “said”

5 are intended to mean there are one or more of the elements. The terms “comprising,” “including,” and “having” are intended to be inclusive and mean that there may be additional elements other than the listed elements. Unless otherwise specified, the terms “set,” “superset,” and “subset” are intended to exclude an empty set, and thus “set” is defined as a non-empty set, “superset” is defined as a non-empty superset, and “subset” is defined as a non-empty subset. Unless otherwise
10 specified, the term “subset” excludes the entirety of its superset (i.e., the superset contains at least one item not included in the subset). Unless otherwise specified, a “superset” can include at least one additional element, and a “subset” can exclude at least one element.

CLAIMS

1. A method (300) implemented at an edge device computer system (101) that includes a processing system (102), comprising:

based on a private key (101) at the edge device, obtaining (302) a device certificate from an authentication service (113), wherein the private key is associated with a public key (207), the public key being associated with a device identifier for the edge device at a directory service (112);

based on the private key, sending (303) a request for a service token to the authentication service from the directory service, wherein the directory service has identified the public key for the edge device;

receiving (304) the service token from the authentication service; and

using (305) the service token to access a service.

2. The method of claim 1, further comprising sending a measurement of edge device state to the authentication service.

3. The method of claim 1 or claim 2, wherein the device identifier for the edge device is mapped with the public key for the edge device.

4. The method of claim 1 to claim 3, wherein the device identifier for the edge device is created by the directory service.

5. The method of claim 1 to claim 4, wherein a first object of the edge device stored in the directory service is mapped with a second object of the edge device stored in a device registry.

6. The method of claim 1 to claim 5, wherein the private key is stored on the edge device during manufacturing, and wherein the public key is stored in a device registry.

7. A method (400) implemented at a computer system (101) that includes a processing system (102), comprising:

based on a private key (108) at an edge device, obtaining (402) a device certificate from an authentication service (113), wherein the private key is associated with a public key (207), the public key being associated with a device identifier for the edge device at a directory service (112);

extracting (403) the device identifier from the device certificate;

sending (404) a request for a service token to the directory service, wherein the request includes the device certificate, a client identifier, and the device identifier;

receiving (405) the service token from the directory service based on the directory service identifying the public key for the edge device; and

using (406) the service token to access a service.

8. The method of claim 7, wherein an operating system on the edge device extracts the device identifier from the device certificate.

9. The method of claim 7 or claim 8, further comprising sending a measurement of edge device state to the authentication service.
10. The method of claim 7 to claim 9, wherein the device identifier for the edge device is mapped with the public key for the edge device.
11. The method of claim 7 to claim 10, wherein the device identifier for the edge device is created by the directory service.
12. The method of claim 7 to claim 11, wherein a first object of the edge device stored in the directory service is mapped with a second object of the edge device stored in a device registry.
13. The method of claim 7 to claim 12, wherein the private key is stored on the edge device during manufacturing, and wherein the public key is stored in a device registry.
14. A computer system (101) comprising:
 - a processing system (102); and
 - a computer storage media (107) that stores computer-executable instructions that are executable by the processing system to at least:
 - based on a private key (108) at an edge device, obtain (402) a device certificate from an authentication service (113), wherein the private key is associated with a public key (207), the public key being associated with a device identifier for the edge device at a directory service (112);
 - extract (403) the device identifier from the device certificate;
 - send (404) a request for a service token to the directory service, wherein the request includes the device certificate and the device identifier;
 - receive (405) the service token from the directory service based on the directory service identifying the public key for the edge device; and
 - use (406) the service token to access a service.
15. The computer system of claim 14, wherein an operating system on the edge device extracts the device identifier from the device certificate.
16. The computer system of claim 14 or claim 15, the computer-executable instructions also executable by the processing system to send a measurement of edge device state to the authentication service.
17. The computer system of claim 14 to claim 16, wherein the device identifier for the edge device is mapped with the public key for the edge device.
18. The computer system of claim 14 to claim 17, wherein the device identifier for the edge device is created by the directory service.
19. The computer system of claim 14 to claim 18, wherein a first object of the edge

device stored in the directory service is mapped with a second object of the edge device stored in a device registry.

20. The computer system of claim 14 to claim 19, wherein the private key is stored on the edge device during manufacturing, and wherein the public key is stored in a device registry.

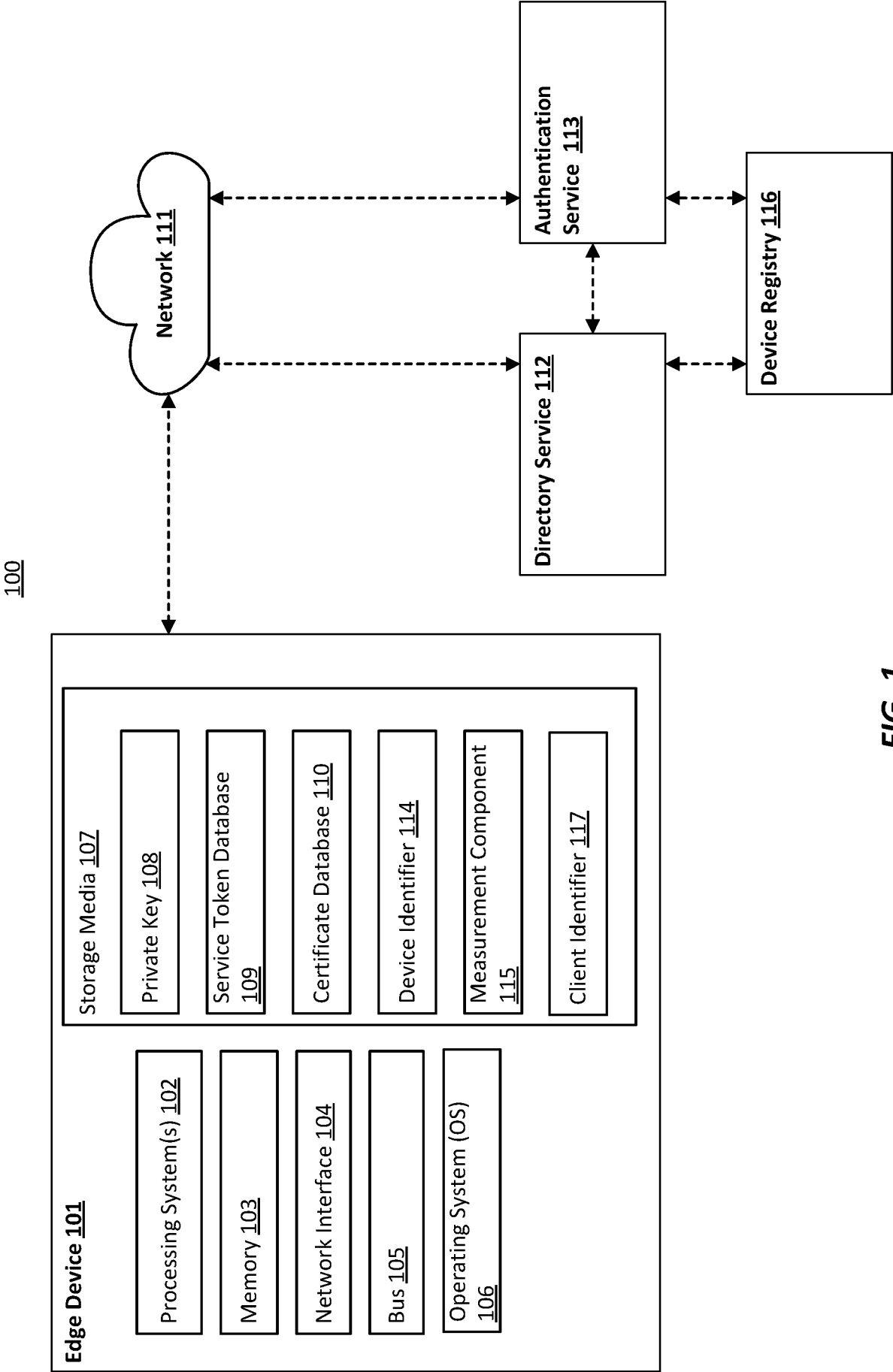


FIG. 1

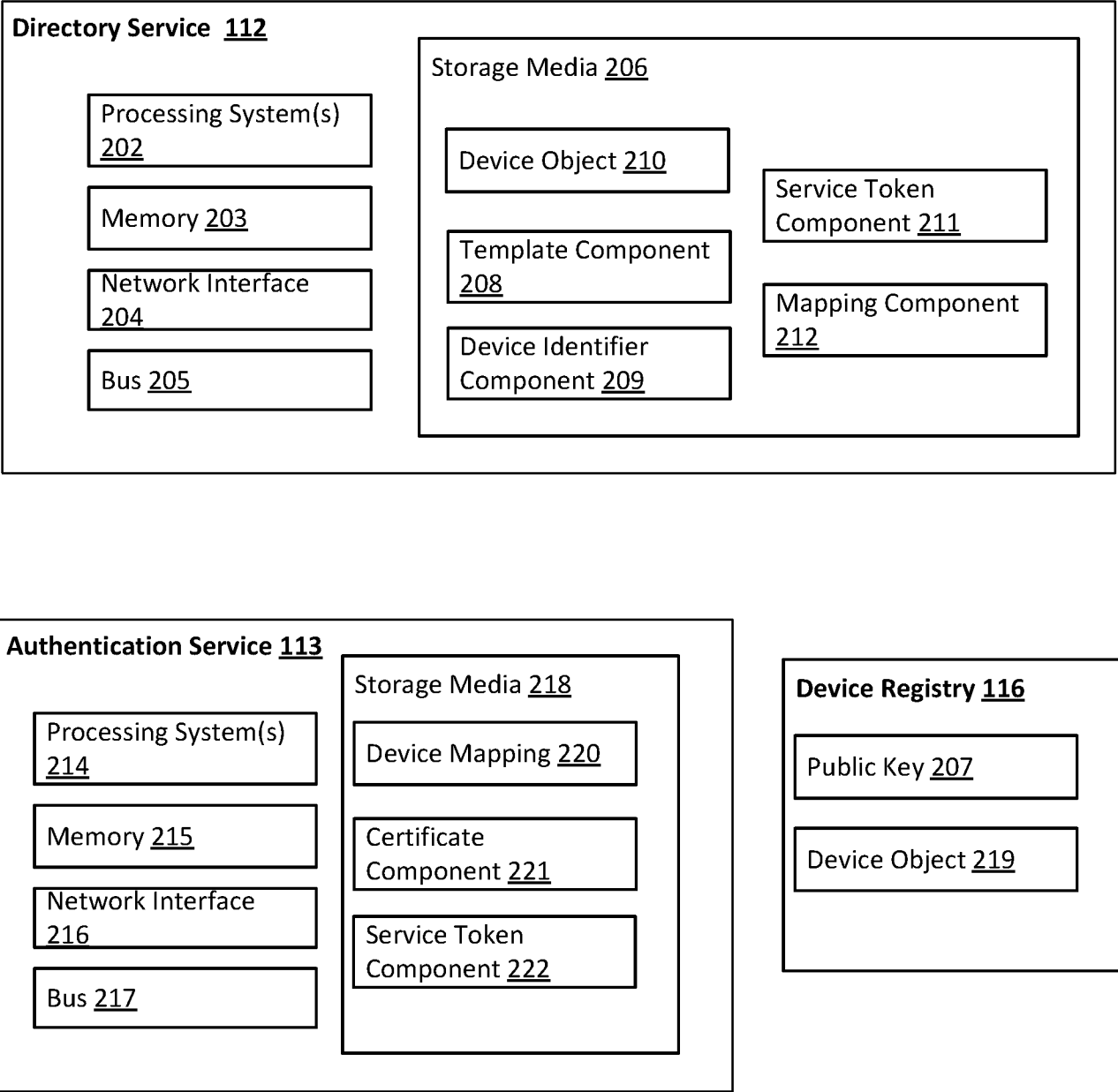
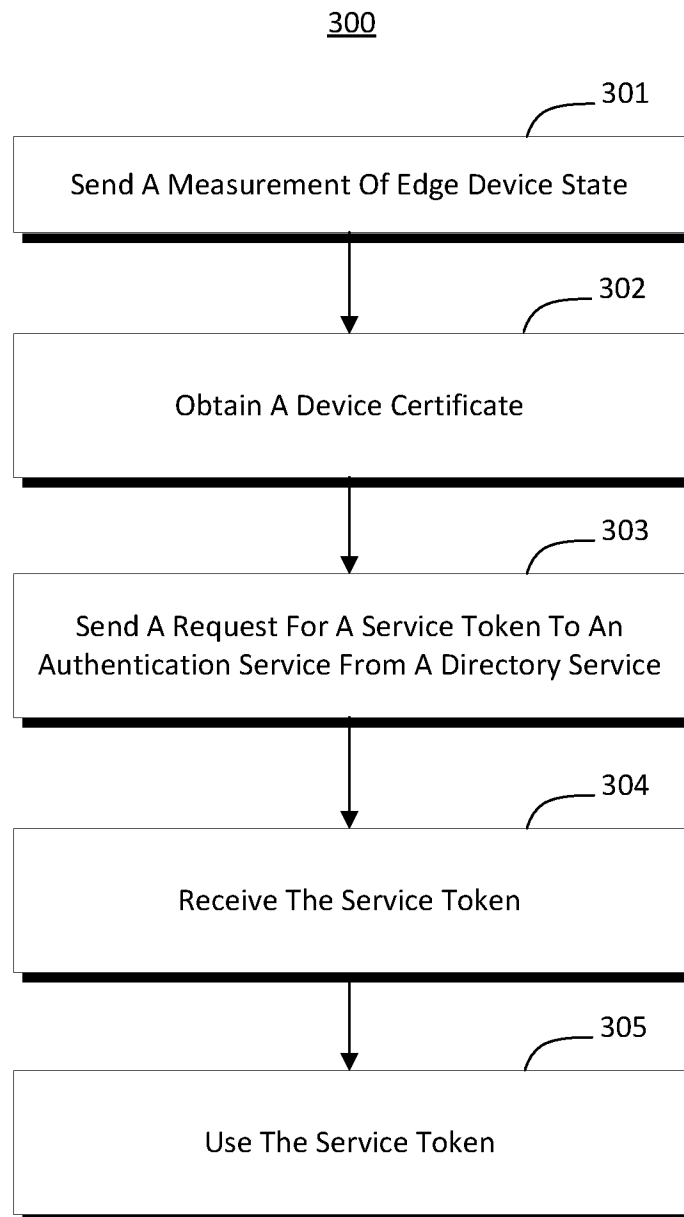
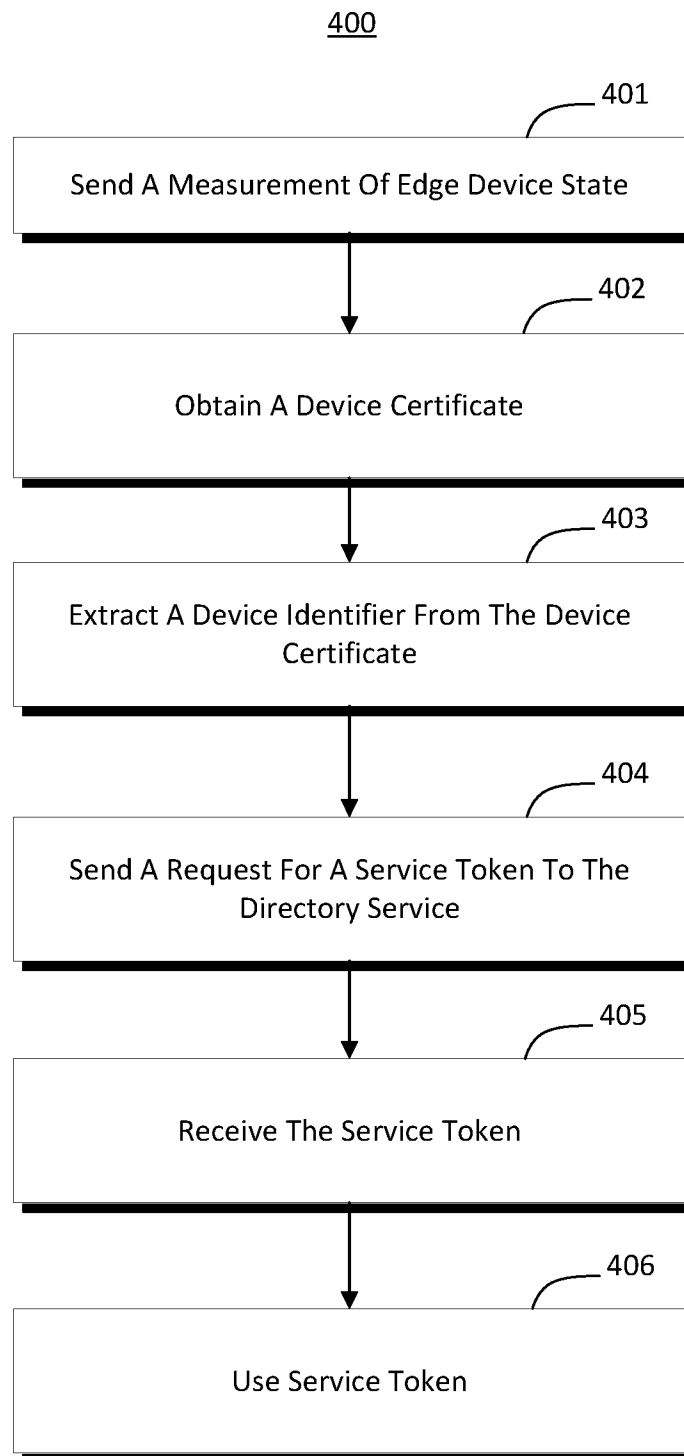


FIG. 2

3/4

**FIG. 3**

4/4

**FIG. 4**

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2024/031520

A. CLASSIFICATION OF SUBJECT MATTER INV. H04L9/40 ADD.				
According to International Patent Classification (IPC) or to both national classification and IPC				
B. FIELDS SEARCHED				
Minimum documentation searched (classification system followed by classification symbols) H04L H04W				
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched				
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO-Internal, INSPEC, WPI Data				
C. DOCUMENTS CONSIDERED TO BE RELEVANT				
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.		
X	MARTINS ROLANDO ET AL: "Iris: Secure reliable live-streaming with opportunistic mobile edge cloud offloading", FUTURE GENERATION COMPUTER SYSTEMS, ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, NL, vol. 101, 20 June 2019 (2019-06-20), pages 272-292, XP085914789, ISSN: 0167-739X, DOI: 10.1016/J.FUTURE.2019.06.011 [retrieved on 2019-06-20] the whole document ----- - / - -	1 - 20		
<table><tr><td>☒ Further documents are listed in the continuation of Box C.</td><td>☒ See patent family annex.</td></tr></table>			☒ Further documents are listed in the continuation of Box C.	☒ See patent family annex.
☒ Further documents are listed in the continuation of Box C.	☒ See patent family annex.			
<table><tr><td>* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed</td><td>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance;; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance;; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family</td></tr></table>			* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance;; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance;; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance;; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance;; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family			
Date of the actual completion of the international search 20 September 2024		Date of mailing of the international search report 02/10/2024		
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer Dujardin, Corinne		

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2024/031520

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CAMPBELL PING IDENTITY J BRADLEY YUBICO N SAKIMURA NOMURA RESEARCH INSTITUTE T LODDERSTEDT YES COM AG B: "OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens; rfc8705.txt", OAUTH 2.0 MUTUAL-TLS CLIENT AUTHENTICATION AND CERTIFICATE-BOUND ACCESS TOKENS; RFC8705.TXT, INTERNET ENGINEERING TASK FORCE, IETF; STANDARD, INTERNET SOCIETY (ISOC) 4, RUE DES FALAISES CH- 1205 GENEV , 29 February 2020 (2020-02-29), pages 1-14, XP015136794, Retrieved from the Internet: URL:https://tools.ietf.org/html/rfc8705 [retrieved on 2020-02-29] the whole document -----	1 - 20
X	US 2018/007035 A1 (ZHANG JENNY QIAN [US] ET AL) 4 January 2018 (2018-01-04) abstract paragraph [0002] - paragraph [0004] paragraph [0011] - paragraph [0048] figures 1-3 -----	1 - 20
A	US 2021/226951 A1 (GOLDSTEIN PETER MARTIN [US] ET AL) 22 July 2021 (2021-07-22) abstract paragraph [0002] - paragraph [0004] paragraph [0037] - paragraph [0468] figures 1A-24 -----	1 - 20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2024/031520

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2018007035	A1	04-01-2018	NONE

US 2021226951	A1	22-07-2021	AU 2021209899 A1 25-08-2022
			AU 2024201925 A1 18-04-2024
			CA 3165696 A1 29-07-2021
			EP 4094417 A1 30-11-2022
			IL 294919 A 01-09-2022
			US 2021226951 A1 22-07-2021
			WO 2021150798 A1 29-07-2021
