



- (51) **International Patent Classification:**
H04L 9/32 (2006.01) *G06F 21/31* (2013.01)
- (21) **International Application Number:**
PCT/US2013/028121
- (22) **International Filing Date:**
28 February 2013 (28.02.2013)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
13/425,143 20 March 2012 (20.03.2012) US
- (71) **Applicant (for all designated States except US):** **MI-CROSOFT CORPORATION** [US/US]; One Microsoft Way, Redmond, Washington 98052-6399 (US).
- (72) **Inventors:** **WELLS, Dean**; c/o Microsoft Corporation, LCA - International Patents, One Microsoft Way, Redmond, Washington 98052-6399 (US). **DIDCOCK, Clifford N.**; c/o Microsoft Corporation, LCA - International Patents, One Microsoft Way, Redmond, Washington 98052-6399 (US). **CHANDER, Girish**; c/o Microsoft Corporation, LCA - International Patents, One Microsoft Way, Redmond, Washington 98052-6399 (US). **ADAMS, Ross**;

c/o Microsoft Corporation, LCA - International Patents, 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, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) **Designated States (unless otherwise indicated, for every kind of regional protection available):** ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) **Title:** IDENTITY SERVICES FOR ORGANIZATIONS TRANSPARENTLY HOSTED IN THE CLOUD

(57) **Abstract:** Embodiments of the invention are disclosed for establishing single identity/single-sign on (SSO) on a cloud computing platform. In an embodiment, a user is validated to the cloud computing platform, and identifies a domain. After establishing that the user has control of the domain, the cloud computing platform configures a directory service for the domain. The user may then use the directory service on the cloud computing platform to log in to his or her computer, as well as software services hosted on the cloud computing platform.

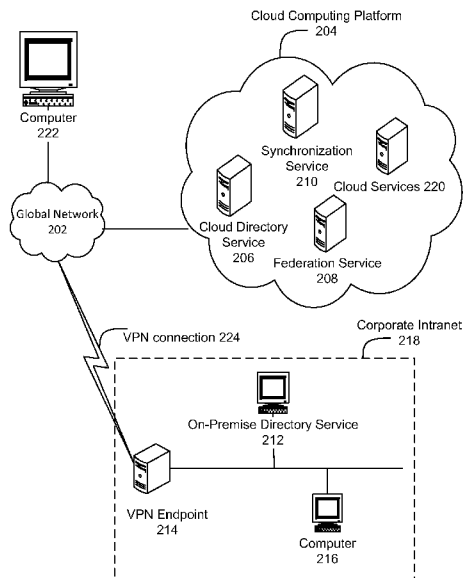
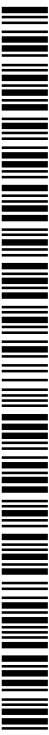


FIG. 2



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))*

IDENTITY SERVICES FOR ORGANIZATIONS TRANSPARENTLY HOSTED IN
THE CLOUD

BACKGROUND

5 [0001] There are techniques that permit a user to log in once, and gain access to multiple software systems. That is, the user gains access to each of those software systems without needing to log in to each of them. These technologies are sometimes referred to as “single sign-on,” (SSO) or “single identity.” However, there are many problems with existing SSO/single identity technologies, some of which are well known.

SUMMARY

10 [0002] One problem with implementing SSO/single identity is the amount of technologies that must be configured and installed. To implement SSO/single identity, an administrator must be able to configure and deploy a directory service, a federation service, a synchronization service, a domain name service (DNS), and operating systems.

15 [0003] Another problem exists with SSO/single identity for services provided by cloud computing platforms. Examples of such services include cloud-based document and file management services (such as MICROSOFT OFFICE 365 SHAREPOINT ONLINE), or email services (such as MICROSOFT OFFICE 365 EXCHANGE ONLINE). Even if an administrator implements an on-premises directory (one that is implemented on his or her premises, rather than implemented on a cloud computing platform), that SSO/single
20 identity does not extend to the cloud. Additionally, where SSO is implemented on premise, the system must have great reliability. If the SSO/single identity is not functional, then a user may not log in to either the on premise services, or the cloud services.

25 [0004] The primary embodiment of the invention described herein is for SSO. It may be appreciated that the invention may be used to implement cloud-based single identity in a similar fashion. Embodiments of the invention provide for SSO to services in the cloud in ways that combine both on-premises and cloud SSO, and improve the reliability of SSO. An embodiment of the invention implements SSO in the cloud where there is no on-premises directory. A user is validated to the cloud platform through the use
30 of credentials, such as a logon and password. The user then identifies a public domain for which he wishes to establish SSO, and proves that he has control of the domain. In response to this, the embodiment stands up a domain controller, and federation services. Users of the domain may then both log in to their computer and access cloud services via a SSO.

[0005] A second embodiment of the invention implements SSO in the cloud where there is no on-premises directory, and where the user wishes to establish SSO for a private domain. In this embodiment, SSO may be established similar to how SSO is established for a public domain, above. However, the user may not be required to prove
5 that he has control of the private domain.

[0006] A third embodiment of the invention implements SSO in the cloud where there is on-premises directory service. In this embodiment, SSO may be established similar to how SSO is established for a public domain, above. Additionally, the user provides a credential to access an on-premises domain controller via a virtual private
10 network (VPN) endpoint that is running on premise. In addition to what is performed above, the embodiment both replicates data in the on-premises domain to the cloud domain service, and stands up a synchronization service that will replicate data between the cloud domain service and the on-premises domain service, as well as synchronize data from the on-premises domain service to services hosted by the cloud computing platform.
15 The embodiment also establishes a VPN connection with the on-premises VPN endpoint, and the synchronization service uses this VPN connection to synchronize data stored in the cloud directory service with data stored in the on-premises directory service.

[0007] These embodiments of the invention may extend a private cloud to the customer's on-premises infrastructure via a VPN, or similar, connection. This extension
20 of a private cloud to the customer's on-premises infrastructure allows the customer to extend its functionality without the addition of visible infrastructure – the infrastructure that is added is invisible to the customer, who sees only the added functionality. As such, the on-premises infrastructure may be kept relatively simple, though the functionality is increased. In this sense, the cloud infrastructure may be logically divided into two
25 categories – (1) the cloud-based extension of the on-premises infrastructure that facilitates the SSO/single-identity access to the (2) public cloud services (e.g., email). The cloud-based extension of the on-premises infrastructure may insert a private cloud footprint on the customer's behalf. This private cloud footprint extends the cloud based services of on-premises synchronization services, federation services, and directory services to the on-
30 premises network.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] FIG. 1 depicts an example computer in which embodiments of the invention may be implemented.

[0009] FIG. 2 depicts an example system in which embodiments of establishing SSO on a cloud computing platform may be implemented.

[0010] FIG. 3 depicts example operating procedures for establishing SSO on a cloud computing platform.

5 [0011] FIG. 4 depicts additional example operating procedures for establishing SSO on a cloud computing platform with a public domain.

[0012] FIG. 5 depicts additional example operating procedures for establishing SSO on a cloud computing platform with a private domain.

[0013] FIG. 6 depicts additional example operating procedures for establishing
10 SSO on a cloud computing platform where there is on-premises directory.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

[0014] Embodiments of the invention may execute on one or more computer systems. FIG. 1 and the following discussion are intended to provide a brief general description of a suitable computing environment in which embodiments of the invention
15 may be implemented.

[0015] FIG. 1 depicts an example general purpose computing system. The general purpose computing system may include a conventional computer 20 or the like, including processing unit 21. Processing unit 21 may comprise one or more processors, each of which may have one or more processing cores. A multi-core processor, as
20 processors that have more than one processing core are frequently called, comprises multiple processors contained within a single chip package.

[0016] Computer 20 may also comprise graphics processing unit (GPU) 90. GPU 90 is a specialized microprocessor optimized to manipulate computer graphics. Processing unit 21 may offload work to GPU 90. GPU 90 may have its own graphics
25 memory, and/or may have access to a portion of system memory 22. As with processing unit 21, GPU 90 may comprise one or more processing units, each having one or more cores.

[0017] Computer 20 may also comprise a system memory 22, and a system bus 23 that communicative couples various system components including the system memory
30 22 to the processing unit 21 when the system is in an operational state. The system memory 22 can include read only memory (ROM) 24 and random access memory (RAM) 25. A basic input/output system 26 (BIOS), containing the basic routines that help to transfer information between elements within the computer 20, such as during start up, is stored in ROM 24. The system bus 23 may be any of several types of bus structures

including a memory bus or memory controller, a peripheral bus, or a local bus, which implements any of a variety of bus architectures. Coupled to system bus 23 may be a direct memory access (DMA) controller 80 that is configured to read from and/or write to memory independently of processing unit 21. Additionally, devices connected to system
5 bus 23, such as storage drive I/F 32 or magnetic disk drive I/F 33 may be configured to also read from and/or write to memory independently of processing unit 21, without the use of DMA controller 80.

[0018] The computer 20 may further include a storage drive 27 for reading from and writing to a hard disk (not shown) or a solid-state disk (SSD) (not shown), a magnetic
10 disk drive 28 for reading from or writing to a removable magnetic disk 29, and an optical disk drive 30 for reading from or writing to a removable optical disk 31 such as a CD ROM or other optical media. The hard disk drive 27, magnetic disk drive 28, and optical disk drive 30 are shown as connected to the system bus 23 by a hard disk drive interface
32, a magnetic disk drive interface 33, and an optical drive interface 34, respectively. The
15 drives and their associated computer-readable storage media provide non-volatile storage of computer readable instructions, data structures, program modules and other data for the computer 20.

[0019] Although the example environment described herein employs a hard disk, a removable magnetic disk 29 and a removable optical disk 31, it should be appreciated by
20 those skilled in the art that other types of computer readable media which can store data that is accessible by a computer, such as flash memory cards, digital video discs or digital versatile discs (DVDs), random access memories (RAMs), read only memories (ROMs) and the like may also be used in the example operating environment. Generally, such computer readable storage media can be used in some embodiments to store processor
25 executable instructions embodying aspects of the present disclosure. Computer 20 may also comprise a host adapter 55 that connects to a storage device 62 via a small computer system interface (SCSI) bus 56.

[0020] A number of program modules comprising computer-readable instructions may be stored on computer-readable media such as the hard disk, magnetic
30 disk 29, optical disk 31, ROM 24 or RAM 25, including an operating system 35, one or more application programs 36, other program modules 37, and program data 38. Upon execution by the processing unit, the computer-readable instructions cause actions described in more detail below to be carried out or cause the various program modules to be instantiated. A user may enter commands and information into the computer 20

through input devices such as a keyboard 40 and pointing device 42. Other input devices (not shown) may include a microphone, joystick, game pad, satellite disk, scanner or the like. These and other input devices are often connected to the processing unit 21 through a serial port interface 46 that is coupled to the system bus, but may be connected by other
5 interfaces, such as a parallel port, game port or universal serial bus (USB). A display 47 or other type of display device can also be connected to the system bus 23 via an interface, such as a video adapter 48. In addition to the display 47, computers typically include other peripheral output devices (not shown), such as speakers and printers.

[0021] The computer 20 may operate in a networked environment using logical
10 connections to one or more remote computers, such as a remote computer 49. The remote computer 49 may be another computer, a server, a router, a network PC, a peer device or other common network node, and typically can include many or all of the elements described above relative to the computer 20, although only a memory storage device 50 has been illustrated in FIG. 1. The logical connections depicted in FIG. 1 can include a
15 local area network (LAN) 51 and a wide area network (WAN) 52. Such networking environments are commonplace in offices, enterprise wide computer networks, intranets and the Internet.

[0022] When used in a LAN networking environment, the computer 20 can be connected to the LAN 51 through a network interface or adapter 53. When used in a
20 WAN networking environment, the computer 20 can typically include a modem 54 or other means for establishing communications over the wide area network 52, such as the INTERNET. The modem 54, which may be internal or external, can be connected to the system bus 23 via the serial port interface 46. In a networked environment, program modules depicted relative to the computer 20, or portions thereof, may be stored in the
25 remote memory storage device. It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between the computers may be used.

[0023] In an embodiment where computer 20 is configured to operate in a networked environment, OS 35 is stored remotely on a network, and computer 20 may
30 netboot this remotely-stored OS rather than booting from a locally-stored OS. In an embodiment, computer 20 comprises a thin client where OS 35 is less than a full OS, but rather a kernel that is configured to handle networking and display output, such as on monitor 47.

[0024] FIG. 2 depicts an example system in which embodiments of establishing SSO on a cloud computing platform may be implemented. Computers depicted in FIG. 2 may be implemented in computer 20 of FIG. 1. A SSO system permits a user to log-in once, and from that one log in, gain access to multiple software systems. In an example SSO environment, a user may be initially prompted for credentials (such as login and password), and in response to providing valid credentials, is issued a ticket-granting ticket (TGT, such as a Kerberos ticket). When additional software systems require logging in, those applications query the TGT to acquire service tickets, which prove the user's identity to those software systems without the user logging in again. In versions of the MICROSOFT WINDOWS operating system environment, WINDOWS login fetches the TGT after the user provides credentials to WINDOWS login. Then, ACTIVE DIRECTORY-aware applications may query the TGT for service tickets.

[0025] The general portions of FIG. 2 as depicted are cloud computing platform 204, which is connected via global network 202 to both corporate intranet 218 and computer 222, which is located outside of corporate intranet 218. Computer 222 does not have an on-premises directory service, while corporate intranet 218 does – on-premises directory service 212. Each of computer 222 and corporate intranet 218 may establish a cloud-based SSO.

[0026] A cloud computing platform (such as the MICROSOFT WINDOWS AZURE PLATFORM cloud computing platform) generally provides computing resources to one or more users as a service (as opposed to a physical product). Examples of such services are email services, calendar services, contacts services, web page-hosting services, document storage and management services, and spreadsheet, presentation, and document viewing and editing services, such as offered in versions of MICROSOFT OFFICE 365. As depicted herein, one or more of these services may be provided by cloud services 220 of cloud computing platform 204. A cloud-computing platform may be embodied in a datacenter of computers. Such a platform may comprise one or more gateway computers that serve as an external contact point to the platform, load balancer computers, which balance the load among the computers of the platform, and virtual machine (VM) host computers, which host VMs that are executed on the cloud computing platform. When a user accesses a cloud computing platform, he or she may interact with one or more of the VMs, in which the user's services are processed. These VMs may be migrated among the VM hosts to optimize system performance (such as to load balance, or to bring a VM host offline for maintenance). A user may be unaware of the specific

implementation of a cloud computing platform, and instead be aware of those services that the cloud computing platform provides on top of this unknown system architecture.

[0027] First discussed is establishing a cloud-based SSO for computer 222, which does not have on-premises directory service. A directory service may comprise a database that is used to authenticate users and/or computers within a domain. An example of such a directory service is the MICROSOFT ACTIVE DIRECTORY directory service. As depicted, computer 222 is not associated with corporate intranet 218, and so setting up cloud-based SSO for corporate intranet 218 will not establish SSO for computer 222. A user of computer 222 may connect to cloud computing platform 204 through global network 202 (such as the INTERNET). As depicted, cloud computing platform 204 comprises cloud directory service 206, federation service 208, and synchronization service 210. These services of cloud computing platform 204 are depicted logically, and may be implemented on fewer than (or more than) three computers.

[0028] The user of computer 222 may log in to cloud computing platform 204 by providing a credential (such as login and password) that cloud computing platform 204 validates. Once validated, computer 222 may be presented with a user interface for establishing cloud-based SSO. This user interface may be, for instance, part of a web page that computer 222 displays in a web browser.

[0029] A user may input data into the user interface indicative of a desire to establish cloud-based SSO, and an identification of a domain to be used in establishing SSO. This information may be sent to cloud computing platform 204. In an embodiment, cloud computing platform 204 determines that the domain identified by computer 222 is a private domain (e.g., contoso.local; a private domain is sometimes referred to as a pseudo domain). In another embodiment, cloud computing platform 204 determines that the domain identified by computer 222 is a public domain (e.g., contoso.com).

[0030] Where the domain is a private domain, cloud computing platform 204 may determine that proof of control of the private domain need not be supplied. It may be that proof of control of the domain does not need to be supplied, because, being a private domain, use of it is already limited to an intranet of computer 222.

[0031] Where the domain is a public domain, cloud computing platform 204 may establish proof that the user of computer 222 has control of the public domain. This may be accomplished by cloud computing platform generating and sending data to computer 222 – for instance, the data may comprise a user identifier (UID) associated with the credential provided by computer 222, the UID having a unique value among UIDs on

cloud computing platform 204. This data may be received by computer 222, and then stored in a known, public location on the domain – for instance in a mail exchanger (MX) record, or a domain TXT (text) record on the domain. After the data has been moved to a known location, computer 222 may notify cloud computing platform 204 that this has
5 occurred. In turn, cloud computing platform 204 may retrieve that data that is stored at the known, public location, and verify that that data matches the data that cloud computing platform 204 sent to computer 222. In embodiments where the known, public location is a web server, cloud computing platform 204 may retrieve the data by downloading it via hypertext transfer protocol (HTTP).

10 **[0032]** In these described embodiments, proving control of a domain may be considered proving the ability to store a file at known, public location on a domain.

[0033] Where cloud computing platform 204 has determined that the domain is a private domain, or that the domain is a public domain for which control has been proven, cloud computing platform 204 may then establish cloud-based SSO functionality for the
15 domain. Establishing cloud-based SSO where there is no on-premises directory may comprise standing up a federation service 208 and directory service 206. A federation service may comprise a computer service that facilitates proving identity across software and organizational boundaries (e.g., across multiple software systems executing on a cloud computing platform). A federation service may interact with a directory service such that
20 the directory service authenticates a user initially, and a federation service further authenticates this identity across software or organizational boundaries. A federation service may use claims based authentication whereby a user is authenticated based on a set of claims about the user's identity that are contained within a trusted token (such as one received from a directory service after the user has authenticated to the directory service).
25 An example of a federation service is the MICROSOFT ACTIVE DIRECTORY FEDERATION SERVICE (AD FS) federation service. After cloud-based SSO has been established, computer 222, and other computers on the domain for which computer 222 established SSO, may be logged into, and various software systems offered by cloud-computing platform 204 may be accessed via a single identity/SSO.

30 **[0034]** In addition to establishing a cloud-based SSO where there is no on-premises directory service, FIG. 2 also depicts computers for which cloud-based SSO may be established where an on-premises directory service does exist. As depicted, corporate intranet 218 has on-premises directory service 212 (as well as VPN endpoint 214 and computer 216). On-premises directory service 212 may serve a function similar to cloud

directory service 206: on premise directory service 212 may validate user credentials to access computers and software systems within corporate intranet 218. VPN endpoint 214 may serve as a communications point that is connected to both the intranet of corporate intranet 218 and global network 202. VPN endpoint 214 may serve functionality offered
5 within corporate intranet 218 to computers outside of corporate intranet 218 that are authenticated to VPN endpoint 214. That is, computers authenticated to VPN endpoint 214 may access services and functionality of corporate intranet 218 as if those computers were located within corporate intranet 218.

[0035] Computer 216 of corporate intranet may communicate with cloud
10 computing platform 204 to establish cloud-based SSO in conjunction with on-premises directory service 212. Operations of validating credentials, identifying a domain, and standing up directory service 206 and federation service 208 may be performed similar to as described with respect to establishing cloud-based SSO where there is no on-premises directory service. After credentials have been validated, and a domain has been identified
15 (and control thereof proven, in the case of a public domain), establishing cloud-based SSO with on-premises directory may differ from establishing cloud-based SSO without on-premises directory because the former may involve both replicating data between on-premises directory service 212 and cloud directory service 206.

[0036] Cloud computing platform 204 may initially replicate data from on-
20 premises directory service 212 to cloud directory service 206. After this initial replication, cloud computing platform 204 may replicate data between on-premises directory service 212 and cloud directory service 206 by standing up synchronization service 210. Synchronization service 210 may perform a function of replicating data between cloud directory service 206 and on-premises directory service 212. In addition to this
25 replicating, synchronization service 210 may also perform a function of synchronizing data between on-premises directory service 212 and cloud services 220. Cloud services 220 may comprise a multi-tenant service platform containing applications (e.g. email) and identity infrastructure – such as a multi-tenant directory and an identity service. In embodiments, the operations of replicating data between cloud directory service 206 and
30 on-premises directory service 212 may occur via VPN connection 224. VPN connection 224 may be used because these operations use a protocol not normally available over the INTERNET (such as MICROSOFT ACTIVE DIRECTORY directory service's replication protocol). In embodiments, the operations of synchronizing data between on-premises directory service 212 and cloud services 220 may occur via a non-VPN

connection. A non-VPN connection may be used because the protocols used for these operations are normally available over the INTERNET (such as through a public web services interface).

5 [0037] In addition to standing up synchronization service 210, cloud computing platform 204 may prompt computer 216 to provide a credential that may be used to access both corporate intranet 218 and on-premises directory service 212. This may be a single credential that may be used to access both corporate intranet 218 and on-premises directory service 212 on-premises.

10 [0038] Cloud computing platform may establish a VPN connection 224 with VPN endpoint using the supplied credential, and use this connection as well as the credential(s) to access on-premises directory service 206. Note that in embodiments, some communications between corporate intranet 218 and cloud computing platform 204 may occur on a network connection that is not a VPN connection. Then, synchronization service 210 may replicate data between cloud directory service 206 and on-premises directory service 212. Thus, the SSO functionality provided by on-premises directory service 206 within corporate intranet 218 is extended to cloud directory service 206 and software systems provided by cloud computing platform 204.

15 [0039] FIG. 3 depicts example operating procedures for establishing SSO on a cloud computing platform. It may be appreciated that there are embodiments of the invention that do not implement all of the operations depicted in FIG. 3 (or FIGs. 4-6), and embodiments of the invention that implement the operations depicted in FIG. 3 (or FIGs. 4-6) in a different order than as depicted herein. The operations of FIG. 3 may be implemented, for instance, on cloud computing platform 204 of FIG. 2.

20 [0040] Operation 302 depicts validating a user credential. In an embodiment, this user credential may be a credential received from a computer (such as computer 222 or computer 216), and thus, may comprise validating a user credential associated with a computer.

25 [0041] Operation 304 depicts receiving an identification of a domain for which SSO is to be established. This indication may be received from the computer that proffered the user credential identified in operation 302. For example, cloud computing platform 204 may provide a user interface to computer 216 or computer 222 via a web page, and data may be input into that web page that identifies a domain for which SSO is to be established.

[0042] Operation 306 depicts configuring the cloud computing platform to authorize sign-ons from users of the domain. Operation 306 may be performed where the user credential has been validated in operation 302. Operation 306 may comprise configuring a directory service and a federation service on the cloud computing platform for users of the domain.

[0043] Operation 308 depicts authorizing a log in to a computer of the domain based on determining that the directory service authorizes a credential associated with the log in. In embodiments, operation 308 comprises determining to permit a log in to a second computer in response to determining that the directory service authorizes a credential associated with the log in.

[0044] Operation 310 depicts authorizing the credential associated with the log in to access a software service provided on the cloud computing platform. Operation 310 may be performed in response to determining that the directory service authorized the credential associated with the log in.

[0045] FIG. 4 depicts additional example operating procedures for establishing SSO on a cloud computing platform with a public domain. In embodiments where the operational procedures of FIG. 4 are performed in conjunction with the operational procedures of FIG. 3, the operational procedures of FIG. 4 (which may be used to determine that the requestor has control of the domain in question) may be implemented before operation 306 (where the cloud computing platform may be configured to authorize sign-ons from the domain).

[0046] Operation 402 depicts determining that the domain is a public domain. This may comprise parsing the providing domain (e.g., contoso.com) to determine that the domain contains a top-level domain (e.g., .COM or .NET) that is publicly available (as opposed to, for example, a private top-level domain, like .LOCAL).

[0047] Operation 404 depicts sending a data to the computer. Operation 404 may be performed in response to determining that the domain is a public domain. Where, instead, it is determined that the domain is a private domain, the operational procedures of FIG. 5 may be implemented. The data may comprise information that may be stored in the domain in a known, publicly-accessible (or, otherwise accessible, with the use of credentials provided to cloud computing platform 204) location. For instance, where cloud computing platform 204 maintains a user identifier (UID) for each user of cloud computing platform 204, and the value stored in these UIDs is unique among UIDs, cloud computing platform 204 may send this UID to the computer as the data. In response to

receiving the data, the computer may then store the data at a known, publicly-accessible location within the domain.

[0048] Operation 406 depicts determining that the data is accessible at a known location in the domain. In embodiments, operation 406 comprises determining that the data is stored within a mail exchanger (MX) record in the domain, or determining that the data is stored within a domain TXT record (text record) in the domain. Where the data is stored on a web server, operation 406 may comprise cloud computing platform 204 making a hypertext transfer protocol (HTTP) request to retrieve what data is stored at the known location. Then, cloud computing platform 204 may compare this retrieved data with the data it provided the computer in operation 404 and determine whether the values match (indicating that the requestor has access to or control of the domain) or the values differ (indicating that the requestor has not shown sufficient access to or control of the domain to merit establishing cloud-based SSO for that domain).

[0049] FIG. 5 depicts additional example operating procedures for establishing SSO on a cloud computing platform with a private domain. In embodiments where the operational procedures of FIG. 5 are performed in conjunction with the operational procedures of FIG. 3, the operational procedures of FIG. 5 (which may be used to determine that the requestor has control of the domain in question) may be implemented before operation 306 (where the cloud computing platform may be configured to authorize sign-ons from the domain).

[0050] Operation 502 depicts determining that the domain is a private domain. This may comprise parsing the provided domain (e.g., contoso.com) to determine that the domain contains a private top-level domain (e.g., .LOCAL) that is not publicly available (as opposed to, for example, a publicly-available top-level domain, like .COM or .NET).

[0051] Operation 504 depicts determining that control of the domain need not be proven. Where the domain is a private domain, control of the domain may be inferred by virtue of the domain being private – e.g., since the private domain is local to the intranet on which it exists, control of it may be inferred. Thus, where the domain is a private domain, cloud computing platform 204 may determine that no additional proof of control of the domain is necessary (such as via the operational procedures of FIG. 4), and cloud computing platform may then begin configuring the cloud computing platform to authorize sign-ons from users of the private domain.

[0052] FIG. 6 depicts additional example operating procedures for establishing SSO on a cloud computing platform where there is on-premises directory. In

embodiments, the operational procedures of FIG. 6 may be used to establish SSO on cloud computing platform 204 for corporate intranet 218, which has on-premises directory 212.

5 **[0053]** Operation 602 depicts determining that the domain has an on-premises directory service. In embodiments, operation 602 may comprise prompting the entity that has requested establishing cloud-based SSO for an indication of whether or not the entity has on-premises directory service. For instance, where cloud computing platform 204 provides a user interface in a web page to computer 216, this user interface may also contain user interface elements that are configured to allow for the indication of whether there is on-premises directory.

10 **[0054]** Operation 604 depicts, configuring a synchronization service on the cloud computing platform. This synchronization service may be used both for replicating data between the on-premises directory service and the cloud computing platform, and for synchronizing data between the on-premises directory service and the cloud services on the cloud computing platform. Operation 604 may be performed in response to
15 determining that the domain has the on-premises directory service. Where the domain does not have on-premises directory service, cloud computing platform 204 may determine not to configure a synchronization service in conjunction with establishing cloud-based SSO.

[0055] Operation 606 depicts receiving an indication of a virtual private network (VPN) endpoint and a credential to access the on-premises directory service. Using the
20 example system of FIG. 2, this VPN endpoint may be VPN endpoint 218. Where cloud computing platform 204 provides a user interface in a web page to computer 216, as in operation 602, this user interface may also comprise user interface elements that are configured for inputting credentials for the VPN endpoint and on-premises directory
25 service.

[0056] Operation 608 depicts establishing, by the cloud computing platform, a VPN connection with the VPN endpoint, using the credential to access the on-premises directory service. Once the VPN connection is established, synchronization service 210 may both replicate data between the on-premises directory service 212 and cloud directory
30 service 206, and synchronize data between on-premises directory service 212 and cloud services 220, as depicted in operation 610.

[0057] This establishment of a VPN connection from cloud computing platform 204 to corporate intranet 218 may be considered to be establishing a VPN connection in the opposite direction of a more typical VPN connection. In a more typical scenario,

computer 222 may initiate a VPN connection with corporate intranet 218 to extend the functionality provided by corporate intranet 218 to computer 222. In contrast, here, cloud computing platform 204 is initiating a VPN connection with corporate intranet 218 to extend the functionality provided by cloud computing platform 204 to corporate intranet 218. That is, instead of computer 222 establishing a VPN connection to increase the functionality that it receives from corporate intranet 218, cloud computing platform 204 is establishing a VPN connection to increase the functionality that is provided to corporate intranet 218 (this functionality including cloud-based SSO that extends to software systems provided by cloud computing platform 204, for which credentials are required).

10 **[0058]** Operation 610 depicts replicating data between the directory service on the cloud computing platform and the on-premises directory service using the synchronization service. As data is modified on either cloud directory service 206 or on-premises directory service 212 (e.g., a new user account is created on one of these directory services), synchronization service 210 may monitor these directory services for modifications, and where synchronization service 210 detects such a modification, it may modify the other directory service accordingly, so that directory service 206 and on-premises directory service 212 contain the same SSO information.

15 **[0059]** While the present invention has been described in connection with the preferred aspects, as illustrated in the various figures, it is understood that other similar aspects may be used or modifications and additions may be made to the described aspects for performing the same function of the present disclosure without deviating there from. Therefore, the present disclosure should not be limited to any single aspect, but rather construed in breadth and scope in accordance with the appended claims. For example, the various procedures described herein may be implemented with hardware or software, or a combination of both. The invention may be implemented with computer-readable storage media and/or computer-readable communication media. Thus, the invention, or certain aspects or portions thereof, may take the form of program code (i.e., instructions) embodied in tangible media, such as floppy diskettes, CD-ROMs, hard drives, or any other machine-readable storage medium. Likewise, the invention, or certain aspects or portions thereof, may be embodied in propagated signals, or any other machine-readable communications medium. Where the program code is loaded into and executed by a machine, such as a computer, the machine becomes an apparatus configured for practicing the disclosed embodiments. In addition to the specific implementations explicitly set forth herein, other aspects and implementations will be apparent to those skilled in the art from

consideration of the specification disclosed herein. It is intended that the specification and illustrated implementations be considered as examples only.

What is Claimed:

1. A method for establishing single identity on a cloud computing platform, comprising:
 - validating a user credential associated with a computer;
 - 5 receiving an identification of a domain for which single identity is to be established from the computer;
 - in response to validating the user credential, configuring a directory service on the cloud computing platform for sign-ons from users of the domain;
 - determining to permit a log in to a second computer in response to determining that
10 the directory service authorizes a credential associated with the log in; and
 - authorizing the credential associated with the log in to access a software service provided on the cloud computing platform in response to determining that the directory service authorized the credential associated with the log in.
2. The method of claim 1, further comprising:
 - 15 determining that the domain has an on-premises directory service;
 - in response to determining that the domain has the on-premises directory service, configuring a synchronization service on the cloud computing platform for replicating data between the directory service on the cloud computing platform and the on-premises directory service;
 - 20 receiving an indication of a virtual private network (VPN) endpoint and a credential to access the on-premises directory service;
 - establishing, by the cloud computing platform, a VPN connection with the VPN endpoint, using the credential to access the on-premises directory service; and
 - replicating credential data between the directory service on the cloud computing
25 platform and the on-premises directory service using the synchronization service.
3. The method of claim 1, wherein configuring the directory service on the cloud computing platform for sign-ons from users of the domain further comprises:
 - configuring a federation service on the cloud computing platform for users of the domain.
- 30 4. The method of claim 1, wherein configuring the directory service on the cloud computing platform for sign-ons from users of the domain comprises:
 - determining that the domain is a public domain;
 - in response to determining that the domain is a public domain, sending data to the computer;

determining that the data is accessible at a known location in the domain;

5. The method of claim 4, wherein determining that the data is accessible at the known location in the domain comprises:

5 determining that the data is stored within a mail exchanger (MX) record in the domain.

6. The method of claim 4, wherein determining that the data is accessible at the known location in the domain comprises:

determining that the data is stored within a domain TXT record (text record) in the domain.

10 7. The method of claim 1, wherein configuring the directory service on the cloud computing platform for sign-ons from users of the domain comprises:

determining that control of the domain need not be proven in response to determining that the domain is a private domain.

15 8. A system for establishing single identity on a cloud computing platform, comprising:

a processor; and

a memory communicatively coupled to the processor when the system is operational, the memory bearing processor-executable instructions that, when executed on the processor, cause the system to at least:

20 validate a user credential associated with a computer;

receive an identification of a domain for which single identity is to be established from the computer;

in response to validating the user credential, configure a directory service on the cloud computing platform for sign-ons from users of the domain;

25 determine to permit a log in to a second computer in response to determining that the directory service authorizes a credential associated with the log in; and

30 authorize the credential associated with the log in to access a software service provided on the cloud computing platform in response to determining that the directory service authorized the credential associated with the log in.

9. The system of claim 8, wherein the memory further bears processor-executable instructions that, when executed on the processor, cause the system to at least:

determine that the domain has an on-premises directory service;

in response to determining that the domain has the on-premises directory service, configure a synchronization service on the cloud computing platform for replicating data between the directory service on the cloud computing platform and the on-premises directory service;

5 receive an indication of a virtual private network (VPN) endpoint and a credential to access the on-premises directory service;

establish, by the cloud computing platform, a VPN connection with the VPN endpoint, using the credential to access the on-premises directory service; and

10 replicate credential data between the directory service on the cloud computing platform and the on-premises directory service using the synchronization service.

10. The system of claim 8, wherein the instructions that, when executed on the processor, cause the system to at least configure the directory service on the cloud computing platform for sign-ons from users of the domain further cause the system to at least:

15 configure a federation service on the cloud computing platform for users of the domain.

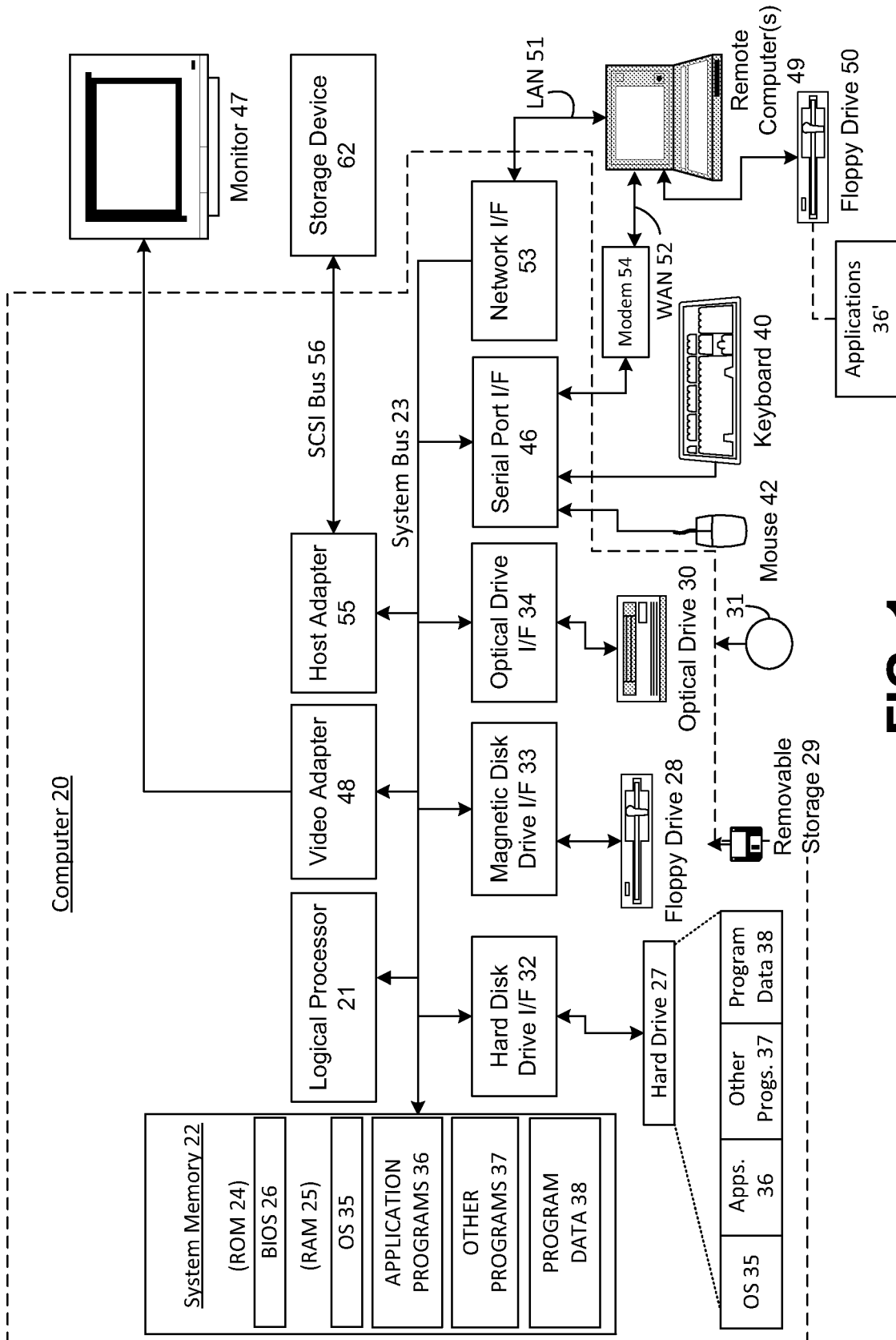


FIG. 1

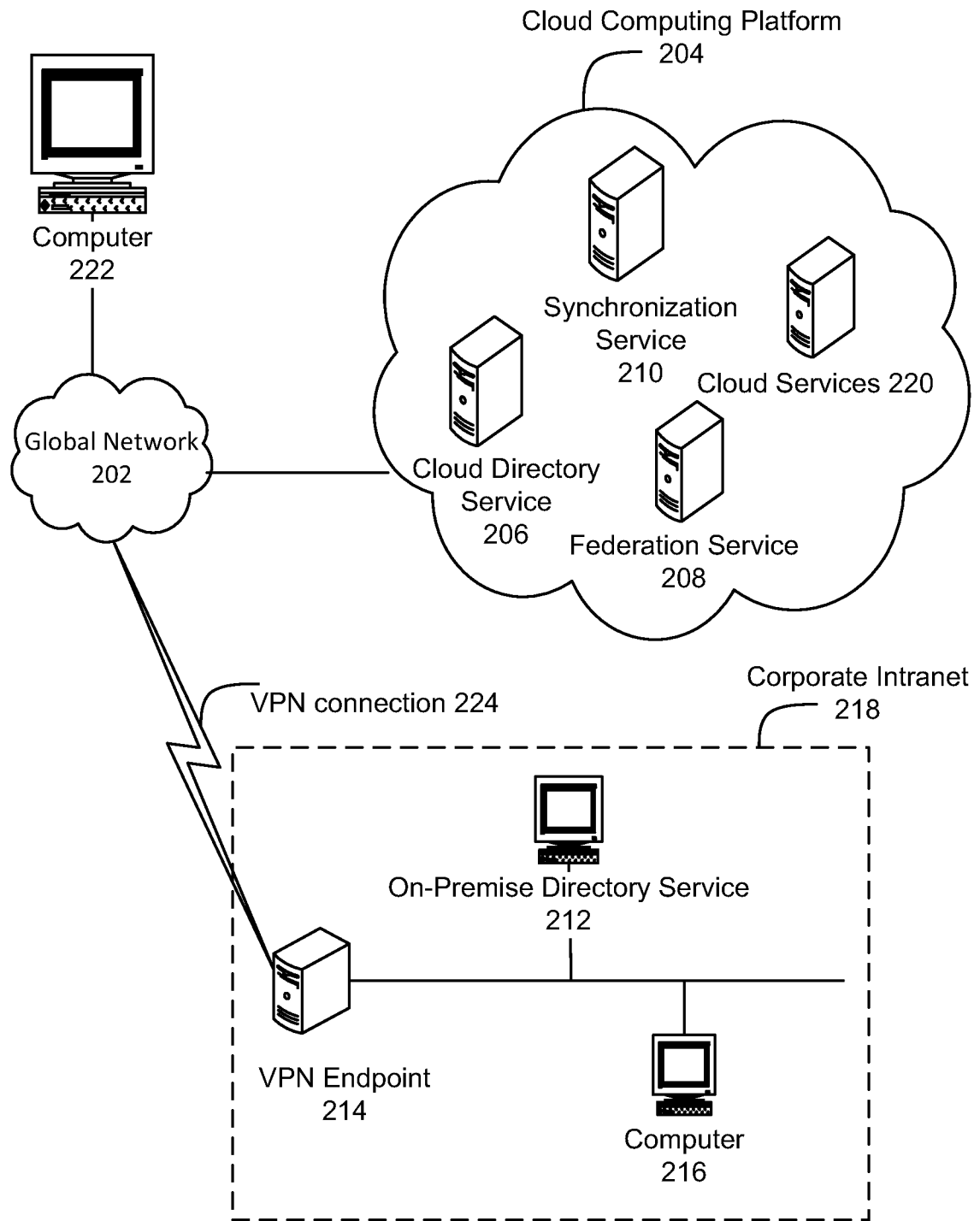
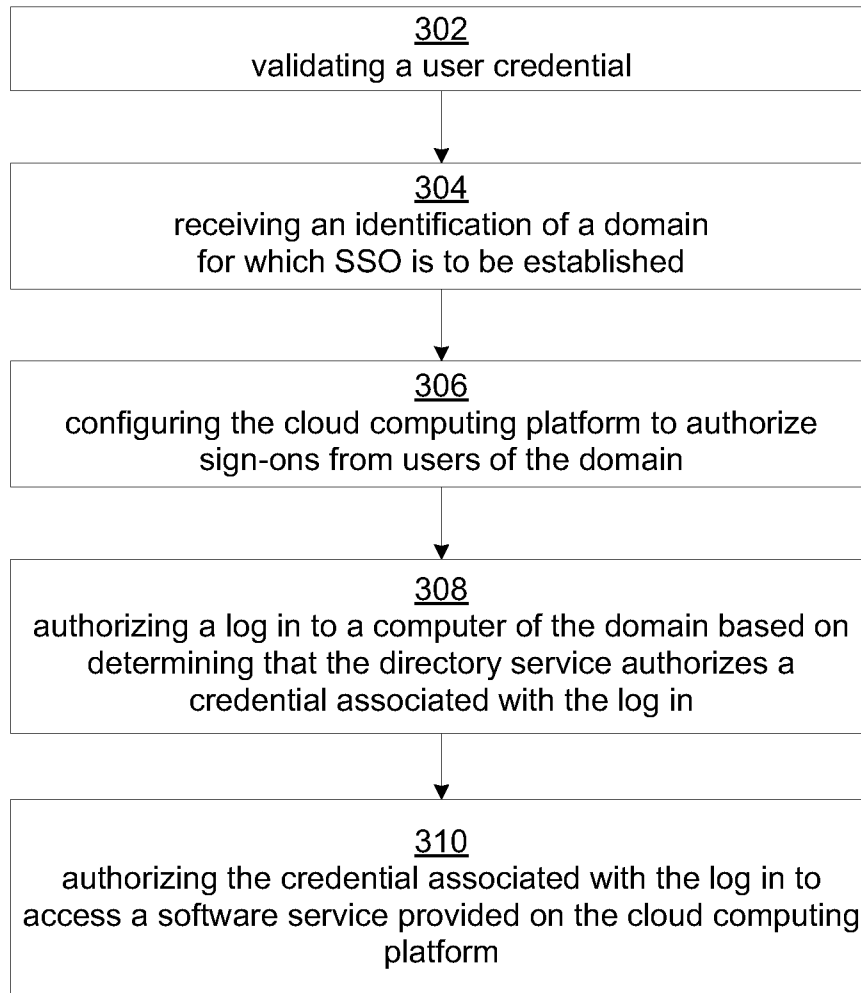


FIG. 2

3/5

**FIG. 3**

4/5

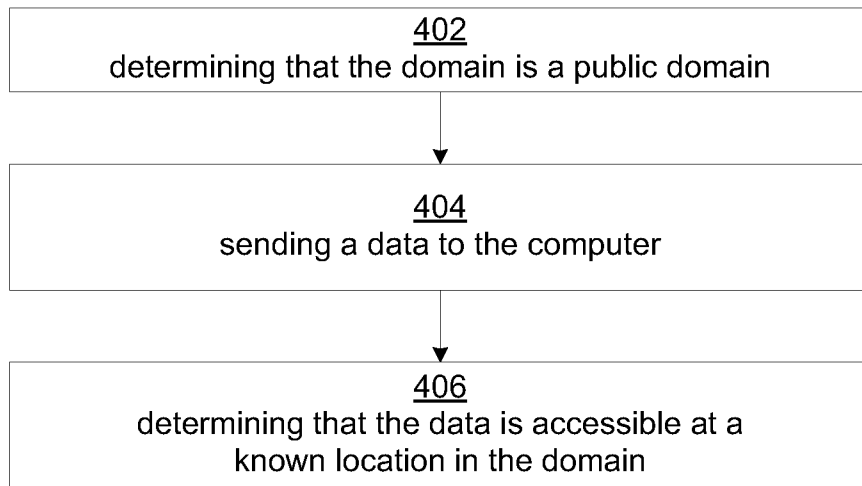


FIG. 4

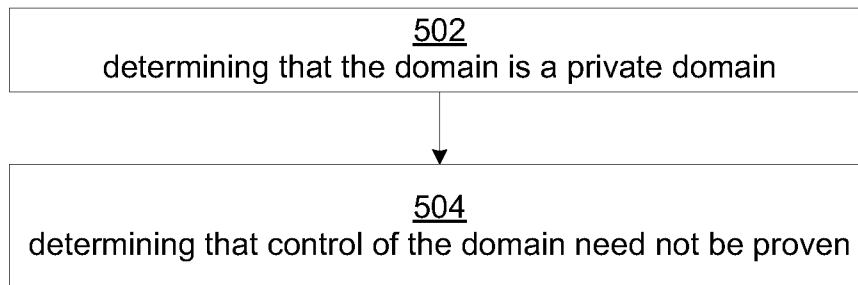


FIG. 5

5/5

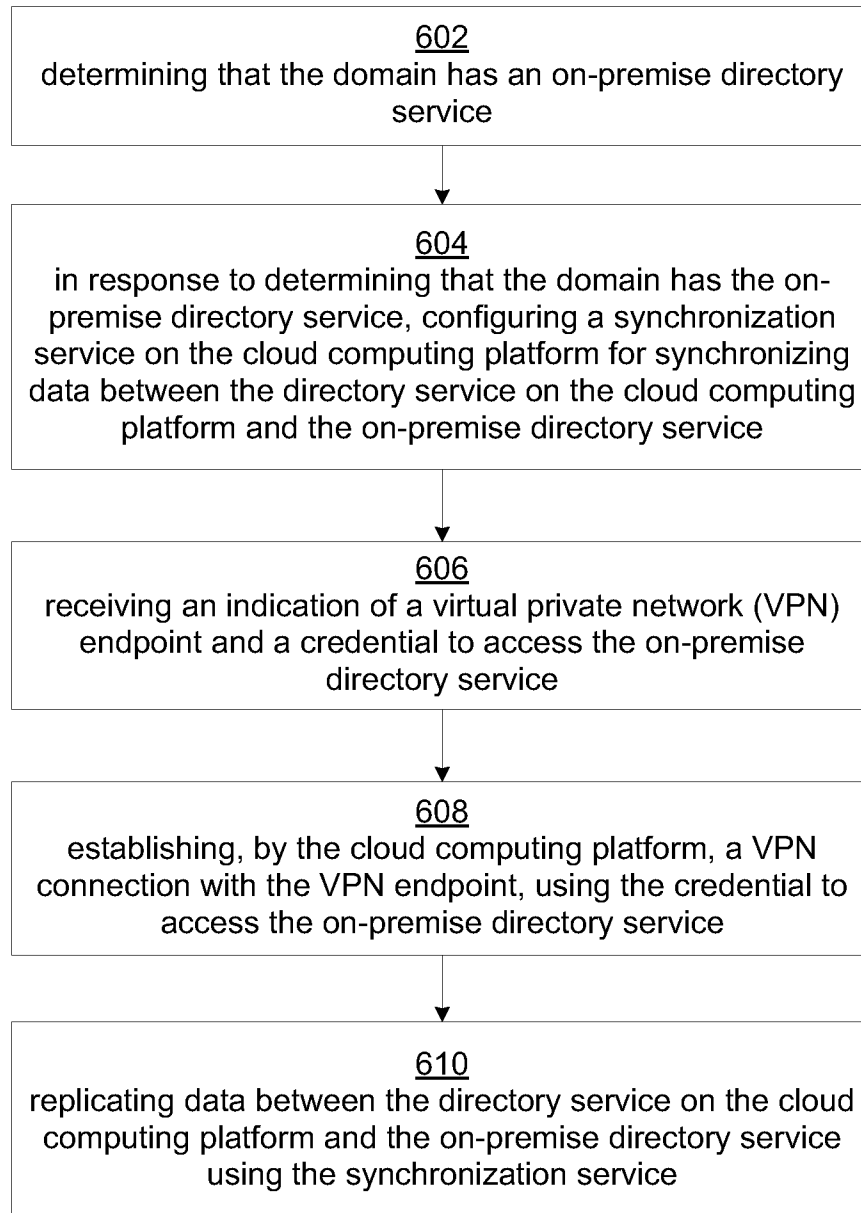

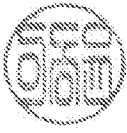


FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/028121

A. CLASSIFICATION OF SUBJECT MATTER		
H04L 9/32(2006.01)i, G06F 21/31(2013.01)i		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) H04L 9/32; G06F 7/04; H04L 9/00; H04K 1/00		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Korean utility models and applications for utility models Japanese utility models and applications for utility models		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) eKOMPASS(KIPO internal) & Keywords: single sign-on, on-premises directory service, cloud, token, pseudo domain		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2008-0059804 A1 (TOGENDRA C. SHAH et al.) 06 March 2008 See paras. 77-85, 88-94; claim 1; and figs. 8-11.	1,3,8,10
A		2,4-7,9
Y	US 2011-0307947 A1 (ASAF KARIV et al.) 15 December 2011 See paras. 23, 31, 50-51, 55-56; claim 1; and figs. 2-4.	1,3,8,10
A	US 2007-0083750 A1 (TAKAYUKI MIURA et al.) 12 April 2007 See paras. 128-134, 242-247; claim 1; and fig. 3.	1-10
A	US 2010-0229224 A1 (CRAIG S. ETCHEGOYEN) 9 September 2010 See paras. 64-71; claim 1; and figs. 6A-10.	1-10
A	US 2005-0278547 A1 (ARN HYNDMAN et al.) 15 December 2005 See paras. 29-39, 58-62; claim 1; and figs. 2-3.	1-10
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of 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 30 May 2013 (30.05.2013)		Date of mailing of the international search report 03 June 2013 (03.06.2013)
Name and mailing address of the ISA/KR  Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140		Authorized officer LEE, Dong Yun Telephone No. 82-42-481-8734 

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2013/028121

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008-0059804 A1	06.03.2008	EP 2055077 A1	06.05.2009
		JP 2010-502109 A	21.01.2010
		KR 10-1005910 B1	06.01.2011
		KR 10-2009-0042864 A	30.04.2009
		KR 10-2009-0048655 A	14.05.2009
		TW 200820716 A	01.05.2008
		TW 200943898 A	16.10.2009
		TW 201141176 A	16.11.2011
		WO 2008-024454 A1	28.02.2008
		US 2011-0307947 A1	15.12.2011
US 2007-0083750 A1	12.04.2007	EP 1662691 A1	31.05.2006
		EP 1662691 A4	09.04.2008
		JP 04617763 B2	05.11.2010
		JP 2005-102163 A	14.04.2005
		KR 10-2006-0101454 A	25.09.2006
		US 7797532 B2	14.09.2010
		WO 2005-025125 A1	17.03.2005
US 2010-0229224 A1	09.09.2010	EP 2396742 A2	21.12.2011
		WO 2010-093683 A2	19.08.2010
		WO 2010-093683 A3	07.10.2010
US 2005-0278547 A1	15.12.2005	None	