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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 December 2016 (08.12.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/192765 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04L 12/24* (2006.01)

(21) International Application Number:
PCT/EP2015/062048

(22) International Filing Date:
29 May 2015 (29.05.2015)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **LONGSAND LIMITED** [GB/GB]; Autonomy House, Cambridge Business Park, Cowley Road, Cambridge CB4 0WZ (GB).

(72) Inventors: **SHELTON, Stuart**; c/o Autonomy House, Cambridge Business Park, Cowley Road, Cambridge, Cambridgeshire CB4 0WZ (GB). **ANGELI, Christakis**; c/o Autonomy House, Cambridge Business Park, Cowley Road, Cambridge, Cambridgeshire CB4 0WZ (GB). **BORSARO, Daniele**; c/o Autonomy House, Cambridge Business Park, Cowley Road, Cambridge, Cambridgeshire CB4 0WZ (GB).

(74) Agent: **EIP**; Fairfax House, 15 Fulwood Place, London WC1V 6HU (GB).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU,

[Continued on next page]

(54) Title: AUTHENTICATION AND AUTHORIZATION BASED ON CREDENTIALS AND TICKET

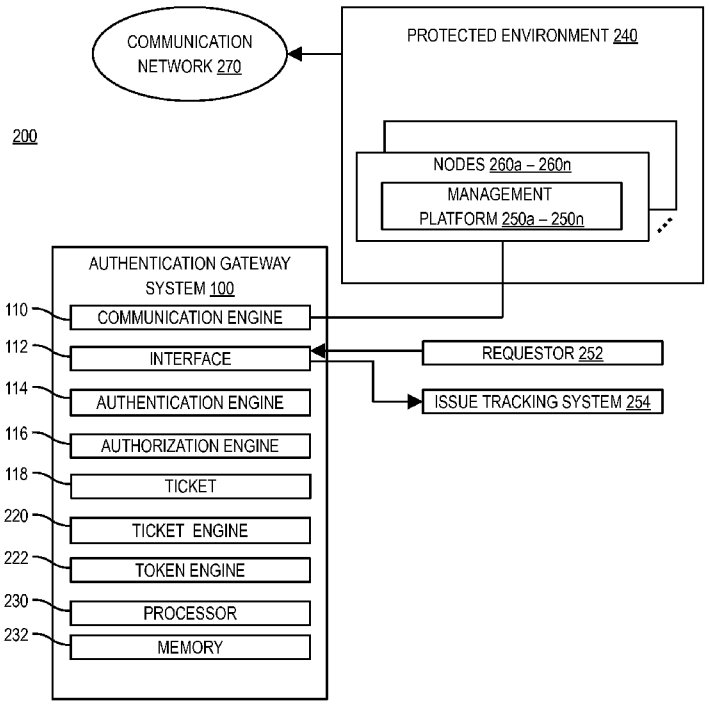

FIG. 2

(57) Abstract: Example embodiments disclosed herein relate to determining permissions to grant for access to a management platform (250a-250n). In one example, a device is connected to a protected environment (240) via a management plane (110). Access to the management platform (250a-250n) can be provided. A request is received for access to the management platform (250a-250n). The request includes credentials of a requestor (252). The credentials are authenticated. The permissions to grant for access to the management platform (250a-250n) is based on the authenticated credentials and a ticket (118).

WO 2016/192765 A1

TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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

AUTHENTICATION AND AUTHORIZATION BASED ON CREDENTIALS AND TICKET

BACKGROUND

[0001] Cloud and traditional data center back-end environments may communicate with other devices (e.g., via the Internet). These types of environments are targets for various types of attacks. Attacks can lead to loss of data, loss of availability of access to nodes in an environment, etc. As such, maintaining security on such environments can be advantageous.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] The following detailed description references the drawings, wherein:

[0003] FIG. 1 is a block diagram of an authentication gateway system for determining permissions to grant for access to a management platform based on a ticket, according to an example;

[0004] FIG. 2 is a block diagram of a system including authentication gateway system for determining permissions to grant for access to a management platform based on a ticket, according to an example;

[0005] FIG. 3 is a flowchart of a method for determining permissions to grant for access to a management platform based on a ticket, according to an example;

[0006] FIG. 4 is a block diagram of a block diagram of a device capable of determining permissions to grant for access to a management platform based on a ticket, according to an example; and

[0007] FIG. 5 is a flowchart of a method for facilitating access to management platforms, according to an example.

DETAILED DESCRIPTION

[0008] Cloud and traditional data center back-end environments may communicate with other devices (e.g., via the Internet). These types of environments are targets for various types of attacks. Attacks can lead to loss of data, loss of availability of access to nodes in an environment, etc. Various approaches can be used to help secure the environments. Most of the approaches, such as web application firewalls, Intrusion Prevention Systems, etc. rely on attempting to stop intruders from entering the network.

[0009] However, effective security within a computer system can be challenging to achieve because a potential attacker or malicious administrator may already be in position to have permitted access to the system. For example, in many cases, an administrator may have root access to each system in an environment, even if the administrator does not need the access for tasks the administrator is to perform. However, environment-level access controls should allow the environment to continue to be accessible and usable by non-malicious authorized users.

[0010] Accordingly, various embodiments disclosed herein relate to authorizing authenticated users with permissions to perform particular tasks. As used herein, the term “authentication” refers to the process of ascertaining that a user is who the user claims to be. Further, as used herein, the term “authorization” refers to rules or permissions to determine what users are allowed to do/access.

[0011] Approaches described herein separate authentication from authorization by having authorizations governed by duties an authenticated user is tasked to perform. An authorization gateway can sit between administrative and/or operations users and an environment protected by the authorization gateway. The authorization gateway can be used to enforce access-restrictions and privileges upon the back-end environment. A ticket system can be used to determine what tasks are to be completed. Authenticated users set to perform the tasks can be provided permissions associated with the respective tasks. A time limit (e.g., a time period, a single session, etc.) can be associated with the

permissions. As used herein a ticket is an identifier associated with a task to be completed related to a protected environment. The ticket can be initiated by a ticketing and/or issue tracking system. The ticket can be formatted in various data structures. For example, a ticket residing on a ticketing and/or issue tracking system may include the identifier and the task while a ticket residing at an authentication gateway may include the identifier and other information associated with the identifier (e.g., an abstraction of the task(s) related to permissions).

[0012] Management platforms of nodes in the protected environment can be connected to the authorization gateway directly or indirectly. The management platforms of the nodes can be segregated from access via other network infrastructures. For example, nodes may be connected to other networks (e.g., an enterprise intranet, the Internet, etc.) via one network connection for normal use (e.g., as a web server) and an associated management platform of the node can be connected via a separate network connection.

[0013] FIG. 1 is a block diagram of an authentication gateway system for determining permissions to grant for access to a management platform based on a ticket, according to an example. FIG. 2 is a block diagram of a system including authentication gateway system for determining permissions to grant for access to the management platform(s) based on tickets, according to an example.

[0014] The authentication gateway system 100 can include a communication engine 110 to communicate with management platform(s) 250a – 250n, an interface 112 to communicate with a user requestor(s) 252 requesting access to the respective management platform(s) 250a – 250n, an authentication engine 114 to authenticate the requestors 252, and an authorization engine 116 to determine permissions to authorize the requestors with based on a ticket 118 or multiple tickets. The management platforms 250a – 250n can be associated with respective nodes 260a – 260n in a protected environment 240.

[0015] The protected environment 240 can be an environment with particular security features. The protected environment 240 can be implemented as a

protected network where the authentication gateway system 100 (or multiple similar systems) are the access points to the management platforms 250 on the nodes 260. A physical or logical sub-network can be implemented for these communications. As such, the authentication gateway system 100 can be implemented as a jump server. In one example, the authentication gateway system 100 can be implemented as a hardened machine using an operating system such as Unix, Linux, etc. configured with a secure shell (SSH) interface and a local firewall. The jump server implementation can allow for a single audit point for traffic connecting to the management platforms 250. Logs can be maintained for actions taken and/or key logging. In some examples, the management platforms can be restricted to a management plane of communication, either physical or logical. A management plane is a part of a network that carries traffic that is to configure, maintain, and/or manage nodes. Further, in these examples, the authentication gateway system 100 can be located in a path between a network with users (e.g., the requestor 252) to access the management platforms 250 and the management platforms 250. In some examples, the protected environment 240 may include tiers (e.g., access to a particular management platform 250 goes through another management platform).

[0016] In some examples, other interfaces of the nodes 260 of protected environment 240 may be available via a communication network 270 (e.g., an Intranet or perimeter network). In some examples, some or all of the nodes of the protected environment 240 may not be connected to the communication network 270. In some examples, the interfaces to the communication network 270, other than via the authentication gateway system 100, can be limited to outbound communications initiated by nodes 260 in the protected environment 240. As used herein, outbound communications are communications that are initiated from within the protected environment 240. Information can be received in response to an initiated communication (e.g., the host receiving the communication can respond to the initiated communication). In some examples, additional protections may be included, for example, outbound communications may be allowed for a whitelist of addresses and not allowed for non-whitelisted systems. Further, as used herein, inbound communications are

communications that are initiated from outside of the protected environment 240. It can be desirous to limit inbound communications to coming via the authentication gateway system 100.

[0017] In some examples, a connection (e.g., an SSH connection) can be created from the requestor 252 and the authentication gateway system 100 (e.g., at interface 112). The connection can be forwarded using SSH forwarding to the associated management platform 250. The connection is based on authentication and authorization. In some examples, the interface 112 can be limited to accepting communications on particular ports (e.g., one port). As such, the interface can be open on one network port and closed on other network ports in a network connecting the requestor 252 to the interface 112. This can reduce the possible attack surface of the interface.

[0018] The management platforms 250a – 250n can provide node level and/or out-of-band or remote management functionality to their respective nodes 260a – 260n. Examples of out-of-band management functionality can include resetting a node 260, viewing hardware logs on a node 260, configuration of hardware of the node 260, emergency access to system consoles, etc. In some examples, node level management functionality includes rebuilding a database, updating software, patching software, viewing software logs, configuration and/or rebooting of virtual machines, etc. Examples of types of tasks that can be performed include security tasks, maintenance tasks, upgrade tasks, troubleshooting tasks, etc. In some examples, a mapping can be maintained of tasks and permissions associated with performing the tasks. The mapping can be pre-determined and may be updated. Further, in some examples, additional permissions may be granted via the ticketing system (e.g., as content included with the ticket). In these examples, additional permissions may be added to a user by a person that has particular access to the ticketing system. In some examples, the person that has particular access to the ticketing system can be disallowed in the system from providing permissions to the person. Further, in some examples, the person may also be limited from being able to authenticate to the authentication gateway system 100 to limit the possibility of unauthorized access by the person.

[0019] When a requestor 252 requests access to a particular management platform 250, the authentication engine 114 can authenticate the requestor 252. The requestor 252 can be a user, a user's terminal or computer, etc. For authentication, the requestor 252 can provide information, such as a username and password, a token, etc. In some examples, an internal authentication database (e.g., a Lightweight Directory Access Protocol (LDAP) server) populated with end-user details of possible requestors can be used. Further, in some examples, a Kerberos Key Distribution Centre or other single sign-on technology can be used to authenticate users into the protected environment 240.

[0020] Once authenticated by the authentication engine 114, the authorization engine 116 can determine what access to provide to the requestor 252. As noted, the access provided can be particular to a task associated. In one example, a ticket server can be used to issue a ticket 118 associated with one or more tasks to be accomplished.

[0021] The ticket server can be part of the authentication gateway system 100 or be a separate component. The ticket server can be considered an issue tracking system 254. When an issue occurs, a ticket 118 can be generated. In some examples, nodes 260a – 260n may automatically send a message to create a ticket 118 is an error occurs. In other examples, a user can enter data into the issue tracking system 254.

[0022] The ticket 118 can be provided to the authentication gateway system 100 (e.g., via the interface 112). In some examples, the authentication gateway system 100 is configured to allow an outbound connection to the issue tracking system 254. The ticket can include information about the particular problem, the status of the problem, and other relevant data. The ticket engine 220 can maintain information associated with the ticket 118. In some examples, the permissions are included in the ticket 118. In other examples, the ticket 118 can be associated with one or more tasks. These tasks can be mapped to permissions. Thus, the ticket engine 220 can be used to help determine the permissions from the tasks. In one example, the mapped permissions can be pre-set for various tasks in the issue tracking system 254. For example, a task

to find an error on a node 260a may be associated with permissions to access the log of node 260a. In another example, a security issue associated with three nodes 260 may be associated with permissions for accessing logs and/or patching capabilities on each of the three nodes 260. The issue tracking system 254 may provide or facilitate some of the actions performed by the ticket engine 220 (e.g., via a server/client relationship).

[0023] Further, in some examples, a component related to the ticket engine 220 may be present on the individual nodes. The component can be used to initiate a ticket (e.g., if a fault occurs on the node). In one example, the component can provide directly to the ticket engine 220 a ticket and/or task to be completed. In another example, the component may recognize an error or task to complete and send a communication to the issue tracking system 254 to initiate a ticket.

[0024] Further, in some examples, a user with higher authority (e.g., a user of the issue tracking system 254 with management level authority) may be able to set one or more privileges associated with a ticket or task. In further examples, the authentication gateway system 100 can implement a rule that a user is not authorized to provide privileges to themselves. The issue tracking system 254 can be separate from the authentication gateway system 100. For example, a user with management level authority in the issue tracking system 254 may not be permitted to also receive permissions from the authentication gateway system 100. This can be used to ensure that a user does not have the capability to provide permissions to themselves and to ensure that permissions are based on task.

[0025] In one example, to find a ticket 118 associated with the requestor 252, the interface 112 may be used to ask for a ticket identifier (e.g., a number). The requestor 252 can provide the ticket identifier, and the ticket identifier can be used by the ticket engine 220 to identify the ticket 118. In another example, the ticket engine 220 can retrieve or be provided tickets from a ticket server. In some examples, the tickets 118 can be associated with particular accounts or users. As such, when a user requestor 252 is authenticated 114, tickets

matching the account can be determined and permissions can be provided for one or more of the tasks associated with the ticket(s) 118.

[0026] The authorization engine 116 can determine permissions to grant the requestor 252 for access based on the authenticated credentials and the associated ticket(s) 118. As noted, the permissions can be determined based on the ticket(s) 118. Once a ticket 118 is identified, the authorization engine 116 can determine what permissions are associated based on a mapping of tasks to associated permissions and/or based on additional information provided with the ticket 118. In some examples, the authorization engine 116 can work with counterparts (e.g., information on the issue tracking system 254, information received from the nodes 260, etc.) to verify permissions.

[0027] In some examples, the authorization engine 116 can also use a token engine 222 to encode information about the requestor and the permissions into a token. The token can also be encrypted. Further, the token may include information about the authentication gateway system 100 that authenticated the requestor 252. The permissions may include, for example, the management platform(s) 250 that access should be granted to, permissions granted to the user for the session (e.g., what parts of the management platform 250 that the requestor is granted access/write permissions to), information about the length of the permissions (e.g., a time duration, a single session, etc.). The authorization engine 116 can further use the communication engine 110 to propagate the token to the management platform(s) 250 that are to be accessed by the requestor 252. As such, the communication engine 110 can be used to provide the management platform 250 with the permissions for the credentials provided by the requestor. With the approaches described herein, selected items from ticket 118 and additional information (e.g., authentication of the user) can be encoded together in a single encrypted token. The token can be passed on from the communication engine 110 to respective nodes 260 and/or management platforms 250.

[0028] According to various examples, tokenization is the process of taking data (e.g., the authentication information and permissions data) and replacing it with a surrogate value that can be de-tokenized (e.g., at the management

platforms). A look-up table can be used to de-tokenize a token to determine what permissions to provide to a user.

[0029] Encryption is the process of using a cipher to mathematically transform data. Encrypted data can be transformed back using a key. The management platforms 250 can have access to the key. In some examples, the encrypted token can represent information that the user has been authenticated and has particular permissions. The management platform 250 is capable of decrypting and/or de-tokenizing the token. With this approach, the management platforms 250 can be able to determine what permissions it should provide to the user from the token.

[0030] In some examples, permissions may be tiered. For example, a first set of permissions may be granted. If the requestor 252 is not able to resolve the issue with these permissions (e.g., because of a particular state of the associated node), the particular state can be mapped to additional permissions that can be granted. In other examples, the resolution information can be sent back to the issue tracking system 254 and another ticket 118 can be generated and processed.

[0031] Further, the authentication gateway system 100 can further use the interface 112 and the communication engine 110 to facilitate access to the management platform(s) 250 according to the permissions. Access can be facilitated by using an SSH tunnel to connect the requestor 252 to the management platform 250. The requestor 252 can be associated with a network address on a network. The communication engine 110 can facilitate establishment of a tunnel between the network address and the management platform 250. In some examples, the interface 112 can be in a firewalled non-responsive mode for all but a set number of ports (e.g., 1 port) to connect users such as the requestor 252. Moreover, the communication engine 110 may also include a firewall. Part of the facilitating of access can include punching a hole through the communication engine firewall to create the tunnel to the management platform 250. In one example, the tunnel can be locked-down to solely accept connections from the originating network address of the requestor 252. This can increase a level of protection from a traffic-snooping attack.

[0032] In one example, a firewall associated with the communication engine 110 can be used to prevent the requestor 252 from setting up arbitrary tunnels that could decrease the security of the protected environment 240. A defined set of allowed tunnels can be automatically set up by the communication engine 110 to allow the requestor 252 to perform its tasks.

[0033] Moreover, in some examples, the tunnel can be used for providing shell access, graphical access using a Virtual Network Client (VNC), remote desktop connection, etc. Further, in some examples, the interface can be menu driven. The menu options available can be based on the permissions.

[0034] Also, in certain examples, user access is separated from other user access. As such, one user cannot interfere or snoop on access of another user. However, user and state data can be recorded and shared so that there is a routable path between various instances of access.

[0035] In other examples, multiple management platforms 250 may be accessed by the requestor 252 for performing a task. As such, the interface 112 can receive another request from the requestor 252 to access another management platform (e.g., management platform 250b) from a first management platform 250a. Because the user has already been authenticated, the user need not be authenticated again. In one example, the token including authorization and authentication information can be forwarded to the second management platform 250b and, based on the associated permissions (e.g., whether the second management platform 250b allows the connection), the management platform 250a can facilitate access to the second management platform 250b if proper (e.g., by facilitating a tunnel to the second management platform 250b). Other management platforms can be accessed similarly depending on permissions granted. In some examples, the propagation of the token occurs when the request for access to the particular management platform 250 is made. As such, access to further management platforms 250 can be granted based on permissions. Further, in some examples, the requestor 252 can connect to the management platform 250a via other management platforms (e.g., via 250b). The token can be passed to the management platforms in the path to facilitate generation of a tunnel.

[0036] In some examples, access can be provided through management platforms 250. For example, in a tiered system, a tunnel can be created from the requestor to a first management platform and a further tunnel can be created from a second management platform, through the first management platform, through the authentication gateway system 100 to the requestor 252. The token can be provided to the second management platform to authenticate and authorize access to the second management platform.

[0037] Moreover, multiple tickets 118 may be used for determining permissions for the user. For example, when the requestor 252 is accessing the second management platform 250b, a different ticket 118 may be requested and a different set of authorization can be used/enforced. In some examples, a new token is created when such a request is made. Further in some examples, multiple tickets may be used initially to generate the initial token. Moreover, in some examples, access can be more restrictive. For example, a user may be limited to authorization for one ticket at a time and/or to authorization from one ticket on a particular management platform 250 at a time.

[0038] In one example, a second requestor can request access to the same management platform 250a concurrently with the first requestor 252. The authentication gateway system 100 can authenticate the second requestor with a second ticket and facilitate access to the management platform 250a. The two sessions can be separate with different authorization enforced for the differing sessions.

[0039] Further, in some examples, the actions conducted by a requestor 252 can be tracked. The tracked actions can included into a data structure (e.g., as metadata) and associated with the ticket 118 by the ticket engine 220. The ticket information can be provided back to the ticket server. As such, an administrator, manager, service technician, etc. viewing the ticket can be apprised of the actions taken.

[0040] The engines 110, 114, 116, 220, 222 include hardware and/or combinations of hardware and programming to perform functions provided herein. Moreover, the modules (not shown) can include programing functions

and/or combinations of programming functions to be executed by hardware as provided herein. When discussing the engines and modules, it is noted that functionality attributed to an engine can also be attributed to the corresponding module and vice versa. Moreover, functionality attributed to a particular module and/or engine may also be implemented using another module and/or engine.

[0041] A processor 230, such as a central processing unit (CPU) or a microprocessor suitable for retrieval and execution of instructions and/or electronic circuits can be configured to perform the functionality of any of the engines or modules described herein. In certain scenarios, instructions and/or other information, such as information about tickets 118, can be included in memory 232 or other memory. Input/output interfaces may additionally be provided by the authentication gateway system 100. For example, input devices, such as a keyboard, a mouse, etc. can be utilized to receive input from an environment surrounding the authentication gateway system. Further, an output device, such as a display, can be utilized to present information to users. Examples of output devices include speakers, display devices, amplifiers, etc. Moreover, in certain embodiments, some components can be utilized to implement functionality of other components described herein. Input/output devices such as communication devices like network communication devices or wireless devices can also be considered devices capable of using the input/output interfaces.

[0042] Modules may include, for example, hardware devices including electronic circuitry for implementing the functionality described herein. In addition or as an alternative, each module may be implemented as a series of instructions encoded on a machine-readable storage medium of a computing device and executable by processor 230. It should be noted that, in some embodiments, some modules are implemented as hardware devices, while other modules are implemented as executable instructions.

[0043] The communication network 270 and other networks connecting the protected environment 240, authentication gateway system 100, requestor 252, etc. can use wired communications, wireless communications, or combinations

thereof. Further, communication networks can include multiple sub communication networks such as data networks, wireless networks, telephony networks, etc. Such networks can include, for example, a public data network such as the Internet, local area networks (LANs), wide area networks (WANs), metropolitan area networks (MANs), cable networks, fiber optic networks, combinations thereof, or the like. In certain examples, wireless networks may include cellular networks, satellite communications, wireless LANs, etc. Further, the communication networks can be in the form of a direct network link between devices. Various communications structures and infrastructure can be utilized to implement the communication network(s).

[0044] By way of example, devices can communicate with each other and other components with access to the communication network 270 or other networks via a communication protocol or multiple protocols. A protocol can be a set of rules that defines how nodes of the network interact with other nodes. Further, communications between network nodes can be implemented by exchanging discrete packets of data or sending messages. Packets can include header information associated with a protocol (e.g., information on the location of the network node(s) to contact) as well as payload information.

[0045] FIG. 3 is a flowchart of a method for determining permissions to grant for access to a management platform based on a ticket, according to an example. FIG. 4 is a block diagram of a block diagram of a computing device capable of determining permissions to grant for access to a management platform based on a ticket, according to an example.

[0046] Although execution of method 300 is described below with reference to computing device 400, other suitable components for execution of method 300 can be utilized (e.g., authentication gateway system 100). Additionally, the components for executing the method 300 may be spread among multiple devices. Method 300 may be implemented in the form of executable instructions stored on a machine-readable storage medium, such as storage medium 420, and/or in the form of electronic circuitry. The computing device 400 can be used to implement an authentication gateway.

[0047] Processor 410 may be, at least one central processing unit (CPU), at least one semiconductor-based microprocessor, at least one graphics processing unit (GPU), other hardware devices suitable for retrieval and execution of instructions stored in machine-readable storage medium 420, or combinations thereof. For example, the processor 410 may include multiple cores on a chip, include multiple cores across multiple chips, multiple cores across multiple devices (e.g., if the computing device 400 includes multiple node devices), or combinations thereof. Processor 410 may fetch, decode, and execute instructions 422, 424, 426, 428 to facilitate access to management platforms according to permissions based on tickets. As an alternative or in addition to retrieving and executing instructions, processor 410 may include at least one integrated circuit (IC), other control logic, other electronic circuits, or combinations thereof that include a number of electronic components for performing the functionality of instructions 422, 424, 426, 428.

[0048] Machine-readable storage medium 420 may be any electronic, magnetic, optical, or other physical storage device that contains or stores executable instructions. Thus, machine-readable storage medium may be, for example, Random Access Memory (RAM), an Electrically Erasable Programmable Read-Only Memory (EEPROM), a storage drive, a Compact Disc Read Only Memory (CD-ROM), and the like. As such, the machine-readable storage medium can be non-transitory. As described in detail herein, machine-readable storage medium 420 may be encoded with a series of executable instructions for authorizing permission to access management platforms based on activity associated with tickets.

[0049] At 302, the communication instructions 422 can be executed by processor 410 to receive, at the computing device 400, a request for access to a management platform of a device in a protected environment from a requestor. Communication instructions 422 can be used to send and/or receive information from the computing device 400. The computing device 400 can interface with the requestor using a user interface and the management platform(s) on a management plane via a management interface separate from the user interface.

[0050] In some examples, connections are via SSH, and make use of an ability of the SSH protocol to form tunnels for arbitrary ports which may listen for connections either locally or remotely. A secured port is used to handle incoming connections from users (e.g., the requestor). This can also be used for state synchronization between nodes when authentication gateway systems are deployed in a redundant cluster. The request can include authentication credentials (e.g., a username and password, an authentication token, etc.). At 304, authentication instructions 424 can be executed by processor 410 to authenticate the user based on the request. In some examples, an internal authentication database (e.g., a LDAP server) populated with end-user details of possible requestors can be used. Further, in some examples, a Kerberos Key Distribution Centre or other single sign-on technology can be used to authenticate users into the protected environment. In some examples, the request may include multiple parts (e.g., a first part to request access to the computing device 400, a second part to provide authentication information, etc.).

[0051] In one example, when the requestor connects to the computing device 400, the requestor can be presented with a menu system which allows a user to select a management platform to which to connect from a pre-configured list which has been established (e.g., by an administrator). Having selected a management platform, there may be a sub-menu which allows the selection of the function to perform (e.g., the connecting user may wish to log on to terminal session within the environment, an internal-only web interface within the environment from their browser, etc.).

[0052] In this example, once the form of access is selected, the user can be prompted to enter a ticket identifier, the details of which are then retrieved from an associated configured ticketing system. The relevant data-items are extracted. Relevant data-items may include any tasks associated with the ticket, authorizations that may be necessary and/or useful to perform the tasks, etc.

[0053] At 306, permissions instructions 426 can be executed at processor 410 to determine permissions to grant for the requested access based on the authenticated credentials and the ticket. The permissions granted can be based on the tasks associated with the ticket. As such, the permissions to access the

protected environment are task based instead of user based. In one example, the administrator may configure the computing device 400 to be fail-no-access, or fail-minimal-privilege, etc. in case the ticketing system is unavailable or unresponsive. In some examples, the permissions granted can be for a limited time. The limited time can be based on a time period, a fixed time, at the end of a session associated with the access, etc.

[0054] At 308, access instructions 428 can be executed by processor 410 to facilitate access to the management platform that access is requested to according to the permissions. The computing device 400 can encode and encrypt the authorization data to form a security token, which can verify connectivity to the management platform in question. The computing device can also validate the token credentials are acceptable to the computing device 400 itself and to the management platform(s) in protected environment. When access is facilitated, the token can be pushed to the management platform(s). As noted above, an SSH tunnel can be created to help facilitate the access.

[0055] If sufficient permissions should be granted, the SSH tunnel is used to verify the data in the token with the management platform. Then, the tunnel is held open to be used by the connecting user. In the example above, the access can be for a menu based console login. The computing device 400 can then punch a hole through its firewall to allow the specific network address (e.g., Internet Protocol address) from which the user has originated to connect to the specific port which has been opened. In another example, a new tunnel can be established (e.g., if web-based access or similar access has been requested). In some examples, when the session is closed or times-out, the hole through the firewall is automatically closed and any associated tunnels torn-down.

[0056] The user can be provided the requested access. For example, the user can be provided with a terminal onto the remote environment of the management platform when console access was requested, given a URL they can copy and paste into their web-browser or remote-desktop client to access a user interface associated with the management platform, etc. for other forms of access. For console access, a wrapper can be installed around tools such as ‘ssh’ which allow connections on to other systems within the environment. This

can be used to transparently push the local copy of the token to a daemon listening on further remote management platforms. With this approach, pre-authentication to further management platforms can occur in advance of the user being able to progress onto the specified follow-up system. In some examples, this step could be performed with a library to pre-load the token in order to work with networking utilities without the need for separate wrappers.

[0057] FIG. 5 is a flowchart of a method for facilitating access to management platforms, according to an example. Although execution of method 500 is described below with reference to computing device 400, other suitable components for execution of method 500 can be utilized (e.g., authentication gateway system 100). Additionally, the components for executing the method 500 may be spread among multiple devices. Method 500 may be implemented in the form of executable instructions stored on a machine-readable storage medium, such as storage medium 420, and/or in the form of electronic circuitry. The computing device 400 can be used to implement an authentication gateway.

[0058] As noted above, access instructions 428 can be executed by processor 410 to generate a token including permissions to grant to a requestor based on authentication of the requestor and information extracted from a ticket (502). The token can be encrypted. According to various examples, tokenization is the process of taking data (e.g., the authentication information and permissions data) and replacing it with a surrogate value that can be de-tokenized (e.g., at the management platforms). A look-up table can be used to de-tokenize a token to determine what permissions to provide to a user. Encryption is the process of using a cipher to mathematically transform data. Encrypted data can be transformed back using a key. The management platforms can have access to the key. In some examples, the encrypted token can represent information that the user provided access (e.g., via a tunnel) has been authenticated and has particular permissions.

[0059] At 504, the encrypted token is provided to the management platform. The management platform is capable of decrypting and/or de-tokenizing the token. The token can be provided via an application programming interface

(API). As noted above, the computing device 400 can execute the access instructions 428 to facilitate access to the management platform by facilitating establishment of a tunnel between a network address of the requesting user device and the management platform (506).

[0060] In some examples, the user may wish to access a second (or further) management platform within the protected environment. The second or further management platform can be located at another node of the protected environment. At 508, the request can go through the computing device 400 to the second management platform. The second request can also be associated with the ticket. The second request can cause providing of the token to the second management platform (510). The providing of the token can come from the computing device and/or be provided by the management platform that is already connected. The second management platform can decrypt and/or de-tokenize the token to determine what permissions the user has on the second management platform. In one example, the user may not have permission and is denied access. In another example, the user has certain permissions and can access actions associated with the permissions on the second management platform.

[0061] At 512, the computing device 400 can facilitate establishment of a tunnel between the network address associated with the user/requestor and the second management platform. In one example, the tunnel is from the network address, through the computing device 400, and to the second management platform via a management plane. In another examples, the tunnel can be routed through the first management platform (e.g., in a tiered network environment). Further, access to additional tiers of management platforms can be provided using this approach.

CLAIMS

What is claimed is:

1. An authentication gateway system comprising:

a communication engine to connect to a protected environment including a plurality of nodes via a management plane;

an interface to provide access to respective management platforms of the nodes,

wherein the interface is further to receive a request for access to one of the management platforms, the request including credentials associated with a requestor;

an authentication engine to authenticate the credentials; and

an authorization engine to determine permissions to grant for the access based on the authenticated credentials and a ticket.

2. The authentication gateway system of claim 1, wherein the requestor is further to identify the ticket.

3. The authentication gateway system of claim 1, wherein the communication engine is further to provide the one management platform with the permissions for the credentials.

4. The authentication gateway system of claim 3, wherein the interface is further to facilitate the access to the one management platform according to the permissions.

5. The authentication gateway system of claim 4,

wherein the requestor is connected to the interface via a network,

wherein the interface is open on one network port of the network and closed on other network ports of the network.

6. The authentication gateway system of claim 5,

wherein the requestor is associated with a network address of the network; and

wherein the communication engine is further to facilitate establishment of a tunnel between the network address and the management platform.

7. The authentication gateway system of claim 4, further comprising:

a token engine to generate an encrypted token including the permissions to grant for the credentials;

wherein the interface receives another request from the requestor to access a second one of the management platforms; and

wherein the communication engine is further to send the encrypted token to the second one management platform.

8. The authentication gateway system of claim 1, wherein the ticket includes a task to be performed, and wherein the permissions are related to activity associated with performing the task.

9. The authentication gateway system of claim 1, wherein access to the management platform is restricted to the management plane and wherein the authentication gateway system is located in a path between the network and the management plane.

10. A method comprising:

receiving, at an authentication gateway, a request for access to a management platform of a device in a protected environment from a requestor,

wherein the request includes credentials;

wherein the authentication gateway interfaces with the requestor using a user interface and the management platform on a management plane via a management interface separate from the user interface;

authenticating the credentials;

determining permissions to grant for the requested access based on the authenticated credentials and a ticket; and

facilitating access to the management platform according to the permissions.

11. The method of claim 10, further comprising:

generating an encrypted token including the permissions to grant for the credentials for a time period;

providing the encrypted token to the management platform.

12. The method of claim 11, further comprising:

receiving a second request from the requestor to access a second management platform of a second device in the protected environment, wherein the second request is associated with the ticket;

providing the encrypted token to the second management platform; and

facilitating access to the second management platform according to the permissions.

13. A non-transitory machine-readable storage medium storing instructions that, if executed by at least one processor of a computing device, cause the computing device to:

receive a request from a requestor for access to a management platform in a protected environment, the management platform associated with one of a plurality of nodes in the protected environment,

wherein the request includes credentials,

wherein the device interfaces with the requestor using a user interface and interfaces with the management platform on a management plane via a management interface separate from the user interface;

authenticate the credentials;

determine permissions to grant for the requested access based on the authenticated credentials and a ticket, wherein the permissions are valid for a predetermined time;

generate an encrypted token including the permissions to grant for the credentials;

provide the encrypted token to the management platform; and

facilitate access to the management platform.

14. The non-transitory machine-readable storage medium of claim 13, further comprising instructions that, if executed by the at least one processor, cause the computing device to:

facilitate establishment of a tunnel between a network address associated with the requestor and the management platform.

15. The non-transitory machine-readable storage medium of claim 14, further comprising instructions that, if executed by the at least one processor, cause the computing device to:

receive a second request from the requestor to access a second management platform of a second one of the nodes in the protected environment, wherein the second request is associated with the ticket;

provide the encrypted token to the second management platform; and

facilitate establishment of another tunnel between the network address and the second management platform.

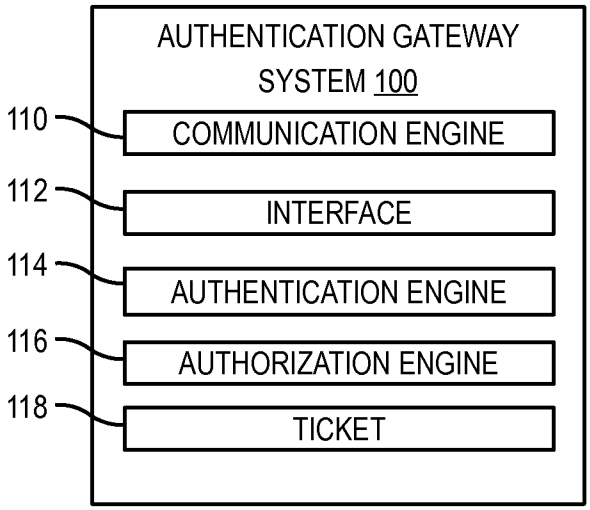
AUTHENTICATION GATEWAY
SYSTEM 100
110
COMMUNICATION ENGINE
112
INTERFACE
114
AUTHENTICATION ENGINE
116
AUTHORIZATION ENGINE
118
TICKET

FIG. 1

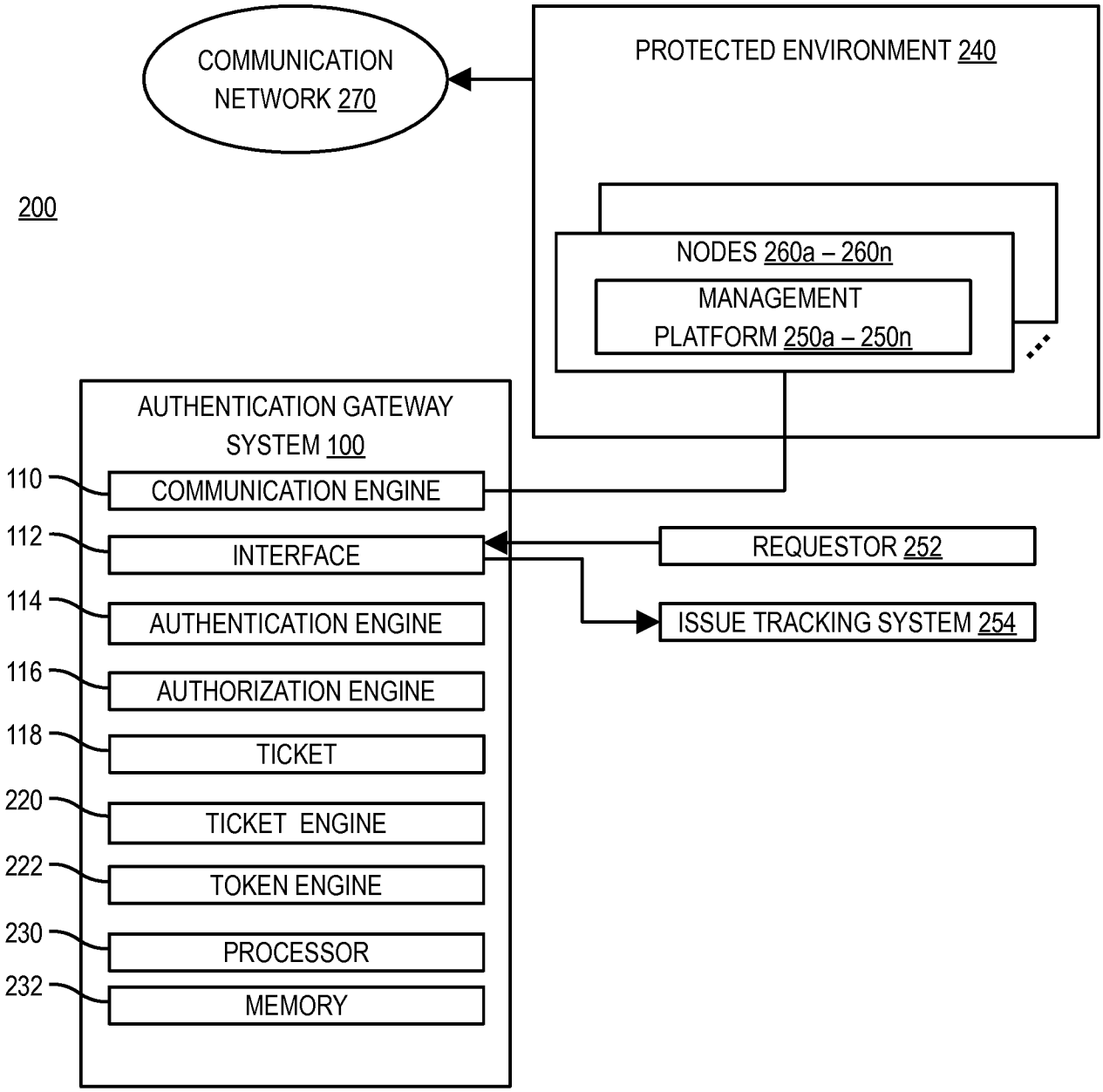
COMMUNICATION NETWORK 270
PROTECTED ENVIRONMENT 240
200
NODES 260a – 260n
MANAGEMENT PLATFORM 250a – 250n
AUTHENTICATION GATEWAY SYSTEM 100
110
COMMUNICATION ENGINE
112
INTERFACE
REQUESTOR 252
114
AUTHENTICATION ENGINE
ISSUE TRACKING SYSTEM 254
116
AUTHORIZATION ENGINE
118
TICKET
220
TICKET ENGINE
222
TOKEN ENGINE
230
PROCESSOR
232
MEMORY

FIG. 2

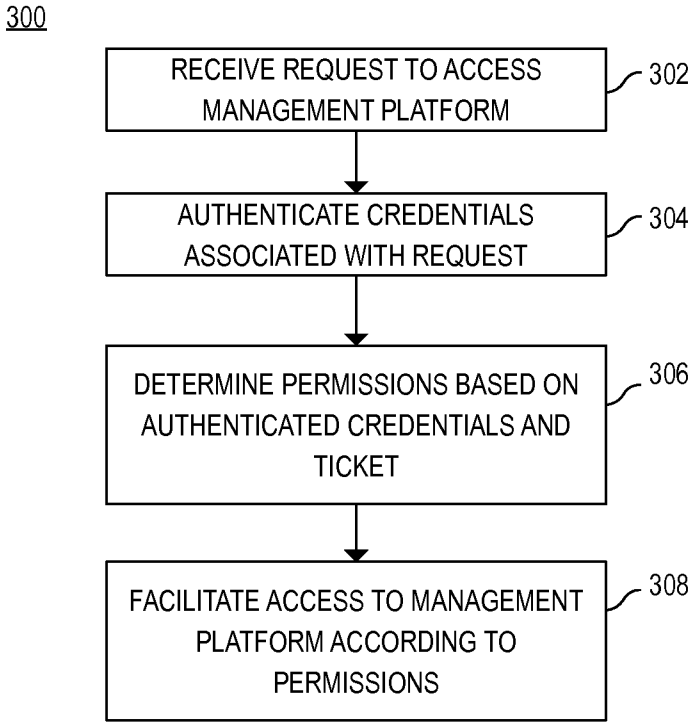
300
RECEIVE REQUEST TO ACCESS MANAGEMENT PLATFORM
302
AUTHENTICATE CREDENTIALS ASSOCIATED WITH REQUEST
304
DETERMINE PERMISSIONS BASED ON AUTHENTICATED CREDENTIALS AND TICKET
306
FACILITATE ACCESS TO MANAGEMENT PLATFORM ACCORDING TO PERMISSIONS
308

FIG. 3

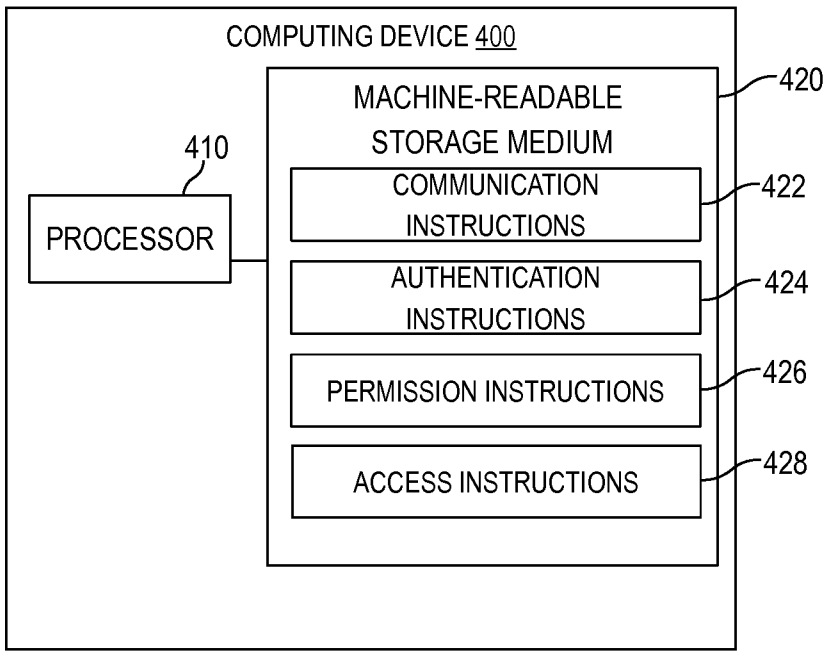
COMPUTING DEVICE 400
MACHINE-READABLE STORAGE MEDIUM
420
410
PROCESSOR
COMMUNICATION INSTRUCTIONS
422
AUTHENTICATION INSTRUCTIONS
424
PERMISSION INSTRUCTIONS
426
ACCESS INSTRUCTIONS
428

FIG. 4

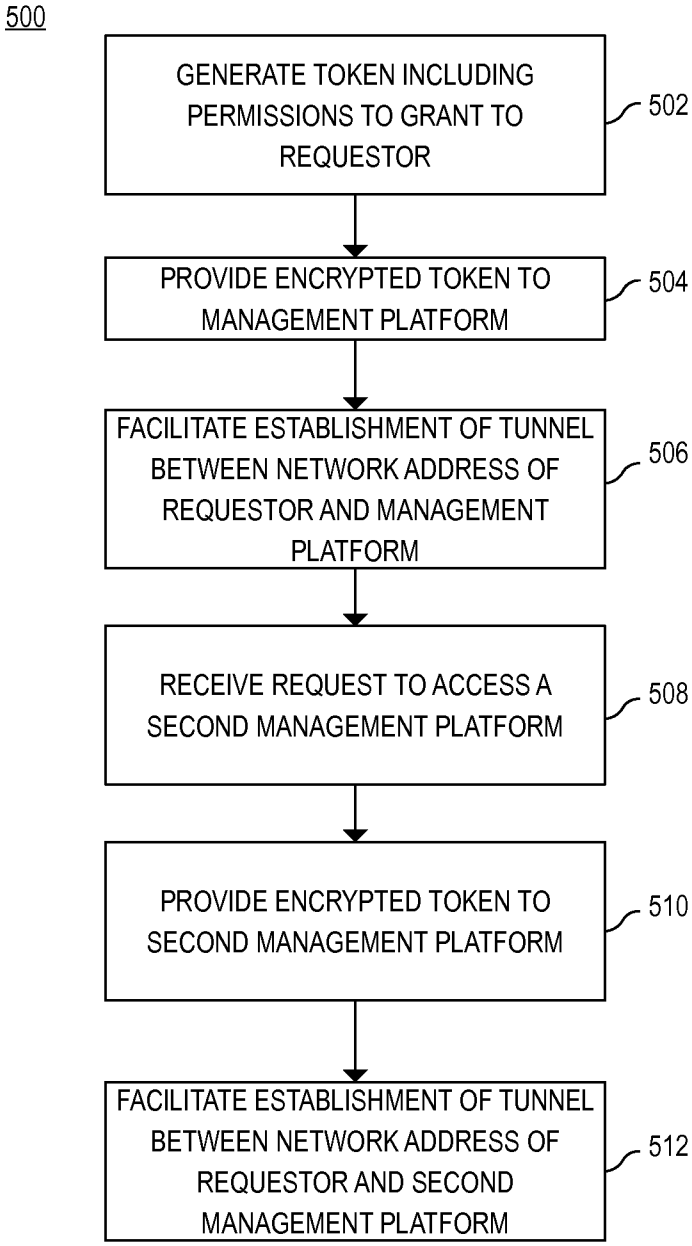
500
GENERATE TOKEN INCLUDING PERMISSIONS TO GRANT TO REQUESTOR
502
PROVIDE ENCRYPTED TOKEN TO MANAGEMENT PLATFORM
504
FACILITATE ESTABLISHMENT OF TUNNEL BETWEEN NETWORK ADDRESS OF REQUESTOR AND MANAGEMENT PLATFORM
506
RECEIVE REQUEST TO ACCESS A SECOND MANAGEMENT PLATFORM
508
PROVIDE ENCRYPTED TOKEN TO SECOND MANAGEMENT PLATFORM
510
FACILITATE ESTABLISHMENT OF TUNNEL BETWEEN NETWORK ADDRESS OF REQUESTOR AND SECOND MANAGEMENT PLATFORM
512

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/062048

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L12/24
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

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, 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	WO 2009/131656 A2 (BARCLAYS CAPITAL INC [US]; VIRTUOSO ANTHONY [US]; DOLPHIN MILES A [US]) 29 October 2009 (2009-10-29) figure 1 paragraphs [0023] - [0025], [0030], [0032] -----	1-15
X	US 7 356 601 B1 (CLYMER ANDREW M [GB] ET AL) 8 April 2008 (2008-04-08) figure 1B column 9, line 51 - line 58 column 13, line 33 - column 15, line 2 -----	1-15
X	EP 0 977 399 A2 (SUN MICROSYSTEMS INC [US]) 2 February 2000 (2000-02-02) paragraphs [0006], [0011], [0048] paragraphs [0049], [0052] - [0056] -----	1-15

-/--

[X] Further documents are listed in the continuation of Box C.

[X] 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 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	Date of mailing of the international search report
18 February 2016	29/02/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Kufer, Léna

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/062048

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2008/276134 A1 (SABIN JASON ALLEN [US] ET AL) 6 November 2008 (2008-11-06) paragraphs [0026] - [0030]	1-15
X	US 2004/093515 A1 (REEVES CHARLES R [US]) 13 May 2004 (2004-05-13) paragraphs [0032], [0033]	1-15

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2015/062048

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2009131656 A2	29-10-2009	EP 2269358 A2	05-01-2011
		JP 2011524559 A	01-09-2011
		US 2010106963 A1	29-04-2010
		WO 2009131656 A2	29-10-2009
US 7356601 B1	08-04-2008	NONE	
EP 0977399 A2	02-02-2000	CA 2278075 A1	28-01-2000
		DE 69923503 D1	10-03-2005
		DE 69923503 T2	16-02-2006
		EP 0977399 A2	02-02-2000
		JP 2000215168 A	04-08-2000
		US 6157953 A	05-12-2000
US 2008276134 A1	06-11-2008	NONE	
US 2004093515 A1	13-05-2004	NONE	