



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

(21) International Application Number:

PCT/US2017/055103

(22) International Filing Date:

04 October 2017 (04.10.2017)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

15/350,912 14 November 2016 (14.11.2016) US

(71) Applicant: **GENERAL ELECTRIC COMPANY**
[US/US]; 1 River Road, Schenectady, NY 12345 (US).

(72) Inventors: **DEVANEY, Louis, Francis**; GE Global Research - SW COE, 2623 Camino Ramon, Suite 500, San Ra-

mon, CA 94583 (US). **SALERNO, Stephen, Anthony**; GE Global Research - SW COE, 2623 Camino Ramon, Suite 500, San Ramon, CA 94583 (US).

(74) Agent: **DIMAURO, Peter, T.** et al.; General Electric Company, Global Patent Operation, 901 Main Avenue, 3rd Floor, Norwalk, CT 06851 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, 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,

(54) Title: SYSTEM AND METHOD FOR TRANSPARENT MULTI-FACTOR AUTHENTICATION AND SECURITY POSTURE CHECKING

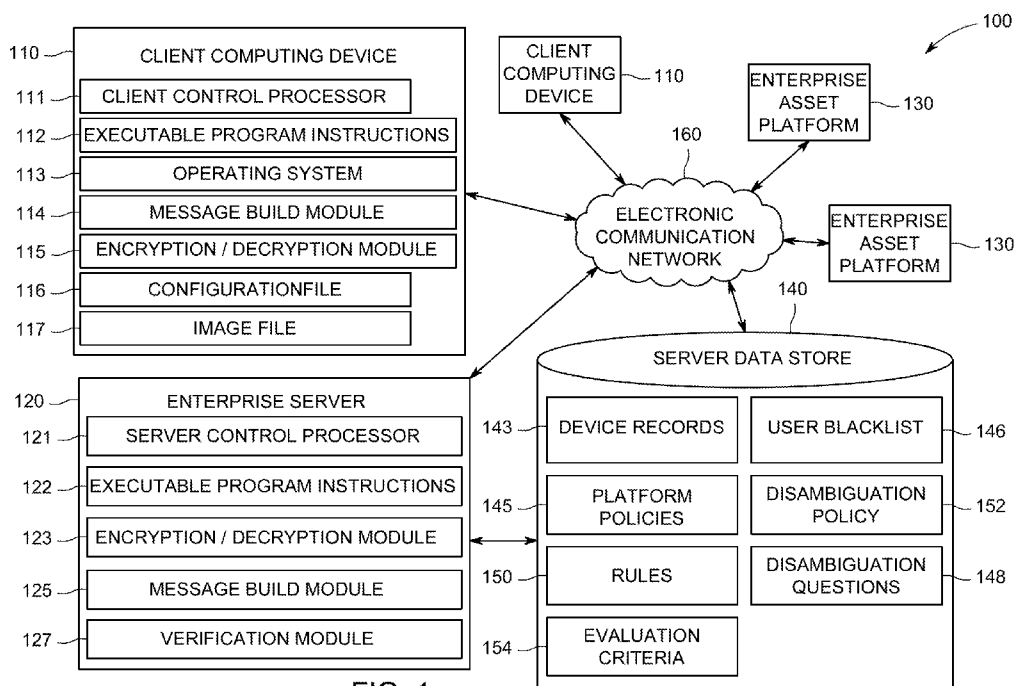


FIG. 1

(57) Abstract: A method for creating a secure connection between a remote client computing device and an enterprise asset platform includes a server receiving from a client computing device (CCD) a request being either a registration request or to access the asset platform, including a CCD unique identifier, determining if the CCD is previously blocked from accessing the asset platform, if so then terminating the method. If the request is a registration request, then generating a disambiguation query in accordance with predefined policy, receiving a response to the disambiguation inquiry from the CCD, verifying the contents of the disambiguation query response in relation to a predefined criteria. If the disambiguation query response does meet the predefined policy, associating the CCD to the predefined policy. A system configured to implement the method and a non-transitory computer-readable medium containing instructions for a processor to perform the method are also disclosed.

SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

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))*

SYSTEM AND METHOD FOR TRANSPARENT MULTI-FACTOR AUTHENTICATION AND SECURITY POSTURE CHECKING

BACKGROUND

[0001] Enterprises invest in remote access services to provide authorized employees, vendors, and other partners with access across a public communication network (e.g., the Internet) into the enterprise's network, data systems, websites, platforms, etc. The remote access should be managed and secure. However, access across shared public networks can be fraught with an array of risks (e.g., unauthorized access, eavesdropping / wire intercept, malware, keylogging & credential misappropriation, data leakage, misplaced / stole device(s), etc.).

[0002] Remote access resources can be exploited to breach the network security by hackers. An overwhelming percentage of all hacking breaches originate through hackers accessing the enterprise computing system from remote access service points. These hacking breaches can lead to threats such as worms, viruses, spyware, data theft, application abuse, etc.

[0003] Conventional approaches grant remote access by implementing a username / password authentication paradigm. Missing from the art is a solution that provide a user-friendly, cost-effective, transparent enhanced security layer for remote access authentication with repeated security checks.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] FIG. 1 depicts a remote access security system in accordance with embodiments;

[0005] FIG. 2 depicts a flowchart of a process for device disambiguation in accordance with embodiments;

[0006] FIG. 3 depicts a flowchart of a process for device validation in accordance with embodiments;

[0007] FIG. 4 depicts a flowchart of a process for device registration in accordance with embodiments; and

[0008] FIG. 5 depicts a flowchart of a process for security posture recheck/authentication in accordance with embodiments.

DETAILED DESCRIPTION

[0009] Embodiment systems and methods determine whether to grant a request to remote access an enterprise asset. The request evaluation can include a username / password authentication process supplemented with examination of a one or more criteria — for example, an issued cryptographic certificate located on the requesting remote device, the configuration of the requesting remote device itself, the security posture of the device, and other factors. In accordance with embodiments, the examination of the one or more criteria is performed in a manner that is transparent to a user of the remote device.

[0010] Embodiment systems and methods leverage an encrypted query and response protocol to evaluate the requesting device against policy and device profile information stored in a manner that is inaccessible to the user. Re-evaluation of access decisions can be performed on a repeated basis, and can use rotating questions to evaluate the authentication of a requesting client. The interval between repeated reevaluations can be varied based on a value set in policy. If a policy violation is detected, various actions can be taken — for example, denial and/or revocation of access (temporary, or permanently) as detailed in a predefined policy.

[0011] Figure 1 depicts system 100 for remote access authentication, validation, and security-posture checking in accordance with embodiments. An embodiment system can include one or more client computing devices 110. The client computing device can be a computing device suitable for use by an end user in performance of the end user's purpose (e.g., personal computer, workstation, thin client, netbook, notebook, tablet computer, mobile device, etc.).

[0012] Client computing device 110 can include client control processor 111 that communicates with other components of the client computing device. Control processor 111 accesses computer executable instructions 113, which can include operating system 113. Message build module 114 can assemble responses to security/ authentication queries. Encryption/decryption module 115 can perform encryption/decryption using symmetric and asymmetric algorithms such as, but not limited to, AES and/or RSA and compression/decompression on messages from/ to the client computing device. Configuration file 116 can include data regarding hardware and/or software contents of the particular client computing device — for example, installation and/or revision identifiers of antivirus software, word processing software, motherboard serial number, processing unit identifier, etc. Image file 117 can include files accessible during the validation/ authentication/ security check

operations. In accordance with embodiments the configuration data file and image file contents can be checked for compliance with predefined policy to verify the client computing device authenticity.

[0013] Enterprise server 120 can include at least one server control processor 121 configured to support embodying verification/ authentication/ security check operations by executing executable instructions 122 accessible by the control processor. Dedicated hardware, software modules, and/or firmware can implement embodying remote access verification/ authentication/ security services disclosed herein.

[0014] Server message build module 125 can assemble security/ authentication queries in accordance with embodying methods. These queries can be sent to a client computing device requesting access to an enterprise asset. Server encryption/decryption module 123 can perform symmetric and asymmetric encryption/decryption and compression/decompression on messages from/ to the client computing device. Verification module 127 can apply rules and/or one or more policies in accordance with embodying operations to determine compliance of a requesting client computing device response to queries sent to server 120.

[0015] Server 120 is in communication with data store 140. Server side message build module 125 can assemble queries for the security/ authentication operations. These queries are based on predefined conditions that are expected from a requesting client computing device. The queries can include references to unique configuration data stored in device records 143 previously collected from the client computing device. Server side encryption/decryption module 123 can perform symmetric and asymmetric encryption/decryption and compression/decompression on messages from/ to the requesting client computing device.

[0016] Elements within the data store can be used in developing the queries sent to a client computing device requesting access to enterprise asset platform 130. These elements can include user blacklist 146 (e.g., a listing of unauthorized client computing device identifiers, and user ids), device records 143 (e.g., unique configuration data previously collected from the client computing device, including policy association), platform policies 145 (e.g., policies aggregating rules associated with a given client device standard software load), disambiguation policy 152 (e.g., mapping data associating disambiguation questions to associated policy with weighted point values), disambiguation questions 148 (e.g., predefined interrogatories), rules 150 (e.g., one or more set of predefined interrogatories used to create queries), and evaluation criteria 154 (information used to determine passing responses, and the actions to take for failing responses).

[0017] System 100 includes one or more enterprise asset platform(s) 130. Each enterprise asset platform is remotely accessible across electronic communication network 160. An enterprise asset platform can be, for example, one of a node on an enterprise's network, a data system, a website, and/or other platform that can be remotely accessed. In some implementations the asset platform can also act as a gateway providing access to a network of protected enterprise resources. In accordance with embodiments, an enterprise asset platform can be included within enterprise server 120.

[0018] Each of the components of system 100 can be in communication across electronic communication network 160. The electronic communication network can be, can comprise, or can be part of, a private internet protocol (IP) network, the Internet, an integrated services digital network (ISDN), frame relay connections, a modem connected to a phone line, a public switched telephone network (PSTN), a public or private data network, a local area network (LAN), a metropolitan area network (MAN), a wide area network (WAN), a wireline or wireless network, a local, regional, or global communication network, an enterprise intranet, any combination of the preceding, and/or any other suitable communication means. It should be recognized that techniques and systems disclosed herein are not limited by the nature of network 160.

[0019] Embodying methods apply an encrypted query/response protocol to verify credentials and evaluate endpoint security at a client computing device requesting access to one of the enterprise remote assets. Data store 140 includes a policy store with endpoint questions and criteria describing how the questions could be evaluated. These questions and criteria are based on predefined paradigms provided by the enterprise personnel — e.g., IT professionals, network security experts, etc.

[0020] In accordance with an implementation, a query can be sent to the client computing device asking for a list of some, or all, programs/applications (and also in some instances version identifiers) that the client computing device is running. The client computing device can assemble a response by examining configuration file 116 for responsive details. Rules 150 specific to a particular policy can evaluate a response in a variety of ways by checking. As a non-limiting example, the rules could check to make sure that approved antivirus software is running, or check to make sure that prohibited software is not installed on the client computing device. Because the evaluation occurs at enterprise server 120, which is remote from the client computing device, the client has no visibility into the evaluation criteria, the policy, or the rules being used.

[0021] Conventional approaches to approving remote access to asset platforms face a significant drawback in that cryptographic certificates can be copied. Thus, enabling for computing device and/or local user impersonation. Embodiment systems and methods perform the security verification in a manner transparent to the client computing device and its local user. Accordingly, embodiments solve this problem by ensuring that the cryptographic certificate can only be used on the client computing device to which it was issued, and by testing the security posture of the client computing device when authentication occurs. Thus, embodiments minimize the risk from certificate theft, while ensuring that the client computing device is policy compliant.

[0022] In accordance with embodiments, the association between User Identity / Certificate / Device Identifiers is maintained within elements of data store elements 140. Query response(s) received from a client computing device requesting access to an asset platform is checked on the server side against the information stored in the data store. In some implementations, device identifiers can be “learned” from individual client computing devices, stored in the data store, and then used later during the verification/ check comparison.

[0023] In accordance with embodiments, the predefined policy and/or paradigms can be updated or modified periodically, or non-periodically. The policy and paradigm can be configured to prevent tampering attempts, identify active session attacks-in-progress, and to enact countermeasures against a detected attacker. By implementing the predefined policy and rules, embodiment systems and methods ensure that authentication is happening in a trustworthy context — for example, is the required software running? Is device tampering detected?)

[0024] Embodiment systems and methods perform a security analysis of client computing device(s) by querying the client computing device for architectural details, and then analyzing the query responses remote from the client computing device. In accordance with embodiments, different levels of access can be granted providing access to different enterprise asset platforms. The queries sent to the client computing device can transparently request multiple factors to be used in the device authentication — for example, user SSO/Password; enterprise-issued User/Device Certificate; Unique Device Attributes (configuration data, image file content, etc.).

[0025] In accordance with embodiment methods can include repeated endpoint validation techniques. These techniques can implement a policy-based approach to require that a client computing device is in compliance with predefined policy and/or criteria. Failure to be in compliance results in access to enterprise asset platforms being denied, or the termination

of in-progress access. In some implementations, individual device fingerprinting can be used to fully or partially identify devices.

[0026] In accordance with embodiments, systems and methods can perform a three stage approach to disambiguate, validate, and register a remote client computing device that is requesting access to an enterprise asset platform. Once a client computing device has registered, the system can transparently validate the user and client computing device to provide secured access. This transparent validation can use repeated security checks during the user session. The operations can be performed transparent to the local user of the client computing device.

[0027] Figure 2 depicts a flowchart of device disambiguation process 200 in accordance with embodiments. Disambiguation process 200 queries a client computing device to associate it with platform policy 145 appropriate for client computing device's configuration using predefined, predetermined disambiguation questions resident in data store 140. By employing embodying systems and methods an enterprise can test different client device software configurations against policies suited for those configurations (for instance, an enterprise could maintain two client device platforms with different but acceptable antivirus software). A registration request for clearance to access the registration server enterprise asset platform resource 130 can be received at server 120 from client computing device 110, step 205. The registration request can be asymmetrically encrypted with the server's public key.

[0028] The server decrypts the registration request. The server compares the identity of the client computing device and/or the local user identity to a listing of blocked identities maintained in user blacklist 146, step 210. If the user or the device is blocked from accessing remote assets, the process terminates.

[0029] If the user or the device identity does not appear on the blocked list, a disambiguation query is generated, step 215. The disambiguation query queries the client computing device for specific configuration information based on predefined policy, rules assigned to the type of request. The disambiguation query can include a timestamp.

[0030] The server transmits, step 220, the disambiguation query to the requesting client computing device. The disambiguation query can be encrypted and/or compressed on the server side. Client message build module 114 can assemble responses to the disambiguation query. Based on the nature of the query, the response can include details on software configuration installation revision identifiers of antivirus software, word processing software,

motherboard serial number, processing unit identifier, data regarding hardware of the client computing device, image file content, and other details in accordance with predefined disambiguation policies.

[0031] The server receives, step 225, from the client computing device a response to the disambiguation query. The response itself can be encrypted and/or compressed. Based on the contents of the response, the client computing device can be assigned to platform policy 145. The response is evaluated, step 230, by assigning points to each portion of the query response. If the assigned points are greater for a particular policy, the client computing device is associated with that policy, step 235. If the response fails the evaluation, the process terminates. In some implementations, for example, a tie between policies, the client computing device can be evaluated based on a configured system default policy. During initial registration, once the client computing device has been associated with a policy, it will be validated using process 300 (FIG. 3).

[0032] Figure 3 depicts a flowchart of device validation process 300 in accordance with embodiments. Validation process 300 queries a client computing device requesting access to an enterprise asset platform to determine its authenticity based on a policy assigned during disambiguation process 200 in combination with predefined, predetermined questions resident in data store 140. A request to access enterprise asset platform resource 130 can be received at server 120 from client computing device 110, step 305.

[0033] The server determines, step 310, the policy assigned to the particular client computing device requesting the access. The determination is based on a policy stored in device records 142 as a result of disambiguation process 200. If the particular client computing device has not yet been assigned a policy, process 300 is terminated, and server 120 executes disambiguation process 200 described above.

[0034] A validation query is built, step 315, using questions from the assigned policy and rules 150. The purpose of the validation query is to evaluate whether the actual requesting client computing device is policy compliant and can be trusted with remote access to the asset platform. Based on defined rules 150, the query can contain rotating questions that vary with each query instance. The query can contain questions associated with the requested enterprise asset platform (e.g., questions asked for a device requesting registration access may vary from questions asked for a device requesting network access). The server transmits, step 320, the validation query to the requesting client computing device. In some implementations the query can be timestamped. The validation query can be encrypted and/or compressed on the server

side. Client message build module 114 can assemble responses to the validation query. Based on the nature of the query, the response can include details on software configuration installation revision identifiers of antivirus software, word processing software, motherboard serial number, processing unit identifier, data regarding hardware of the client computing device, image file content, and other details in accordance with predefined policies.

[0035] The server receives, step 325, from the client computing device a response to the validation query. The response itself can be encrypted and/or compressed. The response is evaluated by checking query answers against evaluation criteria 154 residing in data store 140. The evaluation criteria is resident on the server side of system 100, and the evaluation of the query response is performed on the system's server side. The client computing device is not exposed to the criteria, nor the response evaluation, making the process transparent to the client computing device and its local user.

[0036] If the evaluation of the validation query response determines, step 330, that the response is not correct, validation process 300 terminates. With successful validation, process 300 creates an access token, step 335 for the particular client computing device requesting access to the asset platform. The access token can be an asymmetrically signed using an algorithm such as RSA so that it can only be read by the particular asset platform requested by the client computing device. This access token can include details for validation crosscheck. In addition, the access token can be time stamped and associated with a predetermined expiration deadline for added security. The access token is provided, step 340, to the client computing device. With this token, the client computing device can be verified when connection is made with the enterprise asset platform identified in the received request (step 305). If the token is to be used in an initial registration, it can be passed to a registration enterprise resource platform as described below in registration process 400 (FIG. 4). If the token is to be used for post-registration access to a protected enterprise resource platform, it can be used as described in security posture recheck/authentication process 500 (FIG. 5).

[0037] Figure 4 depicts a flowchart of device registration process 400 in accordance with embodiments. Registration process 400 performs the tasks of verifying a registration access token, and generating a user/device certificate that can be used in validation after registration. A registration request (including a client certificate signing request) with an access token is received, step 405, from the client computing device. This request can be received at the registration asset platform, or server.

[0038] In accordance with implementations, registration process 400 can be performed at the server, at the asset platform, and/or the server and asset platform acting in combination. The asset platform can include a Certificate Authority functionality for generating client user/device certificates. The asset platform can also include an application that performs additional security checking needed for registration, such as user password checking or one-time password checking.

[0039] The token is decrypted, step 410. The decrypted access token is verified, step 415. Verification can include signature checking the token; checking client computing device details resident in data store 140 obtained during device disambiguation process 200 and/or device validation process 300; checking whether the token user matches user authentication and authorization information; and that the token has not yet expired.

[0040] If the token is not verified, access to the asset platform is denied and the process is terminated. If the token is verified, a certificate is generated, step 420, for the client computing device and user. The access certificate is then transmitted to the client computing device, step 425. Once received, the certificate is securely stored, step 425, on the client computing device. In some implementations the certificate can be placed in a client Crypto API (CAPI) certificate store.

[0041] Figure 5 depicts a flowchart of security posture recheck/authentication process 500 for client enterprise asset access in accordance with embodiments. Access to the enterprise asset platform can be accomplished using a web browser or through methods including resource proxying or network tunneling over a Transport Layer Security (TLS) layer for enterprise access platforms allowing access to a protected network segment. When TLS tunneling is used, the client certificate obtained during registration process 400 can be transparently presented for authentication purposes and the connection can be pinned (by having the client check static details about the enterprise asset TLS connection) to prevent interception.

[0042] Client computing device 110 can establish session crosscheck information to be used with the enterprise asset platform. In accordance with implementations, the crosscheck information can be derived locally or provided by the asset platform before access. This crosscheck information is used to request validation, step 505, using device validation process 300. If validated, an access token is provided along with expiration time information. The expiration time can be encrypted.

[0043] The client computing device can track the expiration time of the provided token, step 510. A renewal request can be made utilizing process 300 prior to expiration, step 515. The token is presented to the enterprise asset platform for use in authenticating access. An active session is established, step 520, between the client computing device and the asset platform by passing the token.

[0044] The token is decrypted, step 525. The decrypted access token is verified, step 530, for its being valid for the requested asset platform and valid for the requesting client computing device. Verification can include signature checking the token; checking crosscheck details contained within the token; checking whether the token was issued for the protected resource; checking whether the token user matches the presented client TLS certificate and/or other authentication details; and that the token has not yet expired.

[0045] If the token is invalid or expired, a signal will be sent to the client computing device indicating that a valid token is needed, step 535. Process 500 then returns to step 505, where the client computing device requests a new, valid token using process 400. If the presented token is valid, access is granted for the requested enterprise asset platform, step 540. In accordance with embodiments, Process 500 can enter a loop repeating token verification step 530 at intervals set by the associated policy.

[0046] Table I provides a matrix detailing an overview of controls implemented by embodying systems and methods to counter specific risks identified in the table. These risks include unauthorized access, eavesdropping and communication intercept, malware, keylogging and credential theft, loss or theft of a client computing device, and data theft/leakage.

<u>RISK</u>	<u>EMBODYING CONTROL ACTION</u>
Unauthorized Access	Signed access tokens required and continuously re-checked User must have Password, Certificate obtained in registration, and Device Used to Register
Eavesdropping & Wire Intercept	Pinned Transport Layer Security (TLS) Connections Encrypted proprietary protocol within TLS Disallowed Process Checks Anti-Tamper Checks
Malware	Access denial if approved anti-virus program not running Access denial where management software is not running Disallowed process checks Anti-tamper checks
Keylogging & Credential Theft	Multifactor requires Single sign-on (SSO + Password + Certificate + Device) Token cross-checks and expiration Virtual Machine Detection and Blocking
Laptop loss or theft	Password required to unlock credential store System supports lockouts for lost assets System supports Certificate Revocation
Data Leakage	Access denial if approved anti-virus not running Access denial for unmanaged devices

TABLE 1

[0047] In accordance with some embodiments, a computer program application stored in non-volatile memory or computer-readable medium (e.g., register memory, processor cache, RAM, ROM, hard drive, flash memory, CD ROM, magnetic media, etc.) may include code or executable instructions that when executed may instruct and/or cause a controller or processor to perform methods discussed herein such as a method for providing secure, transparent, multi-factor validation, registration, authentication of client computing devices requesting remote access to asset platforms with security posture recheck/authentications, as described above.

[0048] The computer-readable medium may be a non-transitory computer-readable media including all forms and types of memory and all computer-readable media except for a transitory, propagating signal. In one implementation, the non-volatile memory or computer-readable medium may be external memory.

[0049] Although specific hardware and methods have been described herein, note that any number of other configurations may be provided in accordance with embodiments of the invention. Thus, while there have been shown, described, and pointed out fundamental novel

features of the invention, it will be understood that various omissions, substitutions, and changes in the form and details of the illustrated embodiments, and in their operation, may be made by those skilled in the art without departing from the spirit and scope of the invention. Substitutions of elements from one embodiment to another are also fully intended and contemplated. The invention is defined solely with regard to the claims appended hereto, and equivalents of the recitations therein.

CLAIMS

We claim:

1. A method for creating a secure connection between a remote client computing device and an enterprise asset platform, the method comprising:

receiving at a server a request from a client computing device in communication with the server across an electronic communication network, the request being one of a registration request and a request to access the asset platform, the request including a client computing device unique identifier;

determining if the client computing device is previously blocked from accessing the asset platform, wherein if the client computing device was previously blocked the method terminates;

if the request is a registration request, then:

generating a disambiguation query in accordance with predefined policy at the server;

receiving a response to the disambiguation inquiry from the client computing device;

verifying the contents of the disambiguation query response in relation to a predefined criteria;

the verifying step being done remote from the client computing device in a manner transparent to a user of the client computing device; and

if the disambiguation query response does meet the predefined policy, associating the client computing device to the predefined policy.

2. The method of claim 1, the determining step including comparing the client computing device unique identifier to a listing of blocked client computing devices in a data store that is in communication with the server.
3. The method of claim 1, the disambiguation query including predefined questions resident in a data store in communication with the server.

4. The method of claim 3, the predefined questions based on one or more client computing device configuration details, installed application revision number, listing of installed applications, hardware identifiers, and content from one or more image files.
5. The method of claim 1, the verifying step including evaluating the disambiguation query response by assigning predetermined points for each portion of the response.
6. The method of claim 5, including if a cumulative point score is below a predetermined threshold, at least one of terminating the method and assigning a default policy.
7. The method of claim 1, if the request is an access request, then:
 - determining the predefined policy assigned to the client computing device;
 - building a validation query in accordance with predefined policy at the server;
 - receiving a response to the validation inquiry from the client computing device;
 - if the validation query response does not meet the predefined policy, terminating the method;
 - if the validation query response does meet the predefined policy, creating an access token having crosscheck details for the client computing device; and
 - providing the access token to the client computing device.
8. The method of claim 7, including:
 - examining at least one of device tables and device records in a data store in communication with server to locate an association between a client computing device identifier and the assigned policy; and
 - if no association is located, terminating the method.
9. The method of claim 8, including:
 - inserting a timestamp into the access token; and
 - associating the access token with a predetermined expiration deadline.
10. The method of claim 1, including:

receiving a registration access token from the client computing device with the access request;

decrypting the access token;

verifying the decrypted access token;

if the decrypted access token is not successfully verified, terminating the method;

if the decrypted access token is successfully verified, then:

generating a certificate for the client computing device and the end user of the client computing device; and

transmitting the generated certificate to the client computing device.

11. The method of claim 10, including establishing an active session between the client computing device and the asset platform.
12. The method of claim 11, including renewing the token prior to expiration of a time stamp associated with the token.
13. The method of claim 11, including performing security posture rechecks of the client computing device token validity during the session.
14. A non-transitory computer readable medium containing computer-readable instructions stored therein for causing a control processor to perform a method for creating a secure connection between a remote client computing device and an enterprise asset platform, the method comprising:

receiving at a server a request from a client computing device in communication with the server across an electronic communication network, the request being one of a registration request and a request to access the asset platform, the request including a client computing device unique identifier;

determining if the client computing device is previously blocked from accessing the asset platform, wherein if the client computing device was previously blocked the method terminates;

if the request is a registration request, then:

generating a disambiguation query in accordance with predefined policy at the server;

receiving a response to the disambiguation inquiry from the client computing device;

verifying the contents of the disambiguation query response in relation to a predefined criteria; and

if the disambiguation query response does meet the predefined policy, associating the client computing device to the predefined policy.

15. The non-transitory computer readable medium of claim 14 containing computer-readable instructions stored therein to cause the control processor to perform the method, if the request is an access request, including:

determining the predefined policy assigned to the client computing device;

building a validation query in accordance with predefined policy at the server;

receiving a response to the validation inquiry from the client computing device;

verifying the contents of the disambiguation query response in relation to a predefined criteria;

if the validation query response does not meet the predefined policy, terminating the method;

if the validation query response does meet the predefined policy, creating an access token having crosscheck details for the client computing device; and

providing the access token to the client computing device.

16. The non-transitory computer readable medium of claim 14 containing computer-readable instructions stored therein to cause the control processor to perform the method, if the request is an access request, including:

receiving a registration access token from the client computing device with the access request;

decrypting the access token;

verifying the decrypted access token;

if the decrypted access token is not successfully verified, terminating the method;

if the decrypted access token is successfully verified, then:

generating a certificate for the client computing device and the end user of the client computing device; and

transmitting the generated certificate to the client computing device.

17. The non-transitory computer readable medium of claim 16 containing computer-readable instructions stored therein to cause the control processor to perform the method including:

establishing an active session between the client computing device and the asset platform;

renewing the token prior to expiration of a time stamp associated with the token; and

performing security posture rechecks of the client computing device token validity during the session.

18. A system for creating a secure connection between a remote client computing device and an enterprise asset platform, the system comprising:

a server including a control processor in communication with a client computing device across an electronic communication network, the server in communication with a data store and at least one asset platform across the electronic communication network;

the server including an encryption/decryption module configured to receive for the client computing device a request being one of a registration request and a request to access the asset platform, the request including a client computing device unique identifier;

the server control processor configured to access executable program instructions that cause the server control processor to:

determine if the client computing device is previously blocked from accessing the asset platform by accessing at least one of a device record store and a device table store, wherein if the client computing device was previously blocked terminate creation of the secure connection;

if the request is a registration request, then:

generate at the server a disambiguation query in accordance with a predefined policy;

receive a response to the disambiguation inquiry from the client computing device;

verify the contents of the disambiguation query response in relation to a predefined criteria;

the verifying step being done remote from the client computing device in a manner transparent to a user of the client computing device; and

if the disambiguation query response does meet the predefined policy, associate the client computing device to the predefined policy.

19. The system of claim 18, the server control processor configured to access executable program instructions that cause the server control processor to, if the request is an access request:

determine the predefined policy assigned to the client computing device;

build at the server a validation query in accordance with predefined policy;

receive a response to the validation inquiry from the client computing device;

if the validation query response does not meet the predefined policy, terminate creation of the secure connection;

if the validation query response does meet the predefined policy, create an access token having crosscheck details for the client computing device; and

provide the access token to the client computing device.

20. The system of claim 19, the server control processor configured to access executable program instructions that cause the server control processor to, if the request is an access request:

receive a registration access token from the client computing device with the access request;

decrypt the access token;

verify the decrypted access token;

if the decrypted access token is not successfully verified, terminate creation of the secure connection;

if the decrypted access token is successfully verified, then:

generate a certificate for the client computing device and the end user of the client computing device; and

transmit the generated certificate to the client computing device;

establish an active session between the client computing device and the asset platform;

renew the token prior to expiration of the session; and

perform security posture rechecks of the client computing device token validity during the session.

1/5

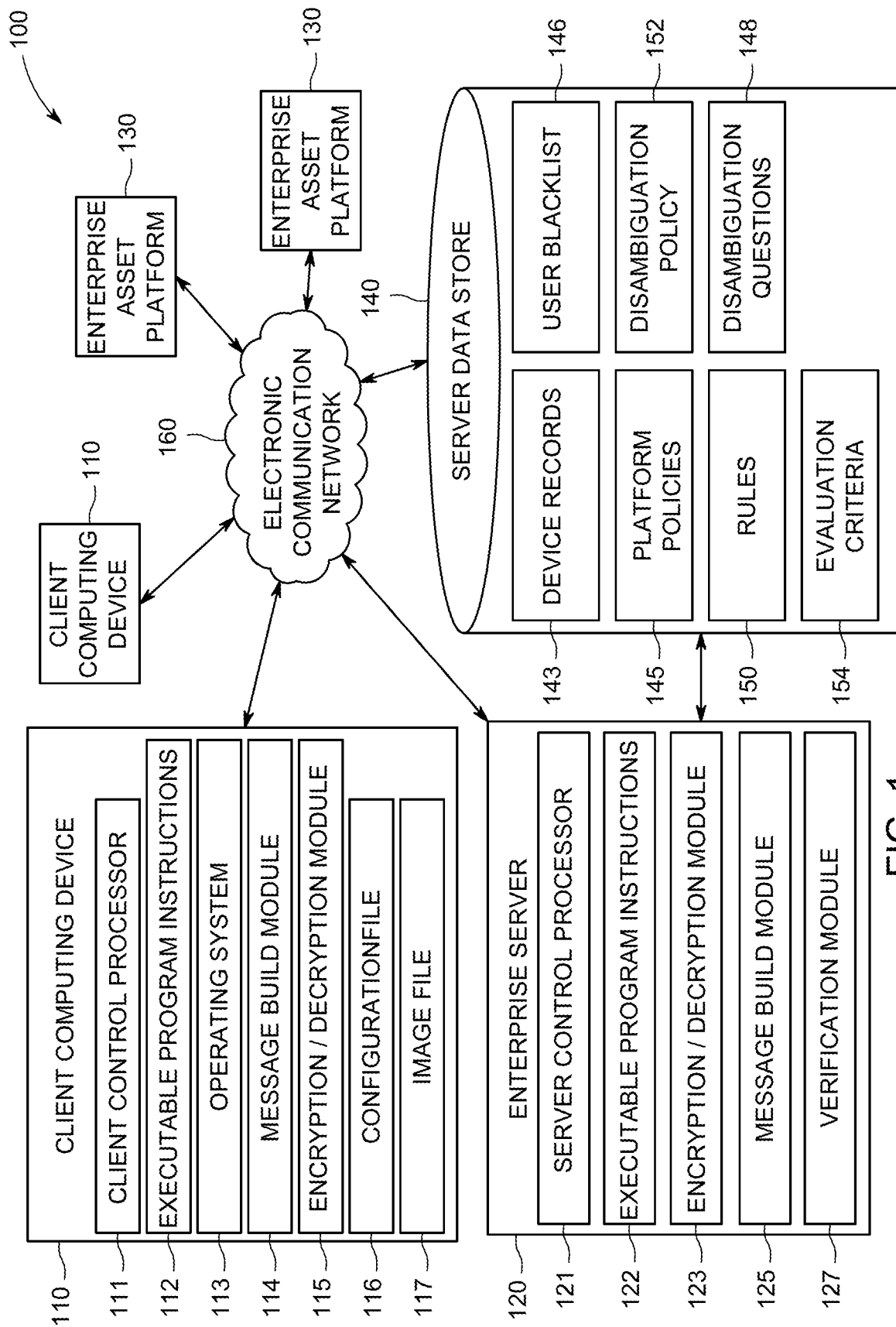


FIG. 1

2/5

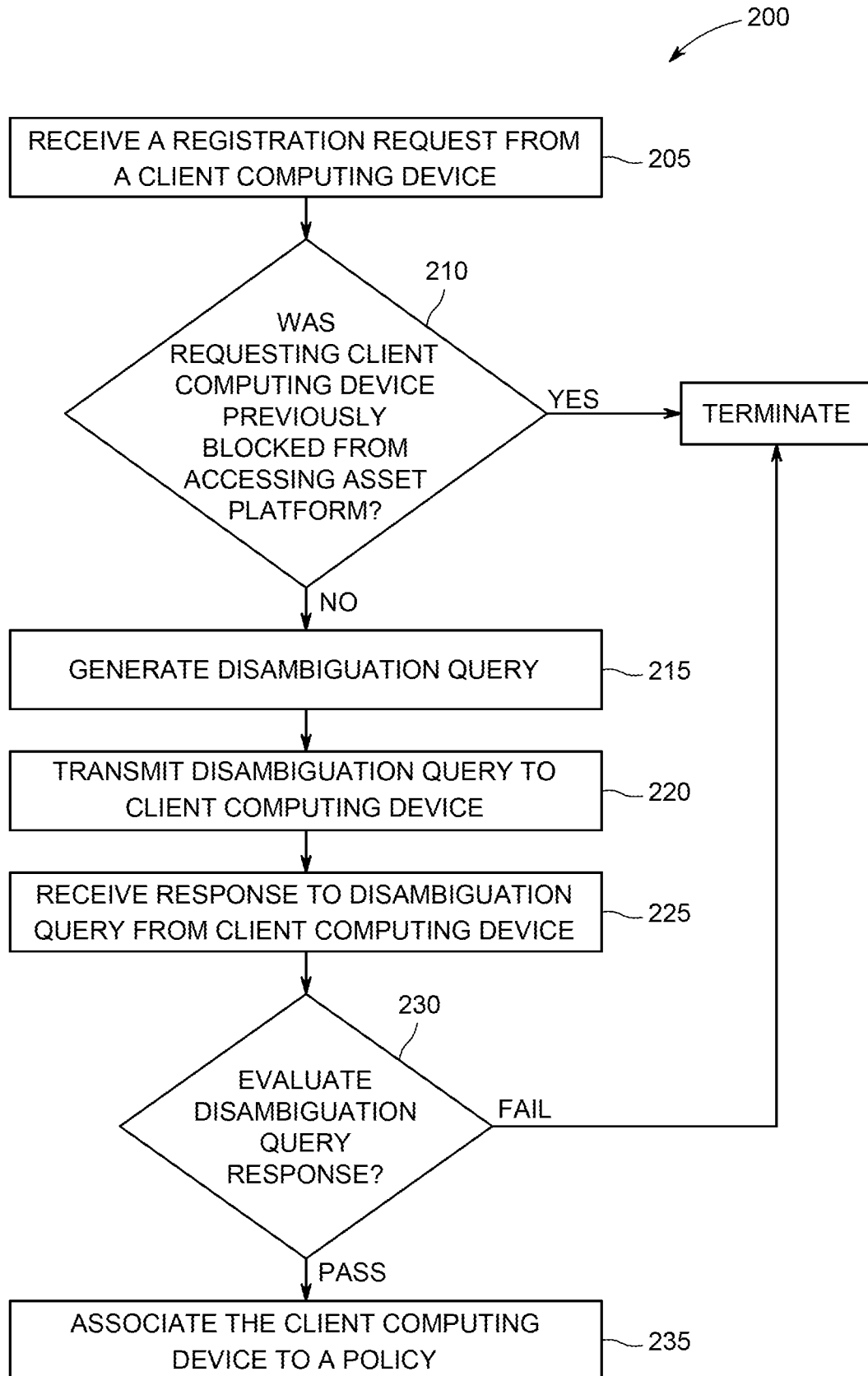


FIG. 2

3/5

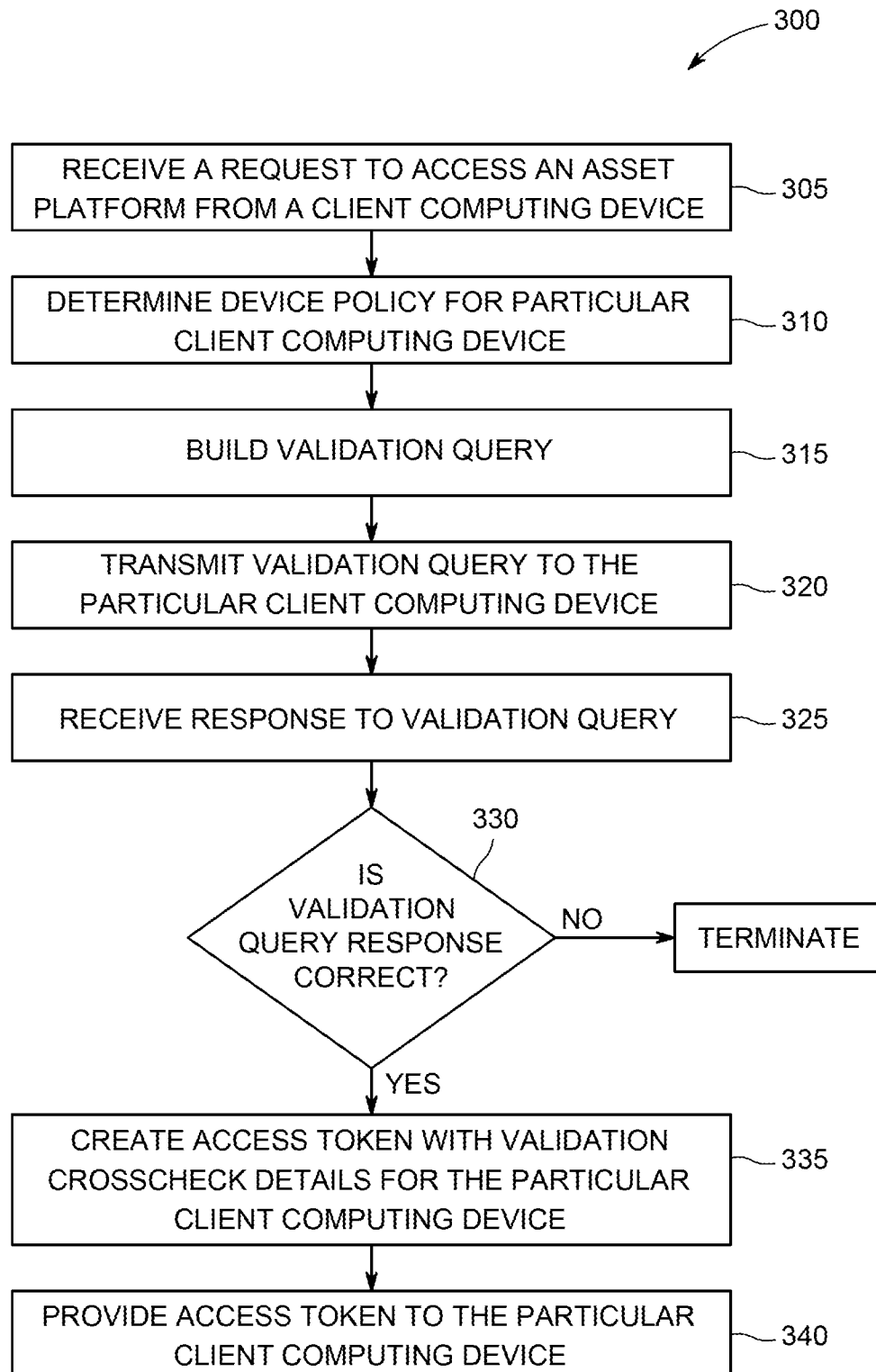


FIG. 3

4/5

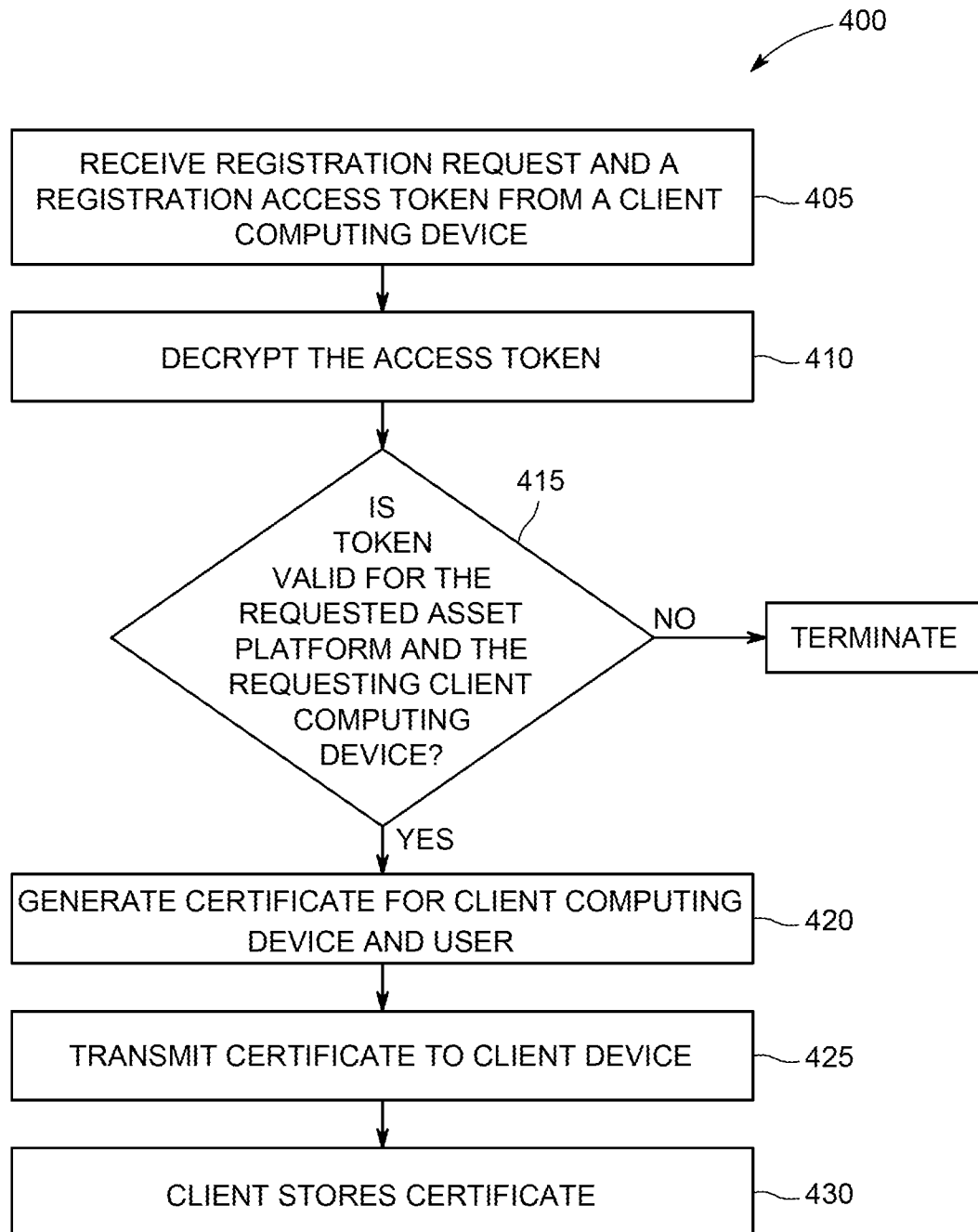


FIG. 4

5/5

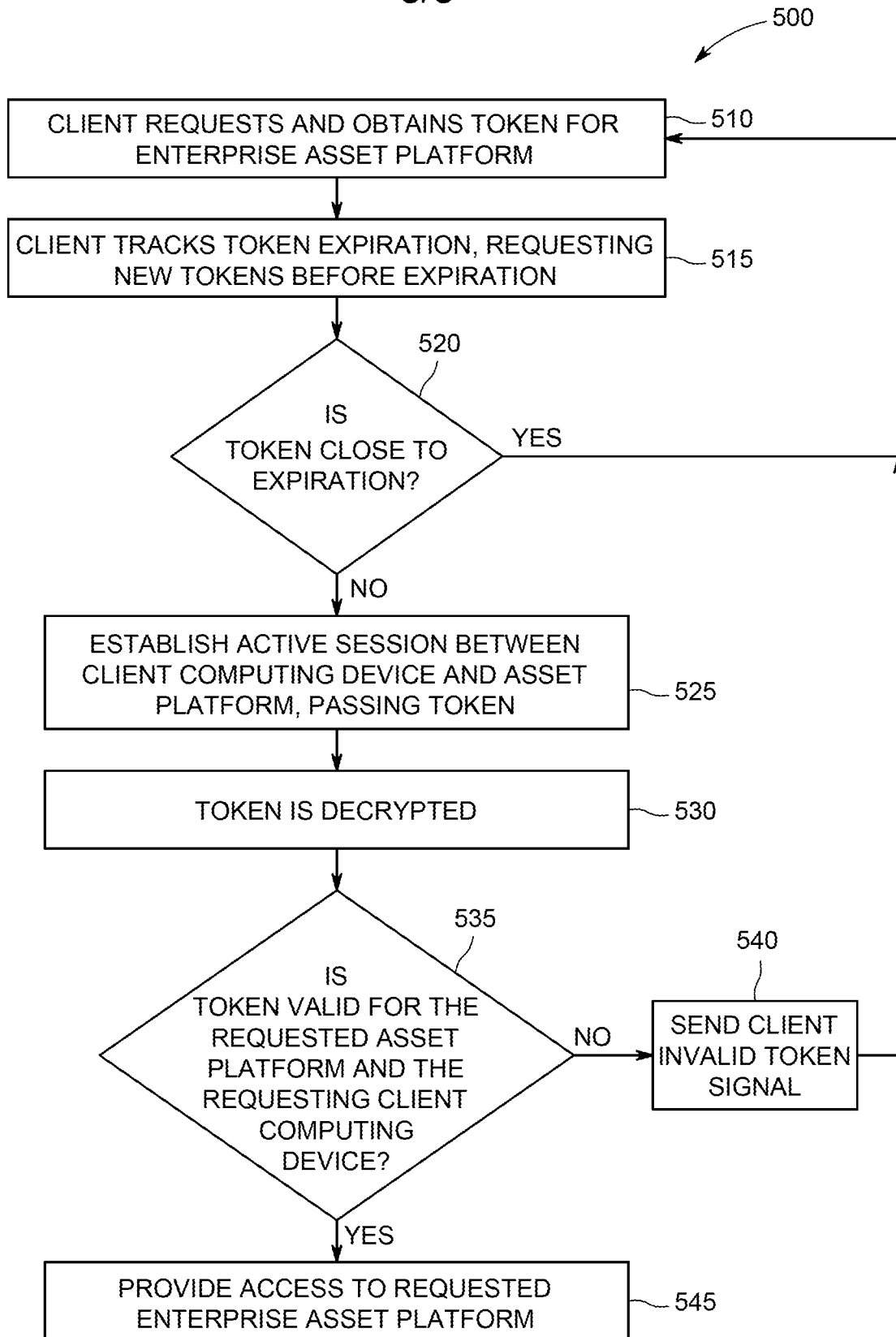


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2017/055103

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
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, COMPENDEX, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013/047228 A1 (RADHAKRISHNAN RAKESH [US]) 21 February 2013 (2013-02-21) paragraphs [0045], [0064], [0067], [0104], [0257]; figures 1, 8-10, 38 -----	1-20
X	US 2016/241599 A1 (QURESHI WAHEED [US]) 18 August 2016 (2016-08-18) paragraphs [0032] - [0038], [0064], [0086], [0117] - [0141] - paragraphs [0153] - [0186]; figures 1,7,8, 10-12 -----	1-20



Further documents are listed in the continuation of Box C.



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

29 November 2017

Date of mailing of the international search report

07/12/2017

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Schumann, Elena

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2017/055103

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013047228	A1	21-02-2013	NONE

US 2016241599	A1	18-08-2016	CN 105247531 A 13-01-2016
			EP 2979218 A1 03-02-2016
			JP 6131381 B2 17-05-2017
			JP 2016519817 A 07-07-2016
			JP 2017168111 A 21-09-2017
			KR 20160018476 A 17-02-2016
			KR 20170045372 A 26-04-2017
			US 8850010 B1 30-09-2014
			US 8850050 B1 30-09-2014
			US 2014297756 A1 02-10-2014
			US 2014297860 A1 02-10-2014
			US 2014297861 A1 02-10-2014
			US 2014298348 A1 02-10-2014
			US 2014298404 A1 02-10-2014
			US 2014298405 A1 02-10-2014
			US 2014298442 A1 02-10-2014
			US 2016241599 A1 18-08-2016
			WO 2014158228 A1 02-10-2014
