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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 February 2016 (04.02.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/018402 A1

(51) International Patent Classification:
H04L 12/66 (2006.01)

(21) International Application Number:
PCT/US2014/049268

(22) International Filing Date:
31 July 2014 (31.07.2014)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.** [US/US]; 11445 Compaq Center Drive West, Houston, Texas 77070 (US).

(72) Inventor: **NEAL-JOSLIN, Robert Raymond**; 4245 Technology Drive, Fremont, California 94538 (US).

(74) Agents: **SU, Benjamin** et al.; Hewlett-Packard Company, Intellectual Property Administration, 3404 E. Harmony Road, Mail Stop 35, Fort Collins, Colorado 80528 (US).

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

[Continued on next page]

(54) Title: SERVICE REQUEST MODIFICATION

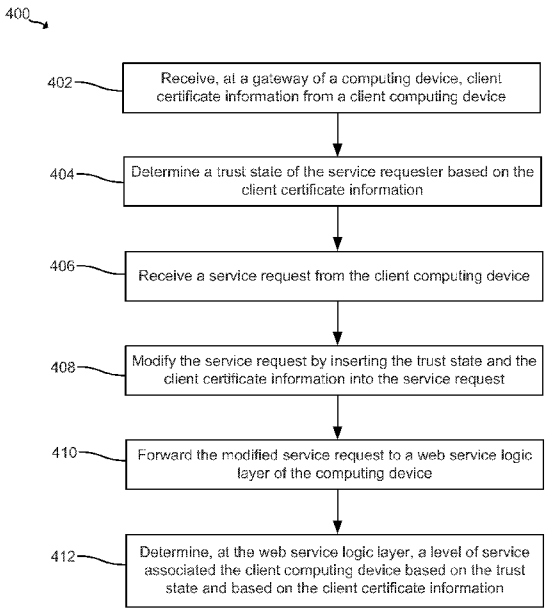

FIG. 4

(57) Abstract: Example implementations relate to providing a web service. For example, an implementation includes a gateway to receive client certificate information from the client computing device and to determine a trust state of the client computing device based on the client certificate information. The gateway is also to receive a service request from the client computing device and to modify the service request. The implementation also includes a web service logic layer to receive the modified service request including the trust state and to determine a level of service associated with the client computing device based on the modified service request.

WO 2016/018402 A1

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

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

SERVICE REQUEST MODIFICATION

BACKGROUND

[0001] In a web service framework, a computing device (service requester) may invoke a software application hosted on a remote computing device (service provider) over a network, such as the Internet, via a service request. For example, a service requester may invoke an application hosted on a service provider to perform credit card payment processing. As another example, a service requester may invoke an application on a service provider to receive stock quotes.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] Some examples of the present application are described with respect to the following figures:

[0003] FIG. 1 is a block diagram of a computing device to provide a web service to another computing device based on a modified service request, according to an example;

[0004] FIG. 2 is a block diagram of a computing device to provide a web service to another computing device based on a modified service request, according to another example;

[0005] FIG. 3 is a block diagram of a computing device to provide a web service to another computing device based on a modified service request, according to another example; and

[0006] FIG. 4 is a flow chart illustrating a method of a computing device providing a web service to a client computing device based on a modified service request, according to an example.

DETAILED DESCRIPTION

[0007] As described above, in a web service framework, a service requester may invoke a software application hosted on a service provider over the Internet via a service request. Prior to granting the service request, the service provider may perform an authentication process with the service requester to verify that the service requester is a trusted service requester. However, the service provider does not learn the identity of the service requester from the authentication process. Thus, the service provider cannot offer differentiated services to different service requesters based on identities of the different service requesters.

[0008] Examples described herein provide a gateway to forward client certificate information of a service requester to a web service logic layer of a service provider so that the web service logic layer may offer a particular level of service to the service requester based on an identity of the service requester. For example, a service requester may establish a connection with a gateway of a service provider via a cryptographic protocol, such as the secure sockets layer protocol. The gateway may receive client certificate information from the service requester during the process of establishing the connection. The gateway may determine a trust state of the service requester based on the client certificate information.

[0009] When the gateway receives a service request from the service requester, the gateway may modify the service request by inserting the trust state and client certificate information into a header portion of the service request. The gateway may forward the modified service request to a web service logic layer of the service provider. Based on the client certificate information, the web service logic layer may learn of the identity of the service requester. Thus, the web service logic layer may determine a level of service that is to be provided to the service requester. In this manner, examples described herein may enable a service provider to offer different levels of service to different service requesters.

[0010] Referring now to the figures, FIG. 1 is a block diagram of a computing device 100 to provide a web service to a client computing device

based on a modified service request, according to an example. As used herein, web service may be any type of processor executable instructions stored in a computing device that can be invoked over a network, such as the Internet, a local area network, a wide area network, etc., by another computing device.

[0011] Computing device 100 may be, for example, a smartphone, a tablet computing device, a notebook computing device, a server computing device, an electronic book reader, a desktop computing device, an all-in-one system, or any other electronic device suitable for providing a web service to another computing device. Thus, computing device 100 may be a service provider. Computing device 100 may include a gateway 102 and a web service logic layer 104. Gateway 102 may be component of computing device 100 to insert client certificate information and/or trust state of a client computing device 106 into a service request from the client computing device. Web service logic layer 104 may be a component of computing device 100 to provide a web service to the client computing device 106. Gateway 102 and web service logic layer 104 may be implemented using processor executable instructions.

[0012] During operation, a client computing device 106 (a service requester) may transmit client certificate information 108 to gateway 102 as part of a handshake process to establish a connection with gateway 102. Client computing device 106 may be, for example, a smartphone, a tablet computing devices, a notebook computing device, a desktop computing device, an electronic book reader, an all-in-one system or any other electronic device suitable for requesting a web service from another computing device.

[0013] Gateway 102 may determine a trust state of client computing device 106 based on client certificate information 108. Client computing device 106 may transmit a service request 110 to request a web service from computing device 100. In response to receiving service request 110, gateway 102 generates a modified service request 112 by modifying service request 110. Gateway 102 may modify service request 110 by inserting client certificate information 108 and the trust state into service request 110. Gateway 102 may forward modified service request 112 to web service logic layer 104. Based on modified service request 112, web service logic layer

104 may determine a level of service associated with client computing device 106.

[0014] FIG. 2 is a block diagram of a computing device 200 to provide a web service to another computing device based on a modified service request, according to another example. Computing device 200 may be similar to computing device 100 of FIG. 1. Computing device 200 may include a firewall 202, gateway 102, a web service interface layer 204, and web service logic layer 104. Firewall 202 may be a component of computing device 200 to filter incoming connection requests from client computing devices (e.g., client computing device 106) based on at least one forwarding criterion. Web service interface layer 204 may be a component of computing device 200 to translate or convert a service request from a first format to a second format that is used by web service logic layer 104. For example, web service interface layer 204 may translate a service request from a markup language format to an internal native computing device language format, such as C++ or JAVA. Firewall 202 and web service interface layer 204 may be implemented using processor executable instructions.

[0015] During operation, client computing device 106 may transmit a connection request 206 to gateway 102 to establish a connection for receiving a web service from computing device 200. Client computing device 106 may generate connection request 206 using a web service uniform resource locator (URL) that is provided to client computing device 106 via an out-of-band mechanism (e.g., a separate connection).

[0016] Firewall 202 may process incoming connection requests destined for gateway 102 to filter out malicious or erroneous connection requests and to accept connection requests for a web service. Thus, firewall 202 may protect other components of computing device 200, such as gateway 102, web service logic layer 104, etc., from being directly accessed. Firewall 202 may filter incoming connection requests based on at least one forwarding criterion. For example, firewall 202 may accept incoming connection requests transmitted via a particular network port. Firewall 202 may deny other incoming connection requests transmitted via a different network port by dropping the incoming connection requests.

[0017] In response to a determination that connection request 206 satisfies a forwarding criterion, firewall 202 may forward connection request 206 to gateway 102. In response to receiving connection request 206 at gateway 102, gateway 102 may establish a first connection 208 with client computing device 106 via a cryptographic protocol, such as secure sockets layer (SSL) protocol, transport layer security (TLS) protocol, etc. In some examples, first connection 208 may be a connection compliant with hypertext transfer protocol (HTTP).

[0018] To establish first connection 208 using the particular network port, gateway 102 and client computing device 106 may engage in a handshake process to exchange credentials. Client computing device 106 may transmit client certificate information 108 to gateway 102. Client certificate information 108 may include a copy of a client certificate 210, a copy of a certificate authority (CA) certificate 212 that signed client certificate 210, or a combination thereof. Client computing device 106 may receive client certificate 210 and/or CA certificate 212 from a certificate authority 214. Client certificate 210 and/or CA certificate 212 may be used to authenticate client computing device 106.

[0019] In response to receiving client certificate information 108, gateway 102 may cache client certificate information 108 or generate a fingerprint of client certificate information 108, such as a hash of client certificate information 108. Gateway 102 may associate first connection 208 with client certificate information 108 or the fingerprint. In addition, gateway 102 may determine a trust state of client computing device 106 based on client certificate information 108. For example, gateway 102 may compare client certificate information 108 to a known trusted service requester information database 218. The trust state may include a trusted service requester and an untrusted service requester. Gateway 102 may determine client computing device 106 as a trusted service requester when client certificate 210 is signed by a CA trusted by computing device 200, such as CA 214, as indicated in known trusted service requester information database 218. Gateway 102 may determine client computing device 106 as an untrusted service requester when client certificate 210 is not signed by a CA 214 trusted by computing device 200, such as an unverified CA, as indicated in known trusted service

requester information database 218. Gateway 102 may determine whether CA 214 is a trusted CA based on CA certificate 212 as indicated in known trusted service requester information database 218.

[0020] In response to establishing first connection 208 with gateway 102, client computing device 106 may transmit service request 110 to gateway 102 via first connection 208. Service request 110 may indicate the type of web service that client computing device 106 is requesting. Service request 110 may be a service request compliant with HTTP. In response to receiving service request 110, gateway 102 may generate modified service request 112 based on service request 110.

[0021] To generate modified service request 112, gateway 102 may insert client certificate information 108 and/or the trust state into a header portion of service request 110, such as a HTTP header portion, as cookies. In some examples, gateway 102 may insert the fingerprint of client certificate information 108 and/or the trust state into the header portion of service request 110 as cookies. Gateway 102 may also detect potential malicious service requests, such as a computer virus, by examining cookies included in the header portion. For example, gateway 102 may remove cookies in the header portion that contains the same cookie names as cookies used by gateway 102. Cookies that have the same cookie names as the cookies used by gateway 102 may indicate that the service request is trying to deceive web service logic layer 104. However, gateway 102 may not modify the remaining data of service request 110. Thus, modified service request 112 may include a header portion containing client certificate information 108 or the fingerprint of client certificate information 108 and the remaining data of service request 110.

[0022] Gateway 102 may forward modified service request 112 to web service logic layer 104 via web service interface layer 204 in a second connection 216. Gateway 102 may use a different network port to establish second connection 216 than the particular network port used to establish first connection 208. In response to receiving modified service request 112, web service interface layer 204 may convert modified service request 112 from a first format to a second format that is used by web service logic layer 104. For example, web service interface layer 204 may convert modified service

request 112 from a markup language, such as Extensible Markup Language, to an internal native computing device language format, such as C++ or JAVA. Web service interface layer 204 may forward the converted, modified service request 112 to web service logic layer 104.

[0023] Web service logic layer 104 may determine a level of service associated with client computing device 106 based on the converted modified service request 112 and provide a web service to client computing device 106 based on the level of service and the web service requested. For example, when the converted modified service request 112 indicates that client computing device 106 is a trusted service requester, web service logic layer 104 may determine the identity of client computing device 106 based on client certificate information 108 in the header portion of modified service request 112. Web service logic layer 104 may determine the level of service by identifying rights and/or privileges of the identity stored in known trusted service requester information database 218.

[0024] Thus, web service logic layer 104 may provide differentiated levels of service to different client computing devices that are trusted service requesters based on identities of the different client computing devices. For example, a first client computing device may have the rights to modify both an account user name and a password while a second client computing device may have the rights to modify the password, but not the user account name.

[0025] After identifying the rights and/or privileges of client computing device 106, web service logic layer 104 may provide a web service to client computing device 106 based on the web service requested and based on the identified rights and/or privileges. For example, web service logic layer 104 may invoke particular processor executable instructions based on the web service requested and based on the identified rights and/or privileges to generate a response 220. Response 220 may be data requested by client computing device 106. Web service logic layer 104 may forward response 220 to gateway 102 via web service interface layer 204. Gateway 102 may forward response 220 to client computing device 106 via firewall 202.

[0026] When the converted modified service request 112 indicates that client computing device 106 is an untrusted service requester, in some examples, web service logic layer 104 may provide a reduced level of service

to client computing device 106. Web service logic layer 104 may determine the reduced level of service using known trusted service requester information database 218. For example, client computing device 106 may request a web service to modify account information, when client computing device 106 is an untrusted service requester, web service logic layer 104 may display the account information instead. However, when client computing device 106 is a trusted service requester, web service logic layer 104 may grant the request to modify the account information.

[0027] In some examples, in response to a determination that client computing device 106 is an untrusted service requester, web service logic layer 104 may request client computing device 106 to supply additional credentials, such as a user name and a password, to authenticate client computing device 106. When client computing device 106 is authenticated, web service logic layer 104 may add client certificate information 108 to known trusted service requester information database 218 as a trusted service requester. Web service logic layer 104 may also update gateway 102 so that gateway 102 may recognize client computing device 106 as a trusted service requester for subsequent web service requests. Thus, when client computing device 106 requests a web service subsequently, client computing device 106 may be recognized as a trusted service requester and receive a higher level of service as compared to a level of service for an untrusted service requester.

[0028] FIG. 3 is a block diagram of a computing device 300 to provide a web service to another computing device based on a modified service request, according to another example. Computing device 300 may be similar to computing device 100 of FIG. 1 and/or computing device 200 of FIG. 2. Computing device 300 may include a processor 302 and a computer-readable storage medium 304.

[0029] Processor 302 may be a central processing unit (CPU), a semiconductor-based microprocessor, and/or other hardware devices suitable for retrieval and execution of instructions stored in computer-readable storage medium 304. Processor 302 may fetch, decode, and execute instructions 306-316 to control a process of providing a web service to a client computing device, such as client computing device 106 of FIG. 1, based on an identity of

the client computing device. As an alternative or in addition to retrieving and executing instructions, processor 302 may include at least one electronic circuit that includes electronic components for performing the functionality of instructions 306, 308, 310, 312, 314, 316, or a combination thereof.

[0030] Computer-readable storage medium 304 may be any electronic, magnetic, optical, or other physical storage device that contains or stores executable instructions. Thus, computer-readable storage medium 304 may be, for example, Random Access Memory (RAM), an Electrically Erasable Programmable Read-Only Memory (EEPROM), a storage device, an optical disc, etc. In some examples, computer-readable storage medium 304 may be a non-transitory storage medium, where the term "non-transitory" does not encompass transitory propagating signals. As described in detail below, computer-readable storage medium 304 may be encoded with a series of processor executable instructions 306-316 for providing a web service to a client computing device based on an identity of the client computing device.

[0031] Client certificate information reception instructions 306 may instruct processor 302 to receive client certificate information from a client computing device. For example, referring to FIG. 2, gateway 102 may receive client certificate information 108 from client computing device 106. Trust state determination instructions 308 may determine a trust state of a client computing device. For example, referring to FIG. 2, gateway 102 may determine a trust state of client computing device 106 based on client certificate information 108.

[0032] Service request reception instructions 310 may instruct processor 302 to receive a web service request from a client computing device. For example, referring to FIG. 2, gateway 102 may receive service request 110 from client computing device 106. Service request modification instructions 312 may modify a service request. For example, referring to FIG. 2, gateway 102 may modify service request 110 by inserting client certificate information 108 and/or the trust state into a header portion of service request 110 as cookies.

[0033] Modified service request forwarding instructions 314 may forward a modified service request from a gateway to a web service logic layer. For example, referring to FIG. 2, gateway 102 may forward modified service

request 112 to web service logic layer 104 via web service interface layer 204. Service provision instructions 316 may provide a differentiated level of service to a client computing device based on client certificate information of the client computing device. For example, referring to FIG. 2, when the converted modified service request 112 indicates that client computing device 106 is a trusted service requester, web service logic layer 104 may determine the identity of client computing device 106 based on client certificate information 108 in the header portion of modified service request 112. Web service logic layer 104 may determine the level of service by identifying rights and/or privileges of the identity stored in a known trusted service requester information database 218.

[0034] FIG. 4 is a flow chart illustrating a method 400 of a computing device, such as computing device 100 of FIG. 1 or computing device 200 of FIG. 2, providing a web service to a client computing device based on a modified service request, according to an example. Method 400 may be implemented using computing device 100 of FIG. 1 and/or computing device 200 of FIG. 2. Method 400 includes receiving, at a gateway of a computing device, client certificate information from a client computing device, at 402. For example, referring to FIG. 2, gateway 102 may receive client certificate information 108 from client computing device 106.

[0035] Method 400 also includes determining a trust state of the service requester based on the client certificate information, at 404. For example, referring to FIG. 2, gateway 102 may determine a trust state of client computing device 106. Method 400 further includes receiving a service request from the client computing device, at 406. For example, referring to FIG. 2, gateway 102 may receive service request 110 from client computing device 106.

[0036] Method 400 further includes modifying the service request by inserting the trust state and the client certificate information into the service request, at 408. For example, referring to FIG. 2, gateway 102 may modify service request 110 by inserting client certificate information 108 and/or the trust state into a header portion of service request 110 as cookies.

[0037] Method 400 further includes forwarding the modified service request to a web service logic layer of the computing device, at 410. For

example, referring to FIG. 2, gateway 102 may forward modified service request 112 to web service logic layer 104. Method 400 further includes determining, at the web service logic layer, a level of service associated the client computing device based on the trust state and based on the client certificate information, at 412. For example, referring to FIG. 2, web service logic layer 104 may determine a level of service associated with client computing device 106 based on the converted modified service request 112 and provide a web service to client computing device 106 based on the level of service and the web service requested.

[0038] According to the foregoing, examples disclosed herein enable a computing device to provide a web service based on an identity of a client computing device that requests the web service. A gateway of the computing device may modify a head portion of a service request by inserting client certificate information and/or trust state of the client computing device into the header portion. The gateway may forward the modified service request to a web service logic layer of the computing device. The web service logic layer may learn of the identity of the client computing device using the client certificate information. Thus, the web service logic layer may provide a differentiated level of service to the client computing device based on the identity of the client computing device.

[0039] The use of "comprising", "including" or "having" are synonymous and variations thereof herein are meant to be inclusive or open-ended and do not exclude additional unrecited elements or method steps.

Claims

What is claimed is:

1. An apparatus comprising:

a gateway to:

establish a connection with a client computing device via a cryptographic protocol;

receive client certificate information from the client computing device;

determine a trust state of the client computing device based on the client certificate information;

receive a service request from the client computing device via the connection; and

generate a modified service request based on the trust state; and

a web service logic layer to:

receive the modified service request including the trust state; and

determine a level of service associated the client computing device based on the trust state.

2. The apparatus of claim 1, further comprising:

a firewall connected to the gateway, wherein the firewall is to:

receive a connection request from the client computing device; and

forward the connection request to the gateway in response to a determination that the connection request matches a forwarding criterion; and

a web service interface layer connected to the gateway, wherein the web service interface layer is to:

receive the modified service request;

convert the modified service request from a first format to a second format; and

forward the converted modified service request to the web service logic layer.

3. The apparatus of claim 2, wherein the gateway is further to:

establish the connection via a first network port;

establish a second connection with the web service interface layer via a second network port; and

forward the modified service request to the web service interface layer via the second connection.

4. The apparatus of claim 1, wherein the gateway is further to modify the service request by inserting the trust state and the client certificate into the service request.

5. The apparatus of claim 1, wherein when the trust state indicates that the client computing device is a trusted service requester, the web service logic layer is to provide a first level of service to the client computing device, and wherein when the trust state indicates that the client computing device is an untrusted service requester, the web service logic layer is to provide a second level of service to the client computing device that is different from the first level of service.

6. The apparatus of claim 1, wherein the cryptographic protocol includes a transport layer security protocol and a secure sockets layer protocol.

7. A method comprising:

receiving, at a gateway of a computing device, client certificate information from a client computing device;

determining a trust state of the client computing device based on the client certificate information;

receiving a service request from the client computing device;

modifying the service request by inserting the trust state and the client certificate information into the service request;

forwarding the modified service request to a web service logic layer of the computing device; and

determining, at the web service logic layer, a level of service associated the client computing device based on the trust state and based on the client certificate information.

8. The method of claim 7, wherein modifying the service request further includes removing a first cookie in a hypertext transfer protocol (HTTP) header portion of the service request that contains the same name as a second cookie used by the gateway.

9. The method of claim 7, further comprising:

establishing, at the gateway, a first connection with the client computing device via a first network port; and

establishing, at the gateway, a second connection with the web service logic layer via a second network port, wherein the modified service request is forwarded via the second connection.

10. The method of claim 7, wherein the level of service is determined via a known trusted service requester information database.

11. A computer-readable storage medium comprising instructions that when executed by a processor of a computing device cause the computing device to:

receive, at a gateway of the computing device, client certificate information from a client computing device;

determine a trust state of the client computing device based on the client certificate information;

receive a service request from the client computing device;

modify the service request by inserting the trust state and the client certificate information into the service request;

forward the modified service request to a web service logic layer of the computing device;

provide, via the web service logic layer, a first level of service to the client computing device in response to a first determination that the client computing device is a trusted service requester; and

provide a second level of service to the client computing device in response to a second determination that the client computing device is an untrusted service requester.

12. The computer-readable storage medium of claim 11, wherein the second level of service corresponds to requesting a user name and a password from the client computing device to authenticate the client computing device.

13. The computer-readable storage medium of claim 11, wherein the second level of service corresponds to a reduced level of service as compared to the first level of service.

14. The computer-readable storage medium of claim 11, wherein the client certificate information includes a copy of a client certificate of the client computing device, a copy of a certificate authority certificate that signed the client certificate, or a combination thereof.

15. The computer-readable storage medium of claim 11, wherein the first level of service is determined via a known trusted service requester information database.

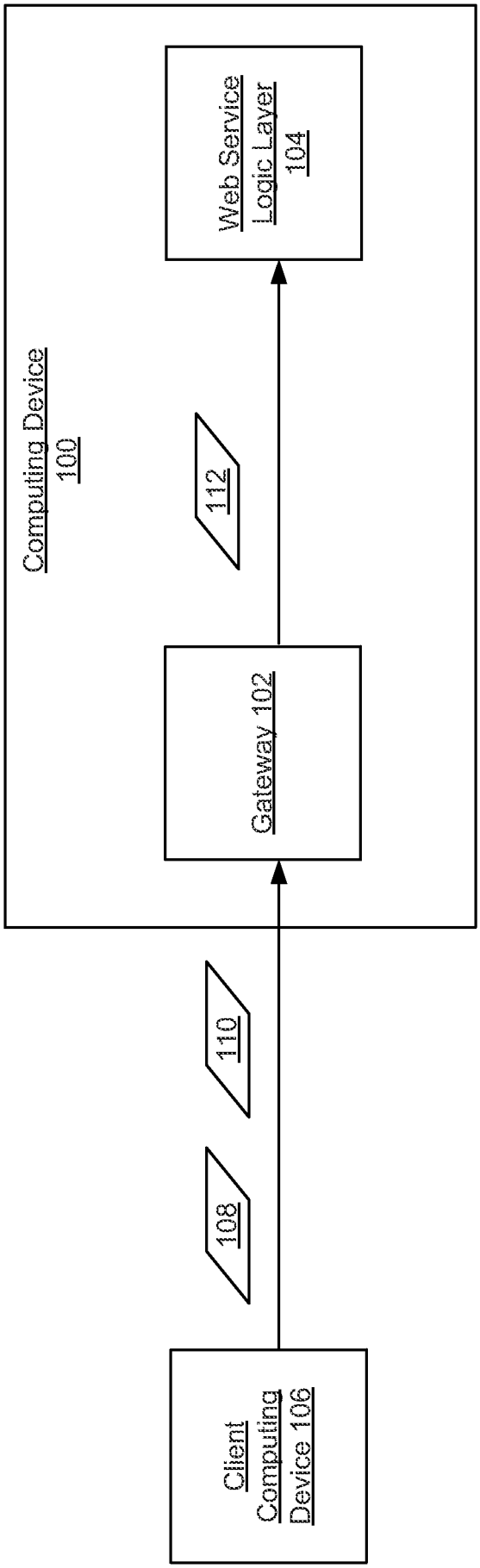
Client Computing Device 106
108
110
Computing Device 100
Gateway 102
112
Web Service Logic Layer 104

FIG. 1

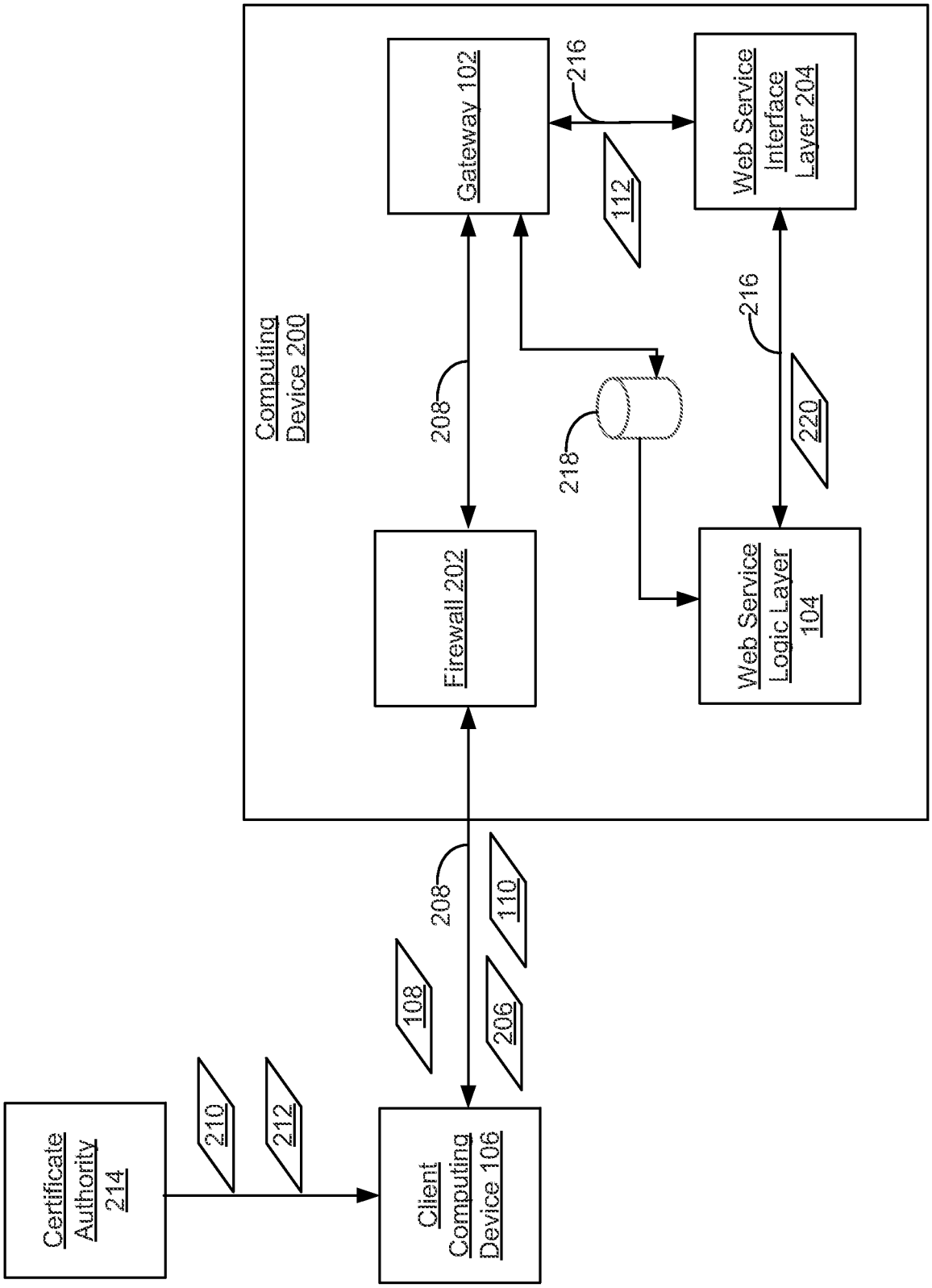
Computing Device 200
Gateway 102
216
Web Service Interface Layer 204
112
216
208
218
220
Firewall 202
Web Service Logic Layer 104
208
110
108
206
Certificate Authority 214
210
212
Client Computing Device 106

FIG. 2

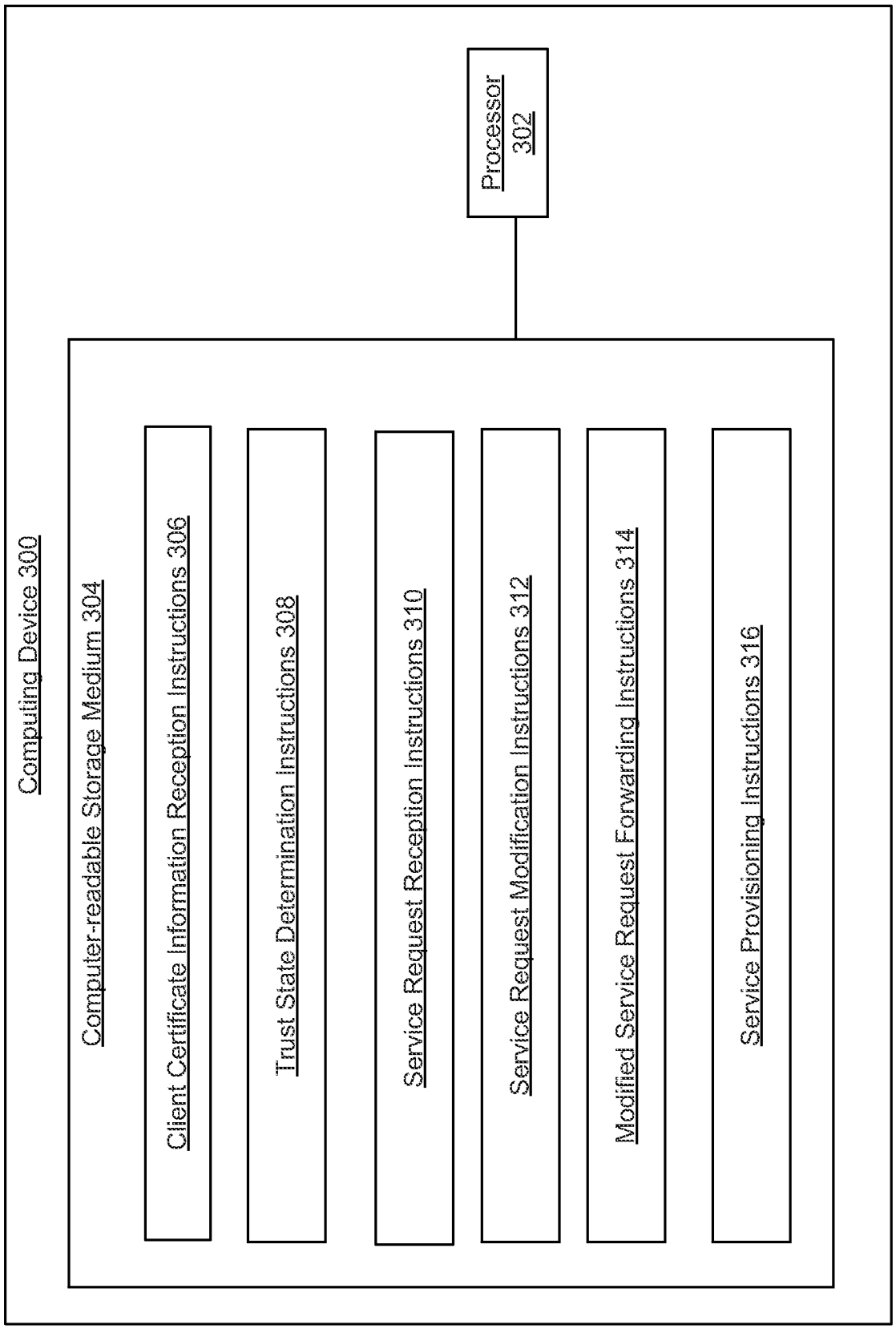
Computing Device 300
Processor 302
Computer-readable Storage Medium 304
Client Certificate Information Reception Instructions 306
Trust State Determination Instructions 308
Service Request Reception Instructions 310
Service Request Modification Instructions 312
Modified Service Request Forwarding Instructions 314
Service Provisioning Instructions 316

FIG. 3

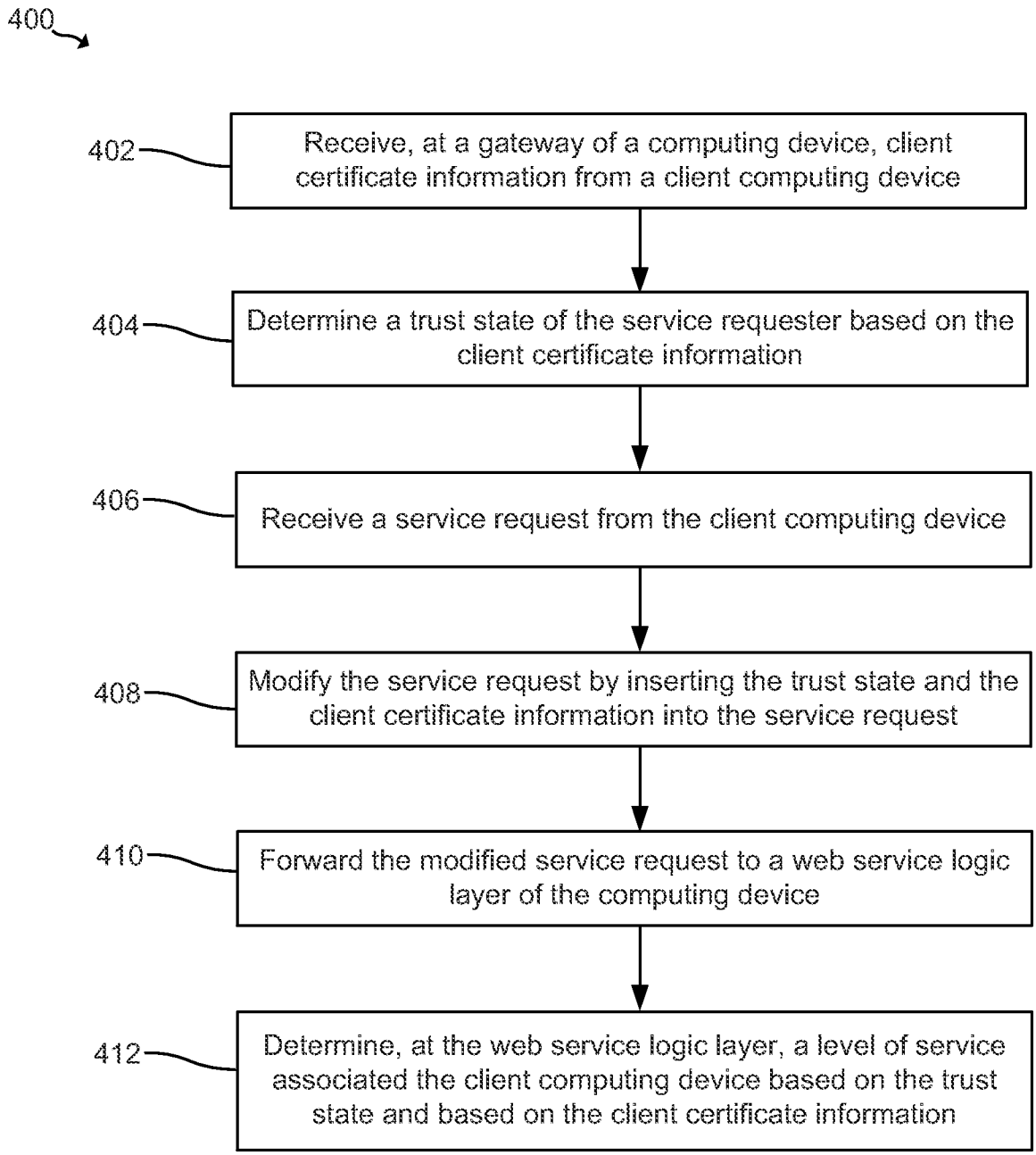
400
402
Receive, at a gateway of a computing device, client certificate information from a client computing device
404
Determine a trust state of the service requester based on the client certificate information
406
Receive a service request from the client computing device
408
Modify the service request by inserting the trust state and the client certificate information into the service request
410
Forward the modified service request to a web service logic layer of the computing device
412
Determine, at the web service logic layer, a level of service associated the client computing device based on the trust state and based on the client certificate information

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/049268

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/66(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L 12/66; G06F 15/16; H04J 3/22; G06F 17/00; G06F 7/00; H04L 9/32; G06F 21/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: modified, service, request, trust, level, and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2007-0094283 A1 (HALEY HOI LEE FUNG et al.) 26 April 2007 See paragraphs [0044], [0055]; and figure 1.	1-15
A	US 2014-0101774 A1 (JOHN P. ARMINGTON et al.) 10 April 2014 See paragraphs [0023]-[0050]; and figures 1-4.	1-15
A	US 2009-0196308 A1 (QIULING PAN et al.) 06 August 2009 See paragraphs [0037]-[0052]; and figure 3.	1-15
A	US 2005-0198154 A1 (NAN XIE et al.) 08 September 2005 See paragraphs [0031]-[0042]; and figure 2.	1-15
A	US 2008-0263652 A1 (CRAIG V. MCMURTRY et al.) 23 October 2008 See paragraphs [0031]-[0044]; and figures 3-4.	1-15

☐ 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	Date of mailing of the international search report
30 March 2015 (30.03.2015)	**15 April 2015 (15.04.2015)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701,
Republic of Korea
Facsimile No. ++82 42 472 7140

Authorized officer
KIM, Seong Woo
Telephone No. +82-42-481-3348

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2014/049268

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007-0094283 A1	26/04/2007	US 07818294 B2	19/10/2010
		US 2007-0083524 A1	12/04/2007
US 2014-0101774 A1	10/04/2014	EP 2697943 A1	19/02/2014
		EP 2697943 A4	17/12/2014
		WO 2012-166087 A1	06/12/2012
US 2009-0196308 A1	06/08/2009	CN 101163120 A	16/04/2008
		CN 101163120 B	21/12/2011
		EP 2079197 A1	15/07/2009
		EP 2079197 A4	02/06/2010
		PI 0719254 A2	28/01/2014
		WO 2008-046287 A1	24/04/2008
US 2005-0198154 A1	08/09/2005	US 08516123 B2	20/08/2013
		WO 2005-081495 A1	01/09/2005
US 2008-0263652 A1	23/10/2008	CN 101663670 A	03/03/2010
		EP 2149102 A1	03/02/2010
		EP 2149102 A4	14/05/2014
		JP 2010-525448 A	22/07/2010
		JP 5334332 B2	06/11/2013
		US 08656472 B2	18/02/2014
		US 2014-143546 A1	22/05/2014
		WO 2008-130760 A1	30/10/2008