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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 March 2010 (25.03.2010)

PCT

(10) International Publication Number
WO 2010/033336 A1

(51) International Patent Classification:
G06F 21/00 (2006.01) *H04L 29/06* (2006.01)

(21) International Application Number:
PCT/US2009/054389

(22) International Filing Date:
20 August 2009 (20.08.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12/233,279 18 September 2008 (18.09.2008) US

(71) Applicant *(for all designated States except US)*: **MOTOROLA, INC.** [US/US]; 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **UPP, Steven, D.** [US/US]; 331 Wentworth Lane, Bartlett, IL 60103 (US). **MEDVINSKY, Alexander** [US/US]; 8873 Hampe Court, San Diego, CA 92129 (US). **NAKHJIRI, Madjid, F.** [US/US]; 4689 Taratella Lane, San Diego, CA 92130 (US).

(74) Agents: **PACE, Lalita W.,** et al.; 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

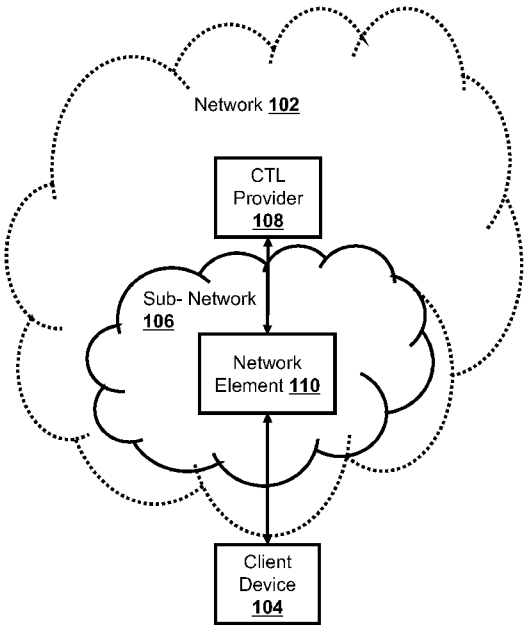
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (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, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SECURE SERVER CERTIFICATE TRUST LIST UPDATE FOR CLIENT DEVICES

(57) Abstract: A method, a network element, and a client device for creating a trusted connection with a network are disclosed. A client device 104 may attempt to access a sub-network 106. The client device 104 may determine that a certificate of the sub-network 106 is issued by a certification authority absent from a device certificate trust list. The client device 104 may receive via the sub-network 106 a certificate trust list update 400 from a certificate trust list provider 108.



100

Figure 1

WO 2010/033336 A1

Published:

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

SECURE SERVER CERTIFICATE TRUST LIST UPDATE FOR CLIENT DEVICES

1. Field of the Invention

[0001] The present invention relates to a method and system for authenticating network elements. The present invention further relates to updating a certificate trust list.

2. Introduction

[0002] A certification authority (CA) may issue a certificate to a communication entity, such as a network, sub-network, or website, to ensure the trustworthiness of that entity. A client device that seeks access to the communication entity or receives information from the communication entity may request the certificate. The client device may then compare the certificate for the certification authority of the certificate with a certificate trust list stored by the client device. For simplicity in this situation, the certificate authority may be referred to as being present on the certificate trust list. If the certification authority is present on the certificate trust list, the client device may connect with the communication entity or accept the information received from the communication entity with full assurances. If the certification authority is not present on the certificate trust list, the client device may choose to avoid connecting with the communication entity or accepting the information received from the communication entity, till such time as the communication entity is vouched as safe. The absence of a certification authority from a certificate trust list may not necessarily mean that the communication entity is not safe, as the certificate trust list may not be up to date.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] Understanding that these drawings depict only typical embodiments of the invention and are not therefore to be considered to be limiting of its scope, the invention will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

[0004] **Figure 1** illustrates one embodiment of a communication system.

[0005] **Figure 2** illustrates a possible configuration of a computing system to act as an access point.

[0006] **Figure 3** is a block diagram that illustrates one embodiment of a user communication device, or terminal, capable of acting as a client device.

[0007] **Figure 4** is a block diagram that illustrates one embodiment of a certificate trust list update.

[0008] **Figure 5** is a flowchart that illustrates one embodiment of a method for updating the certificate trust list with a certificate trust list update stored at the access point.

[0009] **Figure 6** is a block diagram that illustrates one embodiment of an initial sub-network message.

[0010] **Figure 7** is a flowchart that illustrates one embodiment of a method for updating the certificate trust list using a protected access mode with disconnect.

[0011] **Figure 8** is a flowchart that illustrates one embodiment of a method for updating the certificate trust list with a protected access mode without disconnect.

DETAILED DESCRIPTION OF THE INVENTION

[0012] Additional features and advantages of the invention will be set forth in the description which follows, and in part will be obvious from the description, or may be learned by practice of the invention. The features and advantages of the invention may be realized and obtained by means of the instruments and combinations particularly pointed out in the appended claims. These and other features of the present invention will become more fully apparent from the following description and appended claims, or may be learned by the practice of the invention as set forth herein.

[0013] Various embodiments of the invention are discussed in detail below. While specific implementations are discussed, it should be understood that this is done for illustration purposes only. A person skilled in the relevant art will recognize that other components and configurations may be used without parting from the spirit and scope of the invention.

[0014] The present invention comprises a variety of embodiments, such as a method, an apparatus, and an electronic device, and other embodiments that relate to the basic concepts of the invention. The electronic device may be any manner of computer, mobile device, or wireless communication device.

[0015] A method, a network element, and a client device for creating a trusted connection with a network are disclosed. A client device may attempt to access a sub-network and receive a certificate from a network element of the sub-network, such as an authentication, authorization, and accounting (AAA) server. The client device may determine that a certificate of the sub-network is untrustworthy due to the fact that the certificate or certificates is from an issuing certification authority absent from a device certificate store. Alternatively, the entire chain of trust for the network element certificate may be missing from the device certificate store. The client device may receive

via the sub-network a certificate trust list update from a certificate trust list provider in a manner that may limit the interactions with the sub-network to modification of the certificate trust list. The client may then attach to the sub-network again and verify the identity of the sub-network.

[0016] **Figure 1** illustrates one embodiment of a communication system 100. The communication system 100 may include a network 102 and a client device 104. Various communication devices may exchange data or information through the network 102. The network 102 may be an internet protocol (IP) network such as a local area network (LAN), a wide area network (WAN), a wireless local area network (WLAN), the internet or any other type of network. Various communication devices of the network may be grouped into a sub-network 106. The sub-network 106 may, among other services, be an access network or a control network, to provide access to a greater network or to provide configuration information, such as a certificate trust list (CTL), to a client device 110. Member devices of the sub-network 106 may be certified by a certification authority, testifying to the authenticity and trustworthiness of each member device. The sub-network may be a channel in an internet protocol television (IPTV). The chain of trust for each trusted certification authority for each sub-network may be stored on a CTL, maintained by a CTL provider 108. The CTL provider 108 may be a server or other readily accessible storage source of a CTL.

[0017] The client device 104 may connect to the sub-network 106 via a network element 110. For one embodiment, the network element 110 may be a distributed set of servers in the network, including an AAA server. The client device 104 may be one of several types of handheld devices, such as, a mobile phone, a laptop, or a personal digital assistant (PDA). For one embodiment, the client device 104 may be a WiFi capable device, a WiMax capable device, or other wireless devices. The wireless devices may

transmit data using cellular packet data formats such as general packet radio service (GPRS), enhanced data rates for global evolution (EDGE), universal mobile telecommunications system (UMTS), evolution data optimized (EvDO) format, or other cellular packet data formats. In one embodiment, the client device 104 may connect to the network 102 via a wireline or virtual private network (VPN) access. The WiFi capable device may be used to access the network 102 for data or by voice using voice over Internet protocol (VOIP).

[0018] **Figure 2** illustrates a possible configuration of a computing system to act as a network element 110. The network element 110 may include a controller/processor 210, a memory 220, an AAA server interface 230, a transceiver 240, input/output (I/O) device interface 250, and a network interface 260, connected through bus 270. The network element 110 may implement any operating system, such as Microsoft Windows®, UNIX, or LINUX, for example. Client and server software may be written in any programming language, such as C, C++, Java or Visual Basic, for example. The server software may run on an application framework, such as, for example, a Java ® server or .NET ® framework.

[0019] The controller/processor 210 may be any programmed processor known to one of skill in the art. However, the method for authenticating a connection with a client device 104 may also be implemented on a general-purpose or a special purpose computer, a programmed microprocessor or microcontroller, peripheral integrated circuit elements, an application-specific integrated circuit or other integrated circuits, hardware/electronic logic circuits, such as a discrete element circuit, a programmable logic device, such as a programmable logic array, field programmable gate-array, or the like. In general, any device or devices capable of implementing the method for

authenticating a connection with a client device as described herein may be used to implement the system functions of this invention.

[0020] The memory 220 may include volatile and nonvolatile data storage, including one or more electrical, magnetic or optical memories such as a random access memory (RAM), cache, hard drive, or other memory device. The memory may have a cache to speed access to specific data. The memory 220 may also be connected to a compact disc – read only memory (CD-ROM), digital video disc – read only memory (DVD-ROM), DVD read write input, tape drive, or other removable memory device that allows media content to be directly uploaded into the system.

[0021] The network element 110 may have an AAA server interface 230 to interact with an AAA server. The network element 110 may use the AAA server to regulate and control access of the sub-network 106 by the client device 104. The AAA server may store a certificate from a certification authority, as well as any updates to the CTL. The AAA server may typically interact with the client device through the network element 110, acting as a pass-through entity. The AAA server may own a certificate issued by the certificate authority. The AAA server may present this certificate to the client device as part of an access control authentication process.

[0022] The transceiver 240 may create a data connection with the client device 104. The I/O device interface 250 may be connected to one or more input devices that may include a keyboard, mouse, pen-operated touch screen or monitor, voice-recognition device, or any other device that accepts input. The I/O device interface 250 may also be connected to one or more output devices, such as a monitor, printer, disk drive, speakers, or any other device provided to output data. The I/O device interface 250 may receive a data task or connection criteria from a network administrator.

[0023] The network interface 260 may be connected to a communication device, modem, network interface card, a transceiver, or any other device capable of transmitting and receiving signals from the network 104. The network interface 260 may act as a sub-network interface. The network connection interface 260 may be used to connect a client device to a network. The components of the network element 110 may be connected via an electrical bus 270, for example, or linked wirelessly.

[0024] Client software and databases may be accessed by the controller/processor 210 from memory 220, and may include, for example, database applications, word processing applications, as well as components that embody the functionality of the present invention. The network element 110 may implement any operating system, such as Microsoft Windows®, LINUX, or UNIX, for example. Client and server software may be written in any programming language, such as C, C++, Java or Visual Basic, for example. Although not required, the invention is described, at least in part, in the general context of computer-executable instructions, such as program modules, being executed by the electronic device, such as a general purpose computer. Generally, program modules include routine programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Moreover, those skilled in the art will appreciate that other embodiments of the invention may be practiced in network computing environments with many types of computer system configurations, including personal computers, hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, and the like.

[0025] **Figure 3** illustrates one embodiment of a user communication device, or terminal, capable of acting as a client device 104. The client device 104 may be capable of accessing the information or data stored in the network 102 or sub-network 106. For

some embodiments of the present invention, the client device 104 may also support one or more applications for performing various communications with the network 102 or sub-network 106. The client device 104 may be a handheld device, such as, a mobile phone, a laptop, or a personal digital assistant (PDA). For some embodiments of the present invention, the client device 104 may be WiFi® capable device, which may be used to access the network 102 or sub-network 106 for data or by voice using VOIP.

[0026] The client device 104 may include a transceiver 302, which is capable of sending and receiving data over the network 102 or sub-network 106. The client device 104 may include a processor 304 that executes stored programs. The client device 104 may also include a data storage, such as a volatile memory 306 or a non-volatile memory 308, which are used by the processor 304. The client device 104 may store a CTL in a certificate store in the non-volatile memory 308. The client device 104 may include a user input interface 310 that may comprise elements such as a keypad, display, touch screen, and the like. The client device 104 may also include a user output device that may comprise a display screen and an audio interface 312 that may comprise elements such as a microphone, earphone, and speaker. The client device 104 also may include a component interface 314 to which additional elements may be attached, for example, a universal serial bus (USB) interface. Finally, the client device 104 may include a power supply 316.

[0027] The CTL update may be stored upon the AAA server associated with the network element 110 or maintained at the CTL provider 108. **Figure 4** illustrates one embodiment of a CTL update 400. The CTL update may be signed by an authority, with a certificate that the client device 104 trusts. The CTL update 400 may have a CTL provider identifier 402 to allow a client device 104 to identify the CTL provider 108 and to protect the client device 104 from receiving a spoofed CTL 400. The CTL update 400

may have a CTL timestamp 404 to allow a client device 104 to determine if the CTL update 400 predates the CTL stored by the client device 104 in the non-volatile memory 308. The CTL update 400 may have a root certificate 406 indicating the originating trusted source. The CTL provider 108 may determine from a timestamp sent by the client device 104 what new CAs 408 are required by the client device 104 and send just the new CAs 408 to improve transmission efficiency.

[0028] **Figure 5** illustrates one embodiment of a method 500 for updating the CTL with a CTL update 400 stored at the network element 110 or at a location accessible by the network element 110. The client device 104 may attempt to access the sub-network 106 (Block 502). The client device 104 may receive an initial message with a certificate check indicator from the sub-network 106, prompting the client device 104 to check the certificate of the sub-network 106 against the device CTL (Block 504). If the certificate for the network element 110, such as an AAA server, is issued by a certification authority on the device CTL (Block 506), then the client device 104 may complete access to the sub-network 106 (Block 508). If the certificate or root certificate for the network element 110 is absent from the device CTL (Block 506), then the client device 104 may request a CTL update 400 (Block 510). The client device 104 may receive a CTL update 400 stored on the network element 110 (Block 512). The network element may send the CTL update 400 in the form of a media access control (MAC) layer message to the client device 104. The client device 104 may amend the CTL based upon the CTL update 400 (Block 514). If the certificate for the sub-network 106 is issued by a certification authority on the updated device CTL (Block 516), then the client device 104 may complete access to the sub-network 106 (Block 508). If the certificate for the sub-network 106 is issued by a certification authority absent from the update device CTL

(Block 516), then the client device 104 may refuse network entry and seek out an alternative sub-network (Block 518).

[0029] **Figure 6** illustrates one embodiment of an initial sub-network message 600. The initial sub-network message 600 may have a certificate check indicator 610, or a piece of data that may prompt the client device to check the certificate of the sub-network against the device CTL. The certificate check indicator may be an identifier (ID) 612 of the network element 110 or an ID 614 of the service or network provider. The initial sub-network message may also have data informing the client device 104 of the location 620 of the CTL provider 108.

[0030] **Figure 7** illustrates one embodiment of a method 700 for updating the CTL using a protected access mode with disconnect. The client device 104 may attempt to access the sub-network 106 (Block 702). If the certificate for the sub-network 106 is issued by a certification authority on the device CTL (Block 704), then the client device 104 may complete access to the sub-network 106 (Block 706). If the certificate for the sub-network 106 is issued by a certification authority absent from the device CTL (Block 704), then the client device 104 may disconnect from the sub-network 106 (Block 708). The client device 104 may include with a network entry a CTL update request to the network element 110 that the client device 104 is seeking a CTL update 400 (Block 710). The client device 104 may include an update request flag as part of a network access identifier (NAI) before sending the NAI to the network element 110 of the sub-network. The client device 104 may enter the sub-network 106 in a protected access mode (712). The protected mode may allow the client device 104 to access the sub-network in a limited fashion, only accepting messages from the CTL provider 108. The client device 104 may retrieve the CTL update 400 from the CTL provider 108 (Block 714). The client device 104 may disconnect from the sub-network 106 (Block 716).

[0031] The client device 104 may amend the CTL based upon the CTL update 400 (Block 718). If the certificate for the sub-network 106 is issued by a certification authority on the updated device CTL (Block 720), then the client device 104 may complete access to the sub-network 106 in an open access mode, allowing unfettered access to the sub-network 106 (Block 706). If the certificate for the sub-network 106 is issued by a certification authority absent from the update device CTL (Block 720), then the client device 104 may refuse network entry and seek out an alternative sub-network (Block 722).

[0032] **Figure 8** illustrates one embodiment of a method 800 for updating the CTL with a protected access mode without disconnect. The client device 104 may attempt to access the sub-network 106 (Block 802). If the certificate for the sub-network 106 is issued by a certification authority on the device CTL (Block 804), then the client device 104 may complete access to the sub-network 106 (Block 806). If the certificate for the sub-network 106 is issued by a certification authority absent from the device CTL (Block 804), then the client device 104 may disconnect from the sub-network 106 (Block 808). The client device 104 may append an update request flag, indicating that a CTL update 400 is requested, as part of a network entry (Block 810). The client device 104 may include the update request flag as part of a network access identifier (NAI) before sending the NAI to the network element 110 of the sub-network. The client device 104 may enter the sub-network 106 in a protected access mode (812). The client device 104 may retrieve the CTL update 400 from the CTL provider 108 (Block 814). The client device 104 may amend the CTL based upon the CTL update 400 (Block 816). If the certificate for the sub-network 106 is issued by a certification authority absent from the update device CTL (Block 818), then the client device 104 may refuse network entry and seek out an alternative sub-network (Block 820). If the certificate for the sub-network

106 is issued by a certification authority on the updated device CTL (Block 818), then the client device 104 may enter an open access mode, allowing unfettered access to the sub-network 106 (Block 822).

[0033] Much like network access service provided to a mobile, wireless device, configuration, monitoring, or specific software application access, such as video, may be considered a service provided to the device. In such scenarios, internet protocol (IP) connectivity may have already been established, but the device may seek information about a server providing a specific service or configuration or software. The device may seek to establish secure sessions with these servers before trusting the information received or making transactions.

[0034] Internet protocol television (IPTV) providers may use a remote configuration management server (RCMS). The IPTV receiving device may receive information about various network servers from the RCMS. The address of the RCMS may be provided to the IPTV receiving devices. Dynamic host configuration protocol (DHCP) options may provide the address of the RCMS, a CTL update, a certificate check indicator, or a certificate trust list provider location. If the IPTV receiving device is to establish a secure socket layer (SSL)/transport layer security (TLS) session with or receive signed information from the RCMS server, a trustworthy RCMS certificate may be useful. Thus potentially an IPTV receiving device may deal with an RCMS that possesses a certificate issued by a trust authority that is unrecognizable by the IPTV device.

[0035] In addition to using MAC messaging to deliver a CTL update 400 before gaining network entry, a network element 110 may use a network configuration protocol to deliver the CTL as part of IP network connectivity establishment, such as through DHCP or even after the IP network connectivity is established, as part of a configuration protocol, such as network configuration (NETCONF). In such cases, the network

element 110 may deliver the CTL update 400 as an option or an extension to the network protocol.

[0036] One DHCP option may provide the uniform resource locater (URL) or other access information for the RCMS, such as a subject name and CA name for the RCMS certificate. If the IPTV receiving device determines that it does not recognize the CA name, the IPTV device may request that a CTL be downloaded as a different DHCP option to prevent SSL/TLS failure.

[0037] NETCONF protocol may be used to manage network devices, retrieve configuration data information, and upload and manipulate new configuration data. The NETCONF protocol may allow the device to expose a full, formal application programming interface (API). Applications may use the API to send and receive full and partial configuration data sets. Any IPTV service that may use configuration information in order to set the service up may receive such information through setting up a NETCONF connection with the configuration or service providing servers.

[0038] The NETCONF protocol may use a remote procedure call (RPC) paradigm. A client may send one or more RPC requests, to which the server may respond with a series of RPC replies. The RPC replies may communicate a CTL update, a certificate check indicator, or a certificate trust list provider location to the client device 104. NETCONF protocol exchanges may be typically carried over a transport protocol. The RPC requests and responses may be encoded in extendable markup language (XML). As NETCONF connections may provide integrity and confidentially protection, the NETCONF connections may be carried over TLS or secure shell (SSH). When NETCONF connections are used for configuration, the device may establish a TLS session to provide the underlying secure connection for a NETCONF connection with a NETCONF server, with a recognizable and trustworthy certificate. After the TLS and

NETCONF connection is set up, the IPTV device may download the CTL as part of NETCONF protocol exchange and determine the address for a CTL provider through the NETCONF protocol. For example, configuration data may be carried as part of a <config> element that is formatted based on the specific data model used within the device. Alternatively, the CTL and related information may be communicated to the device as a "capability". The server may advertise the availability of a CTL download service for a variety of service providers, treating the content of the element as opaque data.

[0039] The network element 110 may include the CTL as a TLS extension to the TLS exchange. The client device 104 may use the "trusted_CA_indication" extension to indicate to the server which CAs are trusted, so the network element 110 may use one of those CAs. Thus, the network element 110 may send the CTL update 400 to the client device 104 as a sub-network access message, such as a dynamic host configuration protocol option, a NETCONF configuration protocol using a remote procedure call, or a transport layer security exchange.

[0040] Embodiments within the scope of the present invention may also include computer-readable media for carrying or having computer-executable instructions or data structures stored thereon. Such computer-readable media can be any available media that can be accessed by a general purpose or special purpose computer. By way of example, and not limitation, such computer-readable media can comprise RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to carry or store desired program code means in the form of computer-executable instructions or data structures. When information is transferred or provided over a network or another communications connection (either hardwired, wireless, or combination thereof) to a computer, the

computer properly views the connection as a computer-readable medium. Thus, any such connection is properly termed a computer-readable medium. Combinations of the above should also be included within the scope of the computer-readable media.

[0041] Embodiments may also be practiced in distributed computing environments where tasks are performed by local and remote processing devices that are linked (either by hardwired links, wireless links, or by a combination thereof) through a communications network.

[0042] Computer-executable instructions include, for example, instructions and data which cause a general purpose computer, special purpose computer, or special purpose processing device to perform a certain function or group of functions. Computer-executable instructions also include program modules that are executed by computers in stand-alone or network environments. Generally, program modules include routines, programs, objects, components, and data structures, etc. that perform particular tasks or implement particular abstract data types. Computer-executable instructions, associated data structures, and program modules represent examples of the program code means for executing steps of the methods disclosed herein. The particular sequence of such executable instructions or associated data structures represents examples of corresponding acts for implementing the functions described in such steps.

[0043] Although the above description may contain specific details, they should not be construed as limiting the claims in any way. Other configurations of the described embodiments of the invention are part of the scope of this invention. For example, the principles of the invention may be applied to each individual user where each user may individually deploy such a system. This enables each user to utilize the benefits of the invention even if any one of the large number of possible applications do not need the functionality described herein. In other words, there may be multiple instances of the

electronic devices each processing the content in various possible ways. It does not necessarily need to be one system used by all end users. Accordingly, the appended claims and their legal equivalents should only define the invention, rather than any specific examples given.

CLAIMS

We claim:

1. A method for updating a device certificate trust list in a client device, comprising:

determining that a certificate of a chain of trust of a sub-network is absent from the device certificate trust list; and

receiving via the sub-network a certificate trust list update from a certificate trust list provider.

2. The method of claim 1, wherein the certificate trust list update was stored at a network element for the sub-network.

3. The method of claim 1, further comprising:

receiving the certificate trust list update in a sub-network access message from a network element.

4. The method of claim 3, wherein the sub-network access message is at least one of a dynamic host configuration protocol option, a NETCONF configuration protocol using a remote procedure call, and a transport layer security exchange.

5. The method of claim 1, further comprising:

receiving an initial sub-network message with at least one of a certificate check indicator and a certificate trust list provider location.

6. The method of claim 5, wherein the initial sub-network message is at least one of a dynamic host configuration protocol option and a NETCONF configuration protocol using a remote procedure call.

7. The method of claim 1, further comprising:

sending a certificate trust list update request to a network element of the sub-network.

8. The method of claim 1, further comprising:

accessing the sub-network in protected mode;

disconnecting from the sub-network upon receipt of the certificate trust list update from the certificate trust list provider;

amending the device certificate trust list with the certificate trust list update; and

connecting to the sub-network in an open access mode.

9. The method of claim 1, further comprising:

accessing the sub-network in protected mode;

amending the device certificate trust list with the certificate trust list update; and

switching from the protected mode to an open access mode.

10. A client device for accessing a sub-network, comprising:

a data storage that stores the device certificate trust list;

a processor that determines that a certificate of a chain of trust of a sub-network is absent from the device certificate trust list; and

a transceiver that receives via the sub-network a certificate trust list update from a certificate trust list provider.

11. The client device of claim 10, wherein the transceiver receives the certificate trust list update in a sub-network access message from a network element.

12. The client device of claim 10, wherein the sub-network access message is at least one of a dynamic host configuration protocol option, a NETCONF configuration protocol using a remote procedure call, and a transport layer security exchange.

13. The client device of claim 10, wherein the transceiver sends a network access identifier with an update request flag to a network element of the sub-network.

14. The client device of claim 10, wherein the processor disregards any transmission not from the certificate trust list provider as part of a protected mode.

15. The client device of claim 14, wherein:

the processor amends the device certificate trust list with the certificate trust list update; and

the transceiver disconnects from the sub-network upon receipt of the certificate trust list update from the certificate trust list provider and connects to the sub-network in an open access mode.

16. The client device of claim 14, wherein the processor amends the device certificate trust list with the certificate trust list update and switches to an open access mode.

17. A network element for connecting a client device to a sub-network, comprising:

a processor that processes a certificate trust list update request from a client device; and

a transceiver that transmits to the client device a certificate trust list update from a certificate trust list provider.

18. The network element of claim 17, further comprising:

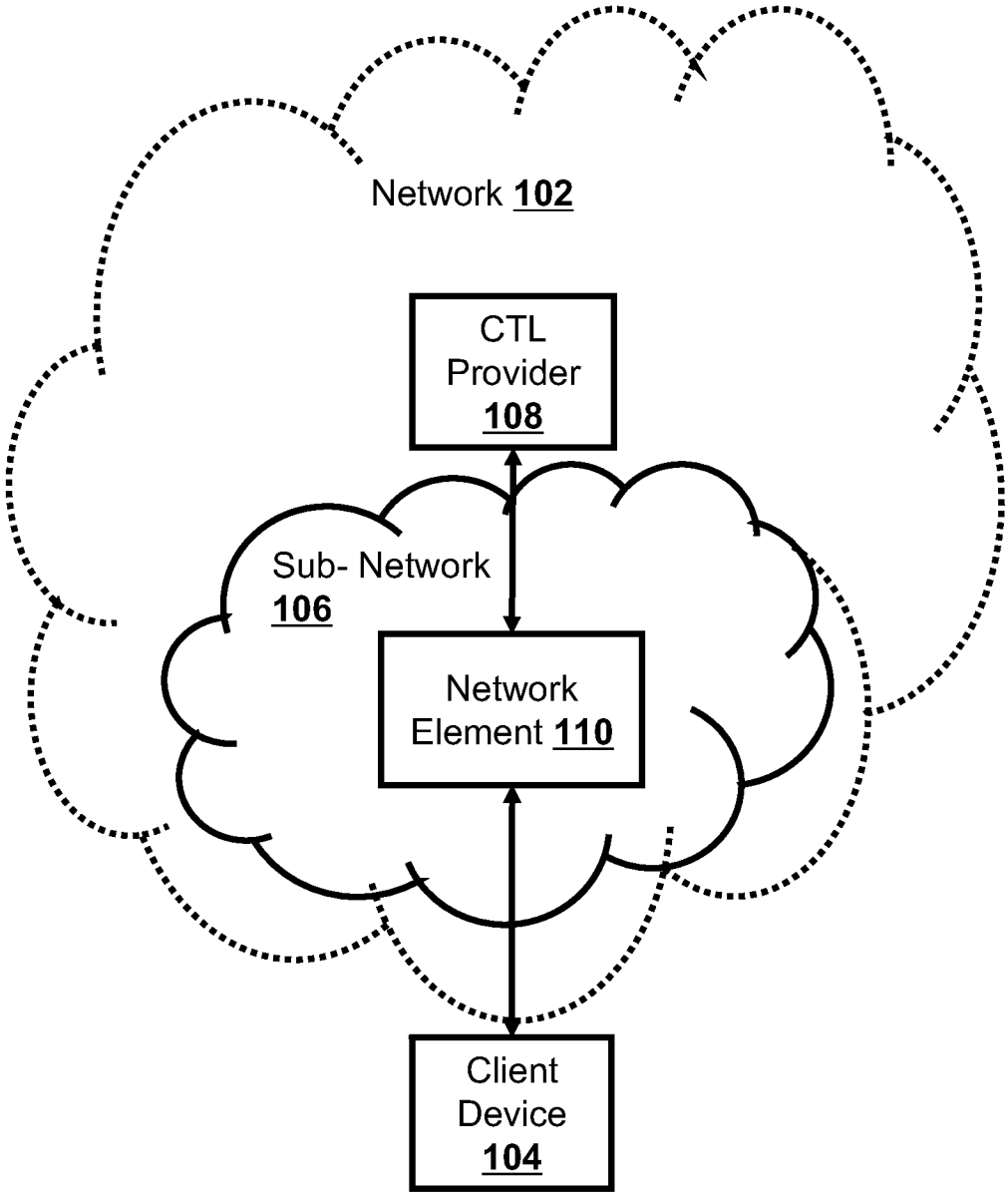
a data storage that stores a certificate trust list update.

19. The network element of claim 17, further comprising:

a sub-network interface that allows the client device to access the certificate trust list provider in a protected mode.

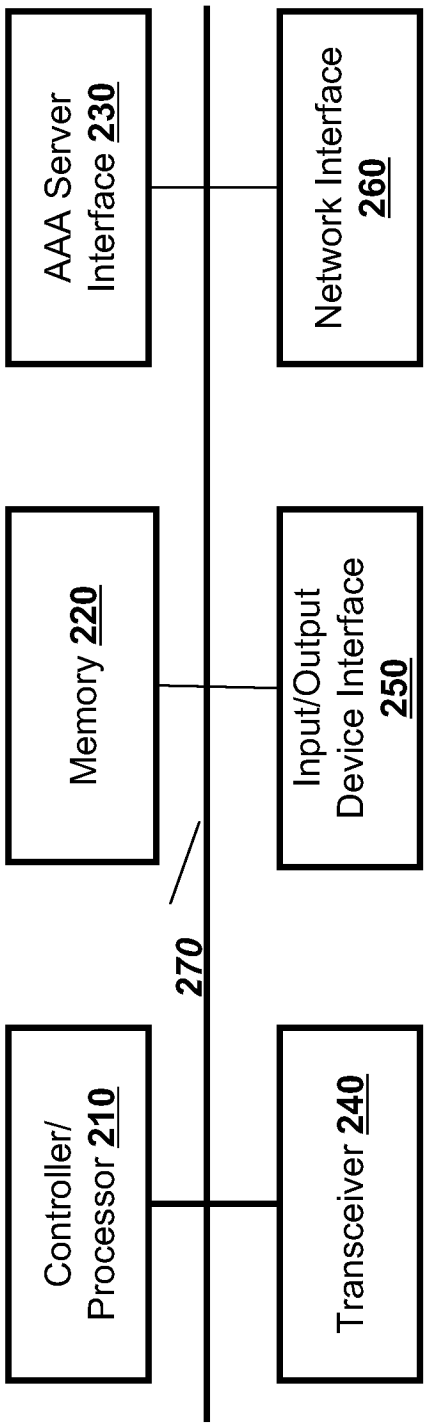
20. The network element of claim 17, wherein the transceiver transmits the certificate trust list update from a network element in at least one of a media access control

message, a dynamic host configuration protocol option, a NETCONF configuration protocol using a remote procedure call, and a transport layer security exchange.


Network 102
CTL Provider 108
Sub- Network 106
Network Element 110
Client Device 104

100

Figure 1


AAA Server Interface 230
Network Interface 260
Memory 220
Input/Output Device Interface 250
270
Controller/ Processor 210
Transceiver 240

110

Figure 2

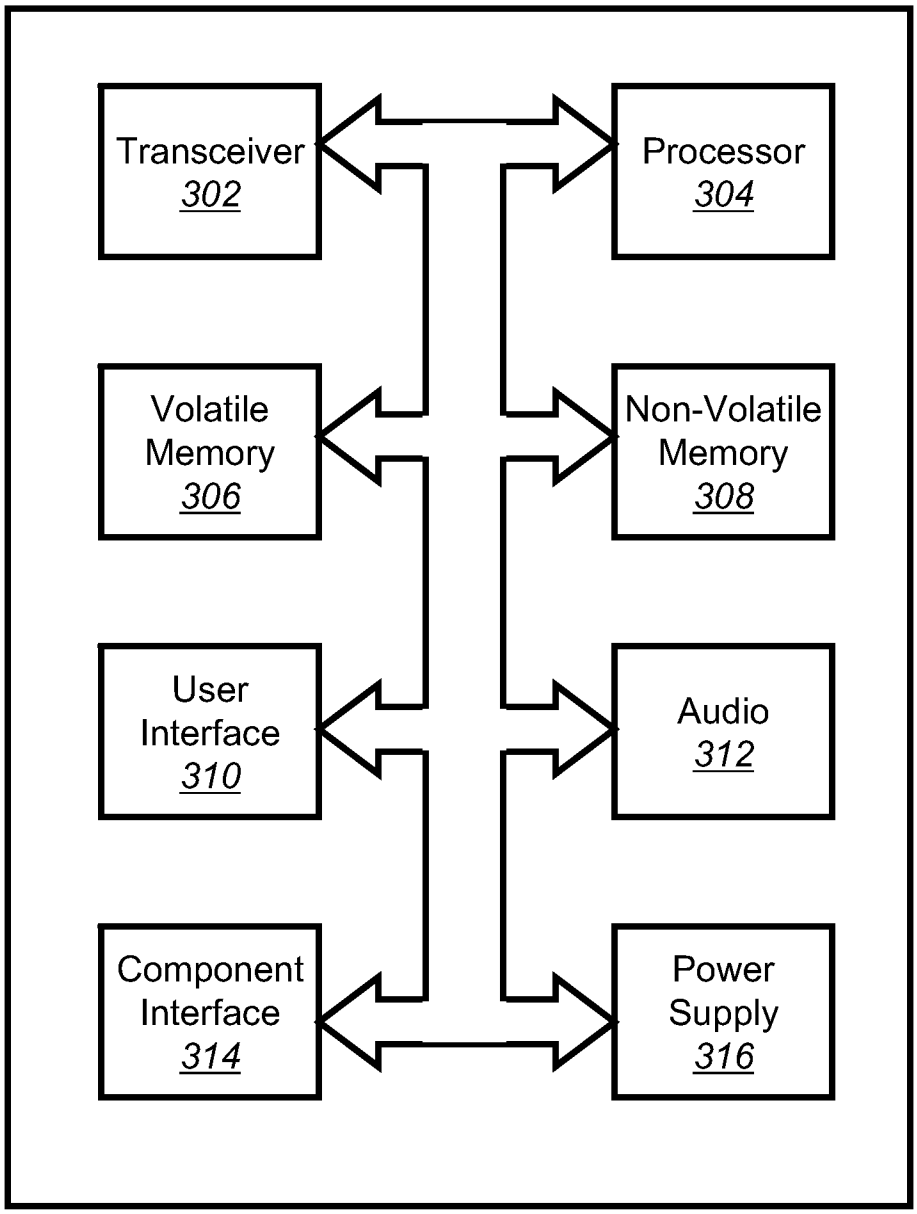
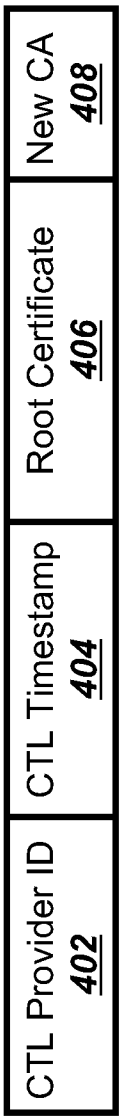
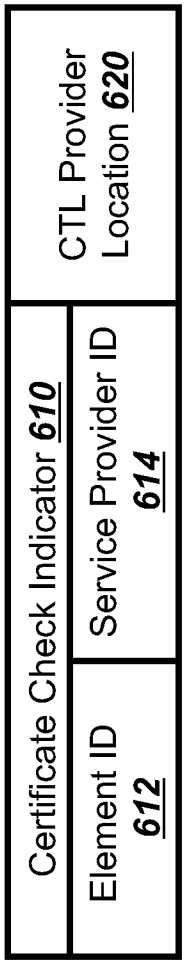

Transceiver
302
Processor
304
Volatile
Memory
306
Non-Volatile
Memory
308
User
Interface
310
Audio
312
Component
Interface
314
Power
Supply
316
104

Figure 3



400
Figure 4



600
Figure 6

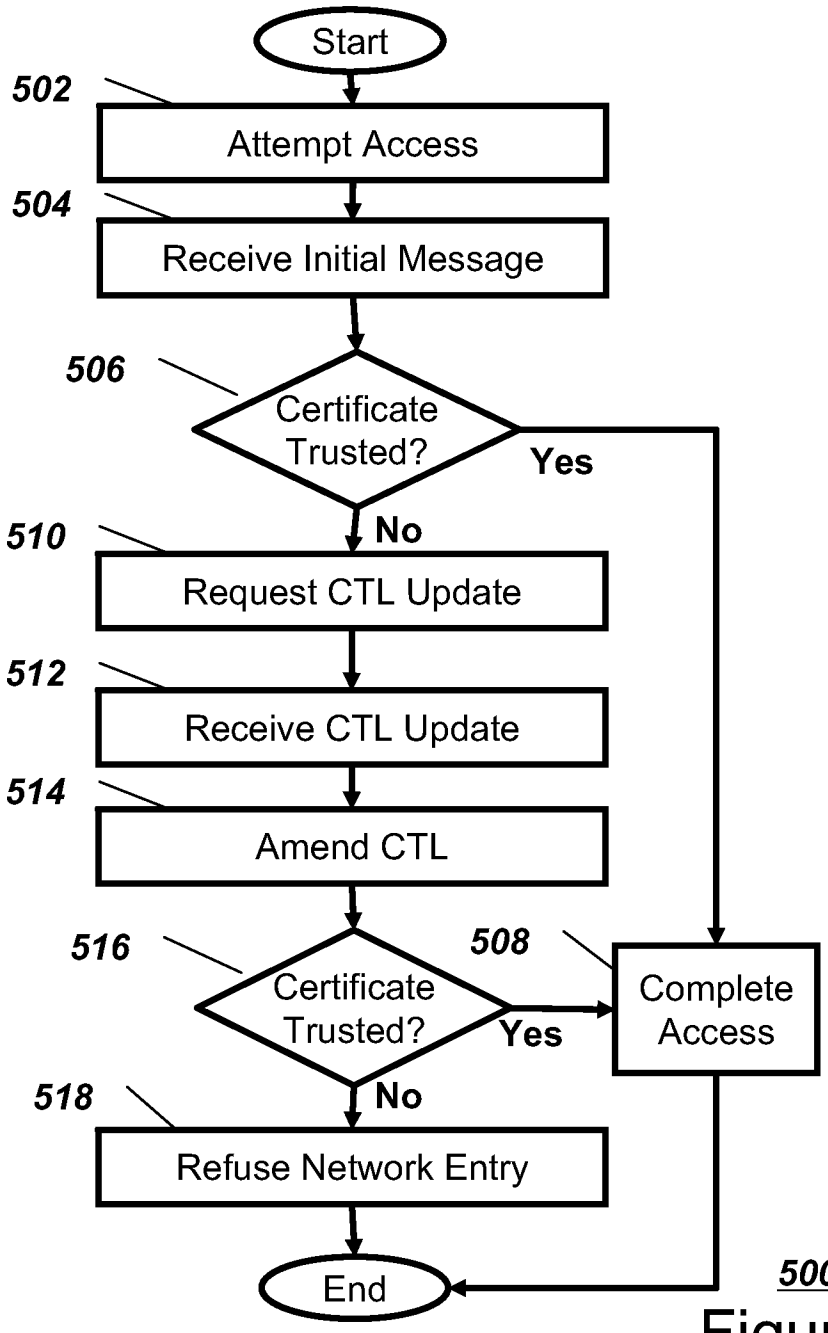

Start
502
Attempt Access
504
Receive Initial Message
506
Certificate Trusted?
Yes
No
510
Request CTL Update
512
Receive CTL Update
514
Amend CTL
516
Certificate Trusted?
508
Complete Access
Yes
No
518
Refuse Network Entry
End
500

Figure 5

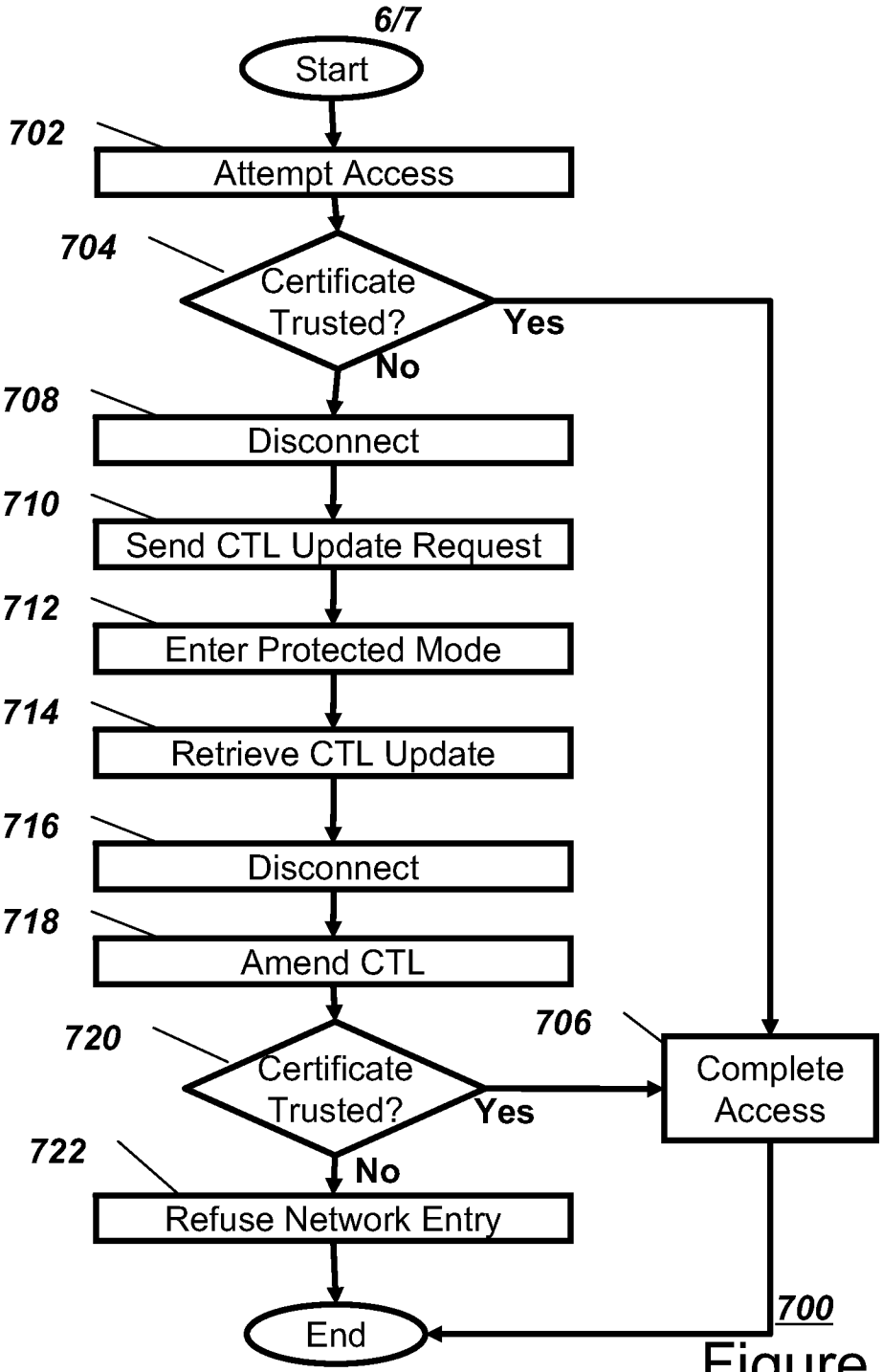

Start
702
Attempt Access
704
Certificate Trusted?
Yes
No
708
Disconnect
710
Send CTL Update Request
712
Enter Protected Mode
714
Retrieve CTL Update
716
Disconnect
718
Amend CTL
720
Certificate Trusted?
Yes
No
706
Complete Access
722
Refuse Network Entry
End
700

Figure 7

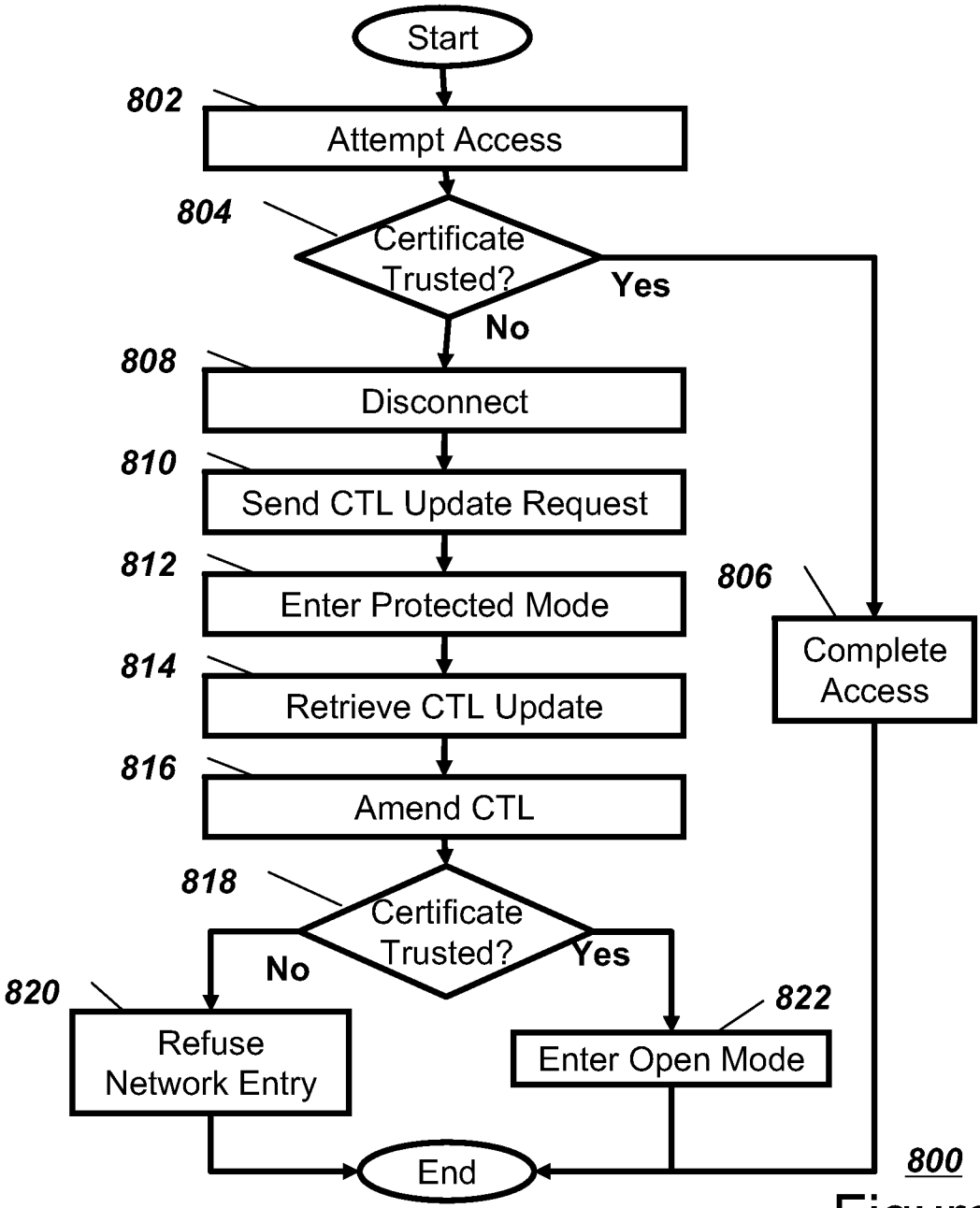

Start
802
Attempt Access
804
Certificate Trusted?
Yes
No
808
Disconnect
810
Send CTL Update Request
812
Enter Protected Mode
814
Retrieve CTL Update
816
Amend CTL
818
Certificate Trusted?
No
Yes
820
Refuse Network Entry
822
Enter Open Mode
806
Complete Access
End
800

Figure 8

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2009/054389

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00 H04L29/06

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)
G06F 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 practical, search terms used)
EPO-Internal, WPI Data, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 816 900 B1 (VOGEL KEITH R [US] ET AL) 9 November 2004 (2004-11-09) abstract; figures 1,3,6 column 3, line 49 - column 4, line 61 column 7, line 10 - column 8, line 25 column 10, lines 11-26 column 10, line 51 - column 11, line 15 -----	1-20
X	US 7 240 194 B2 (HALLIN PHILIP J [US] ET AL) 3 July 2007 (2007-07-03) abstract; figures 1,2 column 3, line 43 - column 4, line 51 column 4, line 63 - column 5, line 44 ----- -/--	1-20

[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 document 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
22 October 2009	29/10/2009

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	Schossmaier, Klaus

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2009/054389

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 6 513 116 B1 (VALENTE LUIS [US]) 28 January 2003 (2003-01-28) abstract; figures 1,4 column 2, line 62 - column 3, line 23 column 4, lines 5-37 column 5, line 52 - column 6, line 39	1-20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2009/054389

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6816900 B1	09-11-2004	US 2005080899 A1	14-04-2005
US 7240194 B2	03-07-2007	US 2003182549 A1	25-09-2003
US 6513116 B1	28-01-2003	NONE	