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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 November 2009 (05.11.2009)

PCT

(10) International Publication Number
WO 2009/134571 A1

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

(21) International Application Number:
PCT/US2009/039054

(22) International Filing Date:
1 April 2009 (01.04.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12/112,319 30 April 2008 (30.04.2008) US

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

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **GUO, Liang** [CN/US]; 20 Brook Street - Apt. 4, Brighton, MA 02135 (US). **BAO, Qi** [CN/US]; 3208 Windsor Ridge Drive, Westborough, MA 01581 (US). **EASTLAKE, Donald, E.** [US/US]; 155 Beaver Street, Milford, MA 01757 (US). **LEE, Whay, Chiou** [US/US]; 16 Michael Way, Cambridge, MA 02141 (US). **METKE, Anthony, R.** [US/US]; 1108 Tuthill Drive, Naperville, IL 60563 (US).

(74) Agents: **KARPINIA, Randi, L.** 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, 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, 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, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND DEVICE FOR DYNAMIC DEPLOYMENT OF TRUST BRIDGES IN AN AD HOC WIRELESS NETWORK

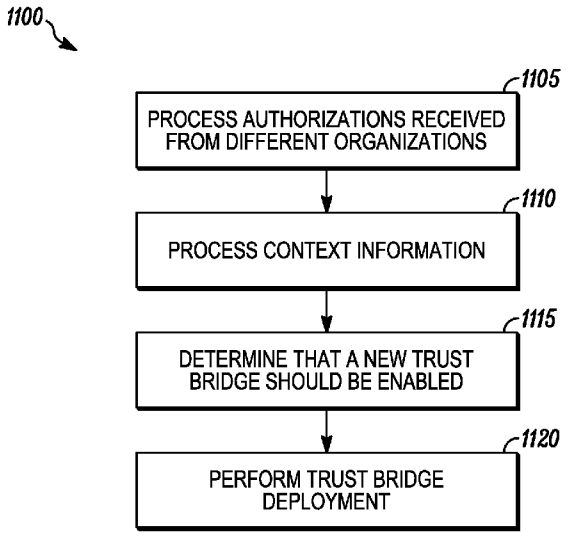


FIG. 11

(57) Abstract: A method for deploying a trust bridge in an ad hoc wireless network can provide interoperability for multi-organizational authentication. The method includes processing at a delegate certification authority (DCA) node device authorizations received from of a plurality of certification authorities (CAs) of different organizations, where the authorizations authorize the DCA node device to serve as a DCA representing the CAs (step 1105). The DCA node device then processes context information received from the ad hoc wireless network (step 1110). Next, the DCA node device determines, based on the context information, that a second node device should be enabled as a new trust bridge (step 1115). The DCA node device then performs a trust bridge deployment to enable the second node device to serve as the new trust bridge (step 1120).

WO 2009/134571 A1

Published:

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

METHOD AND DEVICE FOR DYNAMIC DEPLOYMENT OF TRUST BRIDGES IN AN AD HOC WIRELESS NETWORK

FIELD OF THE DISCLOSURE

[0001] The present invention relates generally to wireless communication networks, and in particular to dynamic deployment of trust bridges in an ad hoc wireless communication network to provide interoperability for multi-organizational authentication.

BACKGROUND

[0002] An ad hoc wireless network is a self-configuring and self-healing localized wireless network that is used to enable communication among a plurality of mobile devices. Connectivity to remote databases or networks is made possible through at least one access point that is connected to such resources over a backhaul network. Mobile devices such as cellular phones, personal digital assistants (PDAs) and notebook computers that operate in ad hoc wireless networks often require authentication when communicating with one another, and when accessing remote databases or networks. A trusted communication path can be established between communicating mobile devices, wherein one device may gain trust in another through a sequence of predominantly logical trust steps.

[0003] A public key infrastructure (PKI), built upon asymmetric cryptographic systems, can be used to enable mobile devices to authenticate one another. In an asymmetric cryptographic system, encryption and decryption of data are performed using different keys, one of which is kept secret and the other is safely divulged as needed. In a PKI, there is at least one trusted entity, known as a certification authority (CA), which issues data structures (referred to as certificates) that bind specific identities to specific public keys and usage information via digital signatures. The

CAs are trusted a priori based on their public keys that are known to be bound to their respective identities in advance. Entities other than CAs may establish trust among themselves by showing one another their respective certificates issued by trusted CAs. There may be a plurality of CAs in a given PKI domain, wherein the CAs may have a hierarchical or a meshed relationship among them. Trust relationships among CAs can be used to build a certification path, which is a chain of certificates where each certificate in the chain is validated by its preceding certificate's public key. A certificate path must terminate with a certificate that has a trusted public key, so that a verifier of the certificate path can verify, using the trusted public key (referred to as a trust anchor of the verifier), a certificate at the other end of the certificate path.

[0004] As described above, when a certificate is produced by an entity (referred to as a target) to demonstrate proof of possession of a valid public key, a verifier of the certification needs to construct a certificate path linking the verifier's trust anchor to the certificate. In a multi-organizational environment, where each organization has its own PKI domain, applications supporting inter-organizational security require additional mechanisms to establish cross-organizational trust relationships, since certificate paths normally remain within respective PKI domains.

[0005] One method for addressing interoperability issues to support inter-organizational security involves use of cross-certificates, wherein CAs of different organizations cross sign one another's certificates to enable members in one organization to trust all user certificates issued by each cross-certified CA. To avoid scalability issues due to meshed CA cross-certification, a bridge CA may be used to cross sign certificates with each participating CA, such that members of each organization can trust all certificates issued by cross-certified CAs. However, both the above methods are undesirable for establishing inter-organizational trust among disparate organizations that have specific and limited relationships. Such disparate organizations have to rely on predetermined policy constraints on certificate validation, where policy rules may include, for example, constraints on at least one of

path length, domain name, and assurance level. Certificate validation therefore can be complicated by policy rules that may be required for large PKI domains.

[0006] Referring to FIG. 1, a network diagram illustrates a problem with cross-certification techniques, as known according to the prior art. Consider, for example, that a first organization has a Root1 certification authority (CA) 105 and several subordinate department CAs, including an engineering department Eng_1 CA 110, a marketing department Mkt_1 CA 115, and a finance department Fin_1 CA 120. Consider also that a second organization has a similar CA hierarchy, including, for example, a Root2 certification authority (CA) 125, a finance department Fin_2 CA 130, and an engineering department Eng_2 CA 135.

[0007] In order to limit a level of cross-organizational trust between the first and second organizations, consider that Fin_1 CA 120 issues a cross-certificate 140 to Fin_2 CA 130 wherein the cross-certificate is a certificate of Fin_2 CA 130 cross-signed by Fin_1 CA 120. A user 145 in the finance department of the second organization may thus use the cross-certificate 140 to gain the trust of a user 150 in the finance department of the first organization. However, the cross-certificate 140 may not effectively prevent the user 145 in the finance department of the second organization from also gaining the trust of the engineering and marketing departments of the second organization. That is because a user 155 in the marketing department and a user 160 in the engineering department of the second organization are not limited to using only the Eng_1 CA 110 and the Mkt_1 CA 115 as trust anchors. In addition, the users 155, 160 also can use the Root1 CA 105 as a trust anchor. The cross-certificate 140 thus creates a valid certificate path from the Root1 CA 105, to the Fin_1 CA 120, to the Fin_2 CA 130.

[0008] To overcome the above described problem of abuse of cross-organizational trust, one method includes policy constraints on certificate validation. For example, in addition to issuing cross-certificates at subordinate CAs, a policy statement is provided between each hierarchically superior CA and subordinate CA to control a range of security domains defined by each cross-certificate. Such a policy

statement may indicate, for example, that an associated cross-certificate cannot be used to validate a level of trust beyond a security domain subordinate to Fin_1 CA 120. For example, referring again to FIG. 1, to prevent the cross-certificate 140 from being used to establish trust between the user 155 in the marketing department of the first organization and the user 145 in the finance department of the second organization, a policy statement would be required between the Root1 CA 105 and the Fin_2 CA 130.

[0009] According to another method, a trust bridge (TB) is used to establish an inter-organizational trust link where a sequence of logical trust steps crosses an organizational boundary. A TB is a device that has been configured with a predetermined set of trust anchors associated with a plurality of organizations with autonomous security domains, and a certificate signed by each of the trust anchors. A device affiliated with an organization may issue a request to a TB in order to bridge authentication between that organization and another organization. A TB must have acquired a certificate from a CA of each participating organization, so that the TB can be trusted by, and can authenticate, relying parties (i.e., certificate verifiers) from different participating organizations. A TB then can assist two relying parties to establish a session key to be used to encrypt data subsequently exchanged between the relying parties. A TB can also assist one relying party to verify authenticity of a message sent by another relying party. A TB also can be responsible for maintaining a status of a certification revocation list, which is a record of certificates that have been revoked.

[0010] There exist several methods to enable relying parties to discover candidate TBs that can bridge their corresponding organizations. These methods enable advertising and discovery of devices that can provide such bridged trust services over an ad hoc wireless network. Compared to the methods of cross-certification and bridged CA as described above, trust bridge based methods can offer increased flexibility in range control, without a burden of complicating backhaul CA relationship topology. However, a trust bridge can be another target for security

attack in a trust chain. Moreover, the task of bridging trust can be computationally intensive as trust bridges may need to handle certificate management for all organizations participating in a network.

[0011] Accordingly, there is a need for an improved method and device for deploying trust bridges in an ad hoc wireless network to provide interoperability for multi-organizational authentication.

BRIEF DESCRIPTION OF THE FIGURES

[0012] The accompanying figures, where like reference numerals refer to identical or functionally similar elements throughout the separate views, together with the detailed description below, are incorporated in and form part of the specification, and serve to further illustrate embodiments of concepts that include the claimed invention, and explain various principles and advantages of those embodiments.

[0013] FIG. 1 is a network diagram illustrating a problem with cross-certification techniques, as known according to the prior art.

[0014] FIG. 2 is a diagram illustrating contents of a delegate certification authority (DCA)-authorizing certificate, according to some embodiments of the present invention.

[0015] FIG. 3 is a diagram illustrating contents of a bridging certificate, according to some embodiments of the present invention.

[0016] FIG. 4 is a network diagram illustrating a method for deploying trust bridges in an ad hoc wireless network, such as an incident area network, to provide interoperability for multi-organizational authentication, according to some embodiments of the present invention.

[0017] FIG. 5 is a general flow diagram illustrating a process for deploying a trust bridge in an ad hoc wireless network, according to some embodiments of the present invention.

[0018] FIG. 6 is a block diagram illustrating components of a delegate certification authority (DCA) node device, according to some embodiments of the present invention.

[0019] FIG. 7 is a network diagram illustrating bridging requests transmitted in an incident area network by devices from a first organization and devices from a second organization, and a subsequent deployment of trust bridges, according to some embodiments of the present invention.

[0020] FIG. 8 is a network diagram illustrating further developments in the network shown in FIG. 7.

[0021] FIG. 9 is a network diagram illustrating further developments in the network shown in FIG. 8.

[0022] FIG. 10 is a network diagram illustrating further developments in the network shown in FIG. 9.

[0023] FIG. 11 is a general flow diagram illustrating a method 1100 for deploying a trust bridge in an ad hoc wireless network to provide interoperability for multi-organizational authentication, according to some embodiments of the present invention.

[0024] Skilled artisans will appreciate that elements in the figures are illustrated for simplicity and clarity and have not necessarily been drawn to scale. For example, the dimensions of some of the elements in the figures may be exaggerated relative to other elements to help to improve understanding of embodiments of the present invention.

[0025] The apparatus and method components have been represented where appropriate by conventional symbols in the drawings, showing only those specific details that are pertinent to understanding the embodiments of the present invention so as not to obscure the disclosure with details that will be readily apparent to those of ordinary skill in the art having the benefit of the description herein.

DETAILED DESCRIPTION

[0026] According to some embodiments of the present invention, a method for deploying a trust bridge in an ad hoc wireless network provides interoperability for multi-organizational authentication. The method includes processing at a special node device, referred to as a delegate certification authority (DCA) node device, authorizations received from a plurality of certification authorities (CAs) of different organizations, wherein the authorizations authorize the DCA node device to serve as a DCA representing the CAs. Next, the DCA node device processes context information received from the ad hoc wireless network. The DCA node device then determines, based on the context information, that a second node device should be enabled as a new trust bridge. The DCA node device then performs a trust bridge deployment to enable the second node device to serve as the new trust bridge.

[0027] Embodiments of the present invention thus can be used to minimize a number of enabled trust bridges operating in an ad hoc wireless network. Devices deployed, for example, at an incident scene such as a large urban fire or natural disaster site, are able to establish through enabled trust bridges cross-organizational trust with other devices as allowed by a current trust policy, and each enabled trust bridge is not overloaded with trust bridging information overhead. Also, a minimum number of trust anchors can be configured at each enabled trust bridge, and a lifetime of a bridge assisted transitive trust can be limited to avoid abuse of cross-organizational trust. By separating cross-organizational trust management from an execution of bridged trust, a DCA node device is not required to handle high loads of trust bridging, which may be computationally intensive. Further, a DCA node device may be the only device in a network that requires high security protection, because security breaches at other node devices will likely affect a smaller number of node devices.

[0028] According to some embodiments of the present invention, a delegate certification authority (DCA) node device is dispatched to a multi-organizational networking environment, such as an incident scene area, to collect appropriate

intelligence on the multi-organizational networking environment. The DCA node device then uses such intelligence to strategically enable a number of existing network node devices to serve as trust bridges. The DCA node device thus serves as an inter-organizational certification authority (CA) having limited authority, and can also serve as a mobile trust bridge. An existing node device operating in a multi-organizational networking environment may also be individually authorized by each of a plurality of CAs from different organizations to serve as a DCA node device.

[0029] After being enabled by a DCA node device, a trust bridge can monitor a local network topology and an organizational membership of each reachable node device within range of the trust bridge. Trust bridges can also exchange collected information with other trust bridges (including the DCA node device), and such exchanged information can be used to collaboratively and dynamically optimize deployment of trust bridges in a network. Further, if multi-organizational networking environment is large, a plurality of DCA node devices can be dispatched, and they can coordinate among themselves to enable selected network devices to operate as trust bridges.

[0030] A DCA node device can include a set of trust anchors, where each trust anchor in the set corresponds to a participating organization in a predetermined set of organizations, and a corresponding set of bridging certificates signed respectively by each trust anchor. With the trust anchors and bridging certificates, the DCA node device can authenticate and be trusted by devices from the different organizations in the predetermined set of organizations. Further, the DCA node device itself can also function as a master trust bridge, which can serve as a trust bridge between any pair of organizations selected from the predetermined set of organizations.

[0031] A DCA node device can include a proxy certificate that is granted by a CA of each organization in the predetermined set of organizations. The DCA node device is thus delegated an authority to provide a limited proxy CA service on behalf of a CA. Such a proxy certificate, referred to herein as a DCA-authorizing certificate, is granted by a CA of an organization to a candidate DCA node device and serves to

bind a unique public key of the candidate DCA node device, within a multi-organizational networking environment of the candidate DCA node device, to its identity. A predetermined set of delegation policies approved by the CAs are also included in the DCA-authorizing certificate.

[0032] According to some embodiments of the present invention, a DCA node device can be preconfigured for dispatch during a pre-planning phase, or can assume a delegation after arriving at a particular incident scene. For each participating organization, a DCA node device first authenticates itself to that organization by, for example, connecting to a backhaul CA of that organization through backhaul connectivity (e.g., through a registration authority at a network service station), and requests a certificate for proxy service and an associated proxy public/private key pair. The backhaul CA (i.e., the issuer of the proxy certificate) is required to create a proxy public/private key pair for the DCA node device, so that the backhaul CA has better control over usage of the DCA-authorizing certificate. Strength of the keys used can be context dependent, and the DCA-authorizing certificate may contain attributes that define policy related constraints such as, for example, a user rank and security level.

[0033] Referring to FIG. 2, a diagram illustrates contents of a DCA-authorizing certificate 200, according to some embodiments of the present invention. For example, the DCA-authorizing certificate 200 includes a DCA name field 205, a DCA public key field 210, a privileges field 215, a conditions field 220, a validity period field 225, a CA name field 230, and a CA signature field 235.

[0034] Referring to FIG. 3, a diagram illustrates contents of a bridging certificate 300, according to some embodiments of the present invention. For example, the bridging certificate 300 includes a bridge name field 305, a bridge public key filed 310, a validity period field 315, a foreign CA public key field 320, a constraints field 325, a DCA name field 330, and a DCA signature field 335.

[0035] A validity period of trust from an organization CA to a DCA node device, such as included in the validity period field 225 of the DCA-authorizing certificate 200, can be defined by a timestamp. The validity period of any trust bridge enabled

by a DCA node device, such as included in the validity period field 315 of the bridging certificate 300, also can be defined by a timestamp. The validity period defined by a bridging certificate then must be within the validity period of a corresponding DCA-authorizing certificate.

[0036] Referring to FIG. 4, a network diagram illustrates a method for deploying trust bridges in an ad hoc wireless network 400 to provide interoperability for multi-organizational authentication, according to some embodiments of the present invention. As illustrated, a first organization certification authority (CA) 405 from a first organization, a second organization CA 410 from a second organization, and a third organization CA 415 from a third organization, are each in communication with a corresponding Registration Authority (RA) at a network service station 420, wherein an RA is an authority in a network that verifies user requests for a digital certificate and tells the certificate authority (CA) to issue it. A delegate certification authority (DCA) node device 425 is also in communication with the RAs in the network service station 420. Therefore, through the RAs, each of the CAs 405, 410, 415 transmits authorizations to the DCA node device 425, where the authorizations authorize the DCA node device 425 to serve as a DCA representing the CAs 405, 410, 415.

[0037] The authorizations transmitted to the DCA node device 425 are in the form of a DCA-authorizing certificate 430 from the first organization CA 405, a DCA-authorizing certificate 435 from the second organization CA 410, and a DCA-authorizing certificate 440 from the third organization CA 415. For example, the DCA-authorizing certificates 430, 435, and 440 may be in the form of the DCA-authorizing certificate 200 shown in FIG. 2. The DCA node device 425 therefore becomes a proxy CA of the first, second, and third organizations.

[0038] Next, as represented by line 445, the DCA node device 425 moves to within radio frequency (RF) range of an ad hoc wireless network 450 operating at a multi-organizational networking environment. The DCA node device 425 then processes context information received from the ad hoc wireless network 450. Such

context information can include, for example, network state information including attributes of various node devices 455, from the three organizations represented by the CAs 405, 410, 415, which are operating in the ad hoc wireless network 450. The context information may also include network topology data and one or more bridging requests received from the various node devices 455. Based at least in part on the context information, the DCA node device 425 can determine that a second node device, such as one of the various node devices 455, is authorized to function as a trust bridge and should be enabled as a new trust bridge 460. Finally, the DCA node device 425 performs a trust bridge deployment, including transmission to the new trust bridge 460 of a bridging certificate 465, to enable the second node device to serve as the new trust bridge 460. For example, the bridging certificate 465 can be in the form of the bridging certificate 300 shown in FIG. 3.

[0039] Similarly, based at least in part on the context information and the needs of the ad hoc network, the DCA node device 425 can also enable a third node device, such as one of the various node devices 455, to serve as a new trust bridge 470. The DCA node device 425 will therefore transmit a bridging certificate 475 to the new trust bridge 470. Each new trust bridge 460, 470 can then install trust anchors associated with the CAs 405, 410, 415. For example, consider that the trust bridge 460 concerns a node device that was originally associated with the first organization CA 405. When being deployed as a trust bridge, the trust bridge 460 will therefore install trust anchors associated with the second organization CA 410 and the third organization CA 415. Such trust anchors will include the bridging certificate 465 and the DCA-authorizing certificates 435, 440, respectively. The trust bridge 460 is then enabled to provide service to bridge its original organization associated with the first organization CA 405, and the foreign organizations associated with the second organization CA 410 and the third organization CA 415. The various node devices 455 from the three different organizations represented by the three CAs 405, 410, 415 are therefore able to obtain effective interoperability, enabling them all to communicate with each other, in the ad hoc wireless network 450.

[0040] It is generally not required that the DCA node device 425 create a proxy key pair for each new trust bridge 460, 470 since it is generally adequate for each new trust bridge 460, 470 to use its own private key to provide a bridging service.

[0041] Referring to FIG. 5, a general flow diagram illustrates a process for deploying a trust bridge in an ad hoc wireless network, according to some embodiments of the present invention. At step 505, a delegate certification authority (DCA) node device, such as the DCA node device 425, receives a bridging request from a requesting node device, such as a device associated with the new trust bridge 460.

[0042] At step 510, it is determined at the DCA node device whether the requesting node device has been authenticated by the DCA node device. If not, the process ends. When it is determined that the requesting node device has been authenticated by the DCA node device , then at step 515 it is determined whether the DCA node device has been authenticated by the requesting node device. If not, the process ends. When it has been determined that the DCA node device has been authenticated by the requesting node device, then at step 520 it is determined whether the requesting node device is allowed to serve as a trust bridge. If not, the process ends. When it is determined that the requesting node device is allowed to serve as a trust bridge, at step 525 the DCA node device issues a bridging certificate to the requesting node device. Finally, at step 530, the DCA node device installs a set of appropriate trust anchor(s) in the requesting node device by transmitting a corresponding DCA-authorizing certificate(s) to the requesting node device. As will be understood by those having ordinary skill in the art, after the process ends it may be restarted at any time when a new bridging request is received.

[0043] Referring to FIG. 6, a block diagram illustrates components of a delegate certification authority (DCA) node device, such as the DCA node device 425, according to some embodiments of the present invention. The DCA node device 425 comprises a random access memory (RAM) 605 and a programmable memory 610 that are coupled to a processor 615. The processor 615 also has ports for coupling to

wireless network interfaces 620, 625. The wireless network interfaces 620, 625 can be used to enable the DCA node device 425 to communicate with other node devices in an ad hoc wireless network or mesh network, such as the ad hoc wireless network 450. For example, the DCA node device 425 can communicate with the new trust bridge 460 using the wireless network interface 620 to receive and route data packets.

[0044] The programmable memory 610 can store operating code (OC) for the processor 615 and code for performing functions associated with a DCA node device. For example, the programmable memory 610 can comprise trust bridge deployment computer readable program code components 630 configured to cause execution of a method for deploying a trust bridge in an ad hoc wireless network as described herein.

[0045] Examples of functional blocks of the computer readable program code components 630 include a trust bridge location algorithm 635 that receives input from a local network topology monitor 640, a bridging offered load monitor 645, and a bridging service manager 650. The local topology monitor 640 and the bridging offered load monitor 645 collect information to enable the trust bridge location algorithm 635 to adaptively enable and disable trust bridges in a network, based on changing demand. The bridging offered load monitor 645 and the bridging service manager 650 also provide data to a bridging certification manager 655 that monitors data such as certificate validity periods, assignments of certificates, and certificate renewals. To facilitate certificate management, the bridging certification manager 655 also records active bridging certificate information in a certificate database 660.

[0046] The trust bridge location algorithm 635 can be used to minimize a number of enabled trust bridges operating in a network, while still maintaining adequate interoperability between various organizations operating at an incident scene. For example, an adequate number of trust bridges should be enabled so that it is possible to establish an acceptable trust path between each pair of node devices operating at an incident scene, while no trust bridge should be overloaded with trust bridging information overhead.

[0047] According to some embodiments of the present invention, a pre-determined number of node devices can be selected as candidate trust bridges during a pre-planning phase. For example, initial selection of node devices can be based on pre-deployment physical or security properties of the devices. Thus a device may be qualified to function as a trust bridge if it has adequate power and computing resources, is within a communication range of a large number of other devices, or has a high trust/security level. For example, in a fire-fighting scenario, devices located in fire engines may be more powerful than handheld devices, and thus may be more qualified to be selected as candidate trust bridges.

[0048] A number of devices that are selected as candidate trust bridges can be set to facilitate load balancing, so that no enabled trust bridge needs to handle an excessive offered load of trust establishment requests. For example, a number of candidate trust bridges can be a function of a number of devices in each distinct organization in a set of organizations that may operate in a particular network. For example, where there are two organizations, a number of candidate trust bridges can be set to be proportional to a product of a total number of devices from each respective organization.

[0049] A delegate certification authority (DCA) node device thus can be preconfigured with the identities of candidate trust bridges, and with respective trust bridging policy constraints. For example, such constraints may include a permission to function as a trust bridge for only a particular organization. Alternatively, each candidate trust bridge can be preconfigured with a certificate that indicates that the candidate trust bridge is permitted, based on a predetermined policy, to serve as a trust bridge for a predetermined list of organizations. Then, upon deployment of the candidate trust bridges, a DCA node device dynamically allocates appropriate bridging certificates, and an appropriate validity period for each bridging certificate, according to policies and periodic updates of physical or security properties forwarded to the DCA node device by the candidate trust bridges. This allows the candidate trust bridges to be enabled dynamically.

[0050] According to still other embodiments of the present invention, candidate trust bridges can be dynamically determined by a facility location algorithm based on dynamic topology information. That enables a selected trust bridge to be centrally located relative to a group of node devices to which the trust bridge provides bridging services. Each node device in a network can announce a set of organization identities with which it seeks to establish trust. For each set of devices that have announced a given organization identity, a logical topology is constructed that connects the set of devices with a set of links, each assigned a link weight. For example, a link weight can be derived from a hop count. Next, a "center" set of the devices that are to be deployed as trust anchors is determined. When a number of devices using the trust bridging services becomes large enough that additional trust bridges are required, a dynamic clustering and cluster-head election algorithm can be used to create multiple size-restricted clusters, where each cluster shares a trust bridge located at a central cluster-head device. Such dynamic clustering and cluster-head election algorithms are well known to those having ordinary skill in the art. For example, see G. Venkataraman, S. Emmanuel and S. Thambipillai, "Size-restricted Cluster Formation and Cluster Maintenance Technique for Mobile Ad Hoc Networks", International Journal of Network Management, Vol. 17, pages 171-194, March 2007, which is hereby incorporated by reference in its entirety herein.

[0051] The dynamic clustering and cluster-head election algorithm ensures that each node device in a network has access to one or more trust bridges that can collectively serve all necessary bridging requirements, while minimizing a hop-count to the furthest trust bridges. For example, such an algorithm can be centralized at a DCA node device, if the DCA node device has a global view of a relevant network topology. Otherwise, the algorithm can be distributed throughout the network.

[0052] According to still other embodiments of the present invention, each node device in an ad hoc wireless network can be selected to serve as a trust bridge. A DCA node device then becomes a default bridging device for all inter-organization pairs. The DCA node device thus keeps track of identities of requesting organizations.

If a particular pair appears very often (e.g., above a predetermined threshold), the DCA node device may grant bridging functionality to a node device that is close to a center of all requests of a given type. The node device with such bridging functionality then intercepts all bridging requests and takes over bridging responsibility for that particular pair of organizations. Such functionality is described in more detail below.

[0053] Referring to FIGs. 7, 8, 9 and 10, sequential network diagrams illustrate bridging requests 705 transmitted in an incident area network 700 by devices 710 from a first organization, and by devices 715 from a second organization, and a subsequent deployment of trust bridges, according to some embodiments of the present invention. As shown in FIG. 7, the bridging requests 705 are first transmitted to a DCA node device 720. However, as shown in FIG. 8, when a number of bridging requests reaches a predetermined limit, the DCA node device selects a particular device to function as a new trust bridge 805. The new trust bridge 805 then monitors and intercepts any bridging request sent to the DCA node device 720, and also takes over the bridging functionality of authentication and key generation.

[0054] Next, referring to FIGs. 9 and 10, if it becomes evident that the new trust bridge 805 is becoming overloaded, the DCA node device 720 may select another device to function as another new trust bridge 1005. The new trust bridge 1005 then shares some of the bridging services load with the other new trust bridge 805. As shown, the new trust bridge 1005 may be located in an area close to where a large number of the bridging requests 705 shown in FIG. 9 are originating.

[0055] For security reasons, a number of trust bridges active in a multi-organizational networking environment should generally be minimized. Maintaining idle or unnecessary trust bridges not only consumes network resources, but also can increase risks of bridging service abuse. Attempts to manage such risks may also include a use of short validity periods for bridging services. An active status of unused trust bridges will then eventually expire. Also, trust bridges that anticipate having long term usage requirements may request extensions of their respective

validity periods. Alternatively, a DCA node device may selectively extend the validity period of bridging services for various trust bridges. Such selective extensions may take into consideration an offered load of bridging requests, so that an adequate number of active trust bridges are maintained to share an offered load.

[0056] Referring to FIG. 11, a general flow diagram illustrates a method 1100 for deploying a trust bridge in an ad hoc wireless network to provide interoperability for multi-organizational authentication, according to some embodiments of the present invention. At step 1105, a delegate certification authority (DCA) node device processes authorizations received from of a plurality of certification authorities (CAs) of different organizations, wherein the authorizations authorize the DCA node device to serve as a DCA representing the CAs. For example, as shown in FIG. 4, authorizations are provided to the DCA node device 425 in the form of the DCA-authorizing certificates 430, 435, 440.

[0057] At step 1110, the DCA node device processes context information received from the ad hoc wireless network. For example, as shown in FIG. 4, the DCA node device 425 processes network topology information concerning the ad hoc wireless network 450.

[0058] At step 1115, the DCA node device determines, based on the context information, that a second node device should be enabled as a new trust bridge. For example, the DCA node device 425 determines that one of the various node devices 455 should be enabled as the new trust bridge 460.

[0059] Finally, at step 1120, the DCA node device performs a trust bridge deployment to enable the second node device to serve as the new trust bridge. For example, the DCA node device 425 transmits to the new trust bridge 460 the bridging certificate 465 and at least some of the DCA-authorizing certificates 430, 435, 440.

[0060] Advantages of some embodiments of the present invention therefore include enabling, in an ad hoc wireless network, an efficient and dynamic deployment of trust bridges. An adaptive number of trust bridges therefore can be strategically deployed and configured to establish trust among organizations actually involved in

an incident scene response, where each trust bridge will not be overloaded with bridging information overhead, such as negative constraints on cross-certificates. Overall interoperability of network device therefore can be improved. Moreover, risks concerning abuse of ad hoc transitive trust between network node devices can be reduced by minimizing a number of bridging devices, minimizing a number of bridging certificates, and minimizing the validity period of bridging services.

[0061] In the foregoing specification, specific embodiments have been described. However, one of ordinary skill in the art appreciates that various modifications and changes can be made without departing from the scope of the invention as set forth in the claims below. Accordingly, the specification and figures are to be regarded in an illustrative rather than a restrictive sense, and all such modifications are intended to be included within the scope of present teachings. The benefits, advantages, solutions to problems, and any element(s) that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as critical, required, or essential features or elements of any or all the claims. The invention is defined solely by the appended claims including any amendments made during the pendency of this application and all equivalents of those claims as issued.

[0062] Moreover in this document, relational terms such as first and second, top and bottom, and the like may be used solely to distinguish one entity or action from another entity or action without necessarily requiring or implying any actual such relationship or order between such entities or actions. The terms "comprises," "comprising," “has”, “having,” “includes”, “including,” “contains”, “containing” or any other variation thereof, are intended to cover a non-exclusive inclusion, such that a process, method, article, or apparatus that comprises, has, includes, or contains a list of elements does not include only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus. An element preceded by “comprises a …”, “has a …”, “includes a …”, or “contains a …” does not, without more constraints, preclude the existence of additional identical elements in the process, method, article, or apparatus that comprises, has, includes, or contains

the element. The terms "a" and "an" are defined as one or more unless explicitly stated otherwise herein. The terms "substantially", "essentially", "approximately", "about" or any other version thereof, are defined as being close to as understood by one of ordinary skill in the art, and in one non-limiting embodiment the term is defined to be within 10%, in another embodiment within 5%, in another embodiment within 1% and in another embodiment within 0.5%. The term "coupled" as used herein is defined as connected, although not necessarily directly and not necessarily mechanically. A device or structure that is "configured" in a certain way is configured in at least that way, but may also be configured in ways that are not listed.

[0063] It will be appreciated that some embodiments may be comprised of one or more generic or specialized processors (or "processing devices") such as microprocessors, digital signal processors, customized processors and field programmable gate arrays (FPGAs) and unique stored program instructions (including both software and firmware) that control the one or more processors to implement, in conjunction with certain non-processor circuits, some, most, or all of the functions of the method and system described herein. Alternatively, some or all functions could be implemented by a state machine that has no stored program instructions, or in one or more application specific integrated circuits (ASICs), in which each function or some combinations of certain of the functions are implemented as custom logic. Of course, a combination of the two approaches could be used.

[0064] Moreover, an embodiment can be implemented as a computer-readable storage medium having computer readable code stored thereon for programming a computer (e.g., comprising a processor) to perform a method as described and claimed herein. Examples of such computer-readable storage mediums include, but are not limited to, a hard disk, a CD-ROM, an optical storage device, a magnetic storage device, a ROM (Read Only Memory), a PROM (Programmable Read Only Memory), an EPROM (Erasable Programmable Read Only Memory), an EEPROM (Electrically Erasable Programmable Read Only Memory) and a Flash memory. Further, it is expected that one of ordinary skill, notwithstanding possibly significant

effort and many design choices motivated by, for example, available time, current technology, and economic considerations, when guided by the concepts and principles disclosed herein will be readily capable of generating such software instructions and programs and ICs with minimal experimentation.

[0065] The Abstract of the Disclosure is provided to allow the reader to quickly ascertain the nature of the technical disclosure. It is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims. In addition, in the foregoing Detailed Description, it can be seen that various features are grouped together in various embodiments for the purpose of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed embodiments require more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive subject matter lies in less than all features of a single disclosed embodiment. Thus the following claims are hereby incorporated into the Detailed Description, with each claim standing on its own as a separately claimed subject matter.

We claim:

1. A method for deploying a trust bridge in an ad hoc wireless network to provide interoperability for multi-organizational authentication, the method comprising:

processing at a delegate certification authority (DCA) node device authorizations received from of a plurality of certification authorities (CAs) of different organizations, wherein the authorizations authorize the DCA node device to serve as a DCA representing the CAs;

processing at the DCA node device context information received from the ad hoc wireless network;

determining at the DCA node device, based on the context information, that a second node device should be enabled as a new trust bridge; and

performing at the DCA node device a trust bridge deployment to enable the second node device to serve as the new trust bridge.

2. The method of claim 1, wherein the trust bridge deployment comprises:

authenticating the second node device at the DCA node device;

determining at the DCA node device that the second node device has authenticated the DCA node device;

determining at the DCA node device that the second node device is authorized to function as a trust bridge;

transmitting a bridging certificate from the DCA node device to the second node device; and

transmitting a DCA-authorizing certificate from the DCA node device to the second node device, whereby the second node device is authorized to function as a trust bridge in the ad hoc wireless network.

3. The method of claim 2, wherein the bridging certificate comprises data selected from the following: a bridge name field; a bridge public key field; a validity period field; a foreign certification authority public key field; a constraints field; a DCA name filed; and a signature field.

4. The method of claim 2, wherein the DCA-authorizing certificate comprises data selected from the following: a DCA name field; a DCA public key field; a privileges field; a conditions field; a validity period field; a CA name field; and a CA signature field.

5. The method of claim 2, wherein the DCA node device can access a predetermined set of trust anchors and a corresponding set of signed certificates received from a plurality of organizations participating in the ad hoc wireless network.

6. The method of claim 5, wherein each organization in the plurality of organizations has granted a DCA-authorizing certificate to the DCA node device, whereby the DCA node device is delegated authority to provide a limited proxy certification authority service on behalf of an organization.

7. The method of claim 2, wherein the DCA node device can function as a master trust bridge in the ad hoc wireless network.

8. The method of claim 2, wherein the DCA node device authorizes the second node device to use a private key of the second node device to facilitate a trust bridging service.

9. The method of claim 2, further comprising, before authenticating the second node device at the DCA node device, processing at the DCA node device a bridging request message received from the second node device.

10. The method of claim 1, wherein the context information comprises network state information, and determining at the DCA node device, based on the context information, that a second node device should be enabled as a new trust bridge employs a predetermined policy based on the network state information.

11. The method of claim 10, wherein the network state information comprises attributes of a node device.

12. The method of claim 10, wherein the network state information comprises network topology data.

13. The method of claim 10, wherein the network state information comprises a plurality of bridging requests.

14. A delegate certification authority (DCA) node device for deploying a trust bridge in an ad hoc wireless network to provide interoperability for multi-organizational authentication, the DCA node device comprising:

computer readable program code for processing at the DCA node device authorizations received from of a plurality of certification authorities (CAs) of different organizations, wherein the authorizations authorize the DCA node device to serve as a DCA representing the CAs;

computer readable program code for processing at the DCA node device context information received from the ad hoc wireless network;

computer readable program code for determining at the DCA node device, based on the context information, that a second node device should be enabled as a new trust bridge; and

computer readable program code for performing at the DCA node device a trust bridge deployment to enable the second node device to serve as the new trust bridge.

15. The DCA node device of claim 14, wherein the computer readable program code for performing at the DCA node device a trust bridge deployment comprises:

computer readable program code for authenticating the second node device at the DCA node device;

computer readable program code for determining at the DCA node device that the second node device has authenticated the DCA node device;

computer readable program code for determining at the DCA node device that the second node device is authorized to function as a trust bridge;

computer readable program code for transmitting a bridging certificate from the DCA node device to the second node device; and

computer readable program code for transmitting a DCA-authorizing certificate from the DCA node device to the second node device, whereby the second node device is authorized to function as a trust bridge in the ad hoc wireless network.

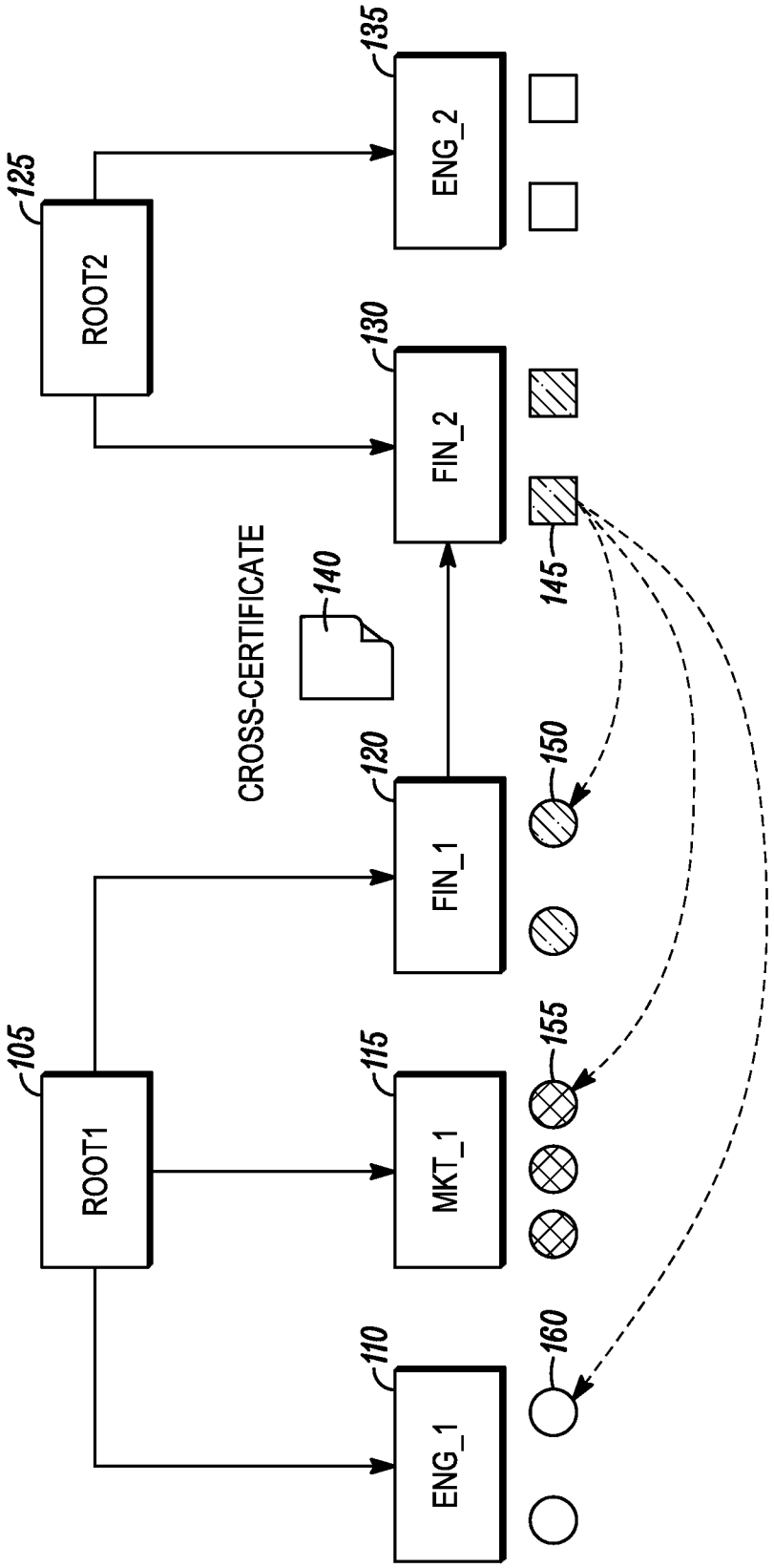
16. The DCA node device of claim 15, wherein the bridging certificate comprises data selected from the following: a bridge name field; a bridge public key field; a validity period field; a foreign certification authority public key field; a constraints field; a DCA name filed; and a signature field.

17. The DCA node device of claim 15, wherein the DCA-authorizing certificate comprises data selected from the following: a DCA name field; a DCA public key field; a privileges field; a conditions field; a validity period field; a CA name field; and a CA signature field.

18. The DCA node device of claim 15, wherein the DCA node device can access a predetermined set of trust anchors and a corresponding set of signed certificates received from a plurality of organizations participating in the ad hoc wireless network.

19. The DCA node device of claim 18, wherein each organization in the plurality of organizations has granted a DCA-authorizing certificate to the DCA node device, whereby the DCA node device is delegated authority to provide a limited proxy certification authority service on behalf of an organization.

20. The DCA node device of claim 14, wherein the context information comprises network state information, and determining at the DCA node device, based on the context information, that a second node device should be enabled as a new trust bridge employs a predetermined policy based on the network state information.



(PRIOR ART)

FIG. 1

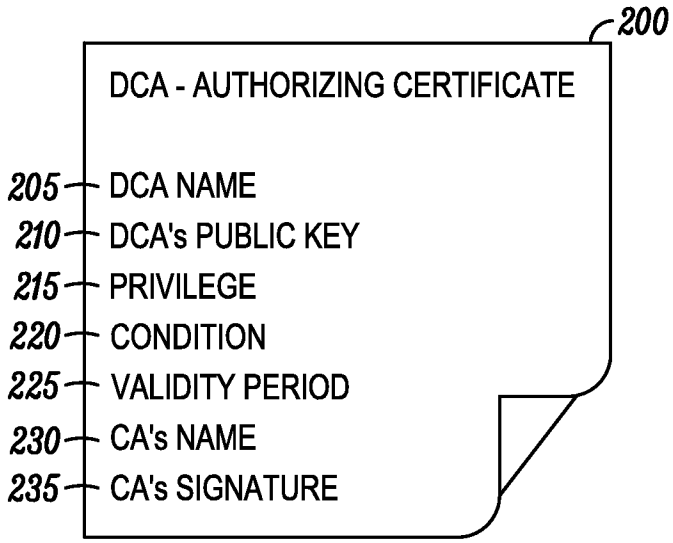

200
DCA - AUTHORIZING CERTIFICATE
205
DCA NAME
210
DCA's PUBLIC KEY
215
PRIVILEGE
220
CONDITION
225
VALIDITY PERIOD
230
CA's NAME
235
CA's SIGNATURE

FIG. 2

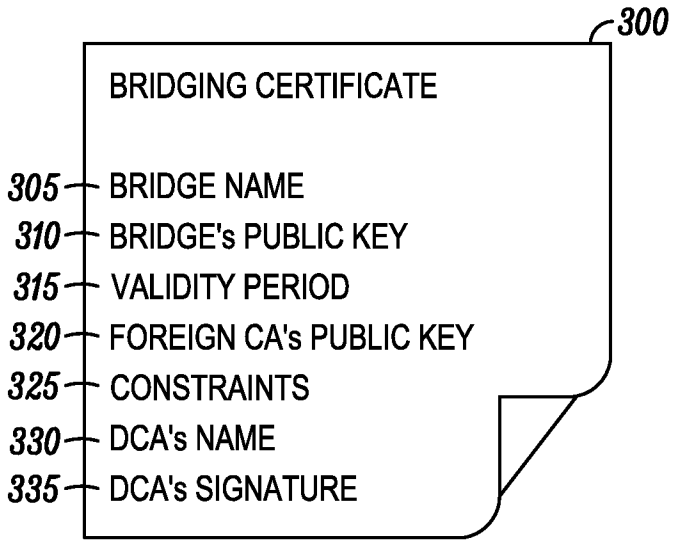

300
BRIDGING CERTIFICATE
305
BRIDGE NAME
310
BRIDGE's PUBLIC KEY
315
VALIDITY PERIOD
320
FOREIGN CA's PUBLIC KEY
325
CONSTRAINTS
330
DCA's NAME
335
DCA's SIGNATURE

FIG. 3

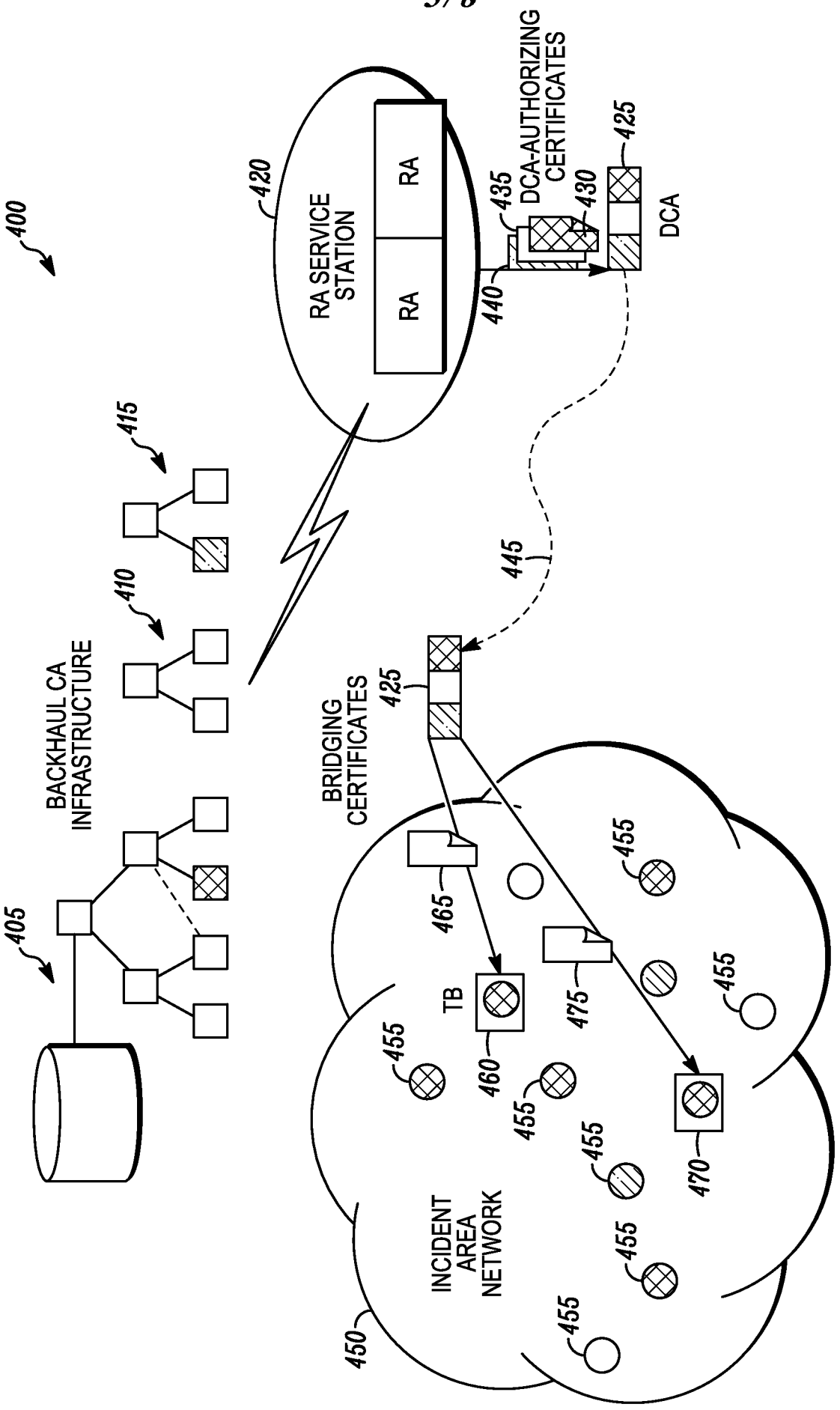

400
405
BACKHAUL CA INFRASTRUCTURE
410
415
420
RA SERVICE STATION
RA
RA
435
DCA-AUTHORIZING CERTIFICATES
430
425
DCA
440
445
BRIDGING CERTIFICATES
425
465
TB
460
475
455
455
455
455
455
455
470
INCIDENT AREA NETWORK
450

FIG. 4

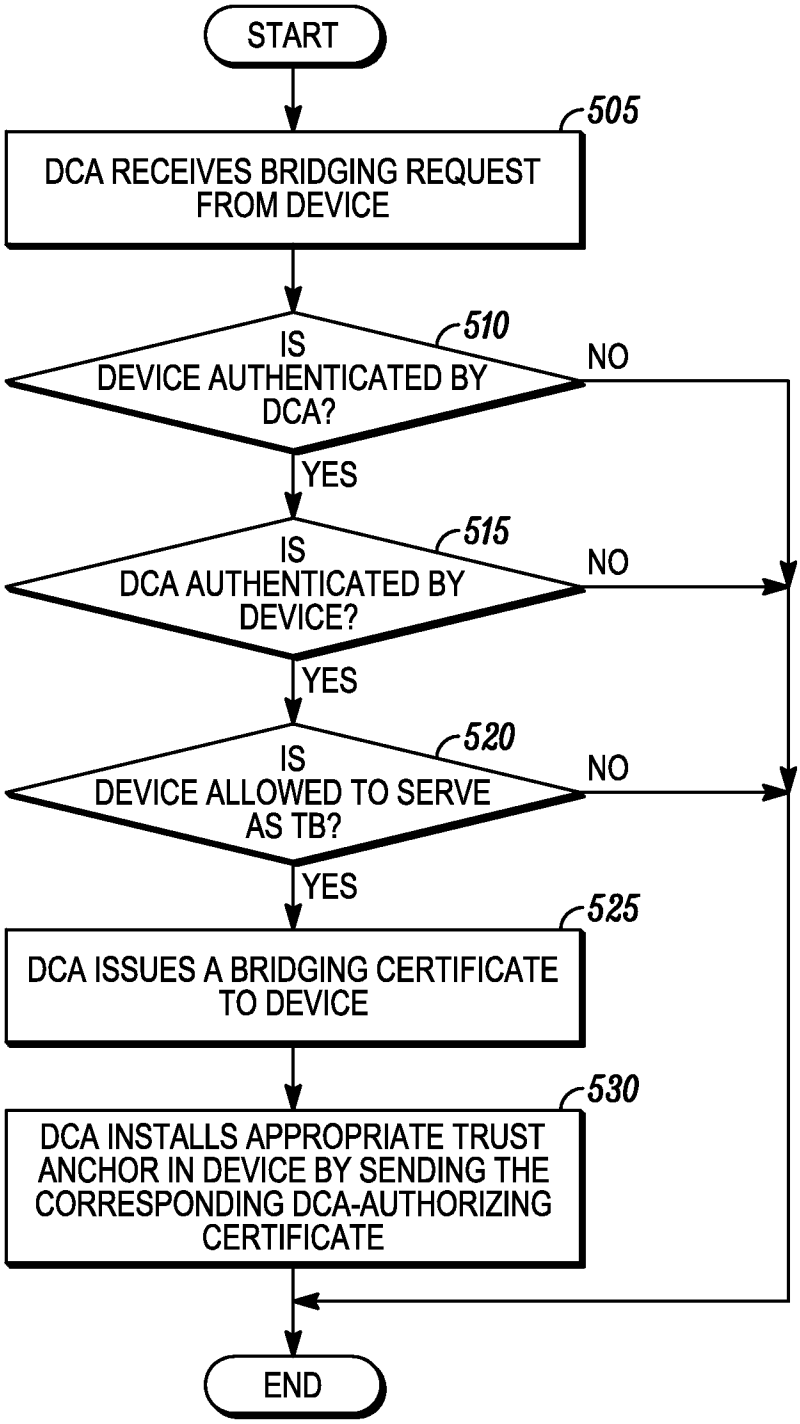

START
505
DCA RECEIVES BRIDGING REQUEST FROM DEVICE
510
IS DEVICE AUTHENTICATED BY DCA?
NO
YES
515
IS DCA AUTHENTICATED BY DEVICE?
NO
YES
520
IS DEVICE ALLOWED TO SERVE AS TB?
NO
YES
525
DCA ISSUES A BRIDGING CERTIFICATE TO DEVICE
530
DCA INSTALLS APPROPRIATE TRUST ANCHOR IN DEVICE BY SENDING THE CORRESPONDING DCA-AUTHORIZING CERTIFICATE
END

FIG. 5

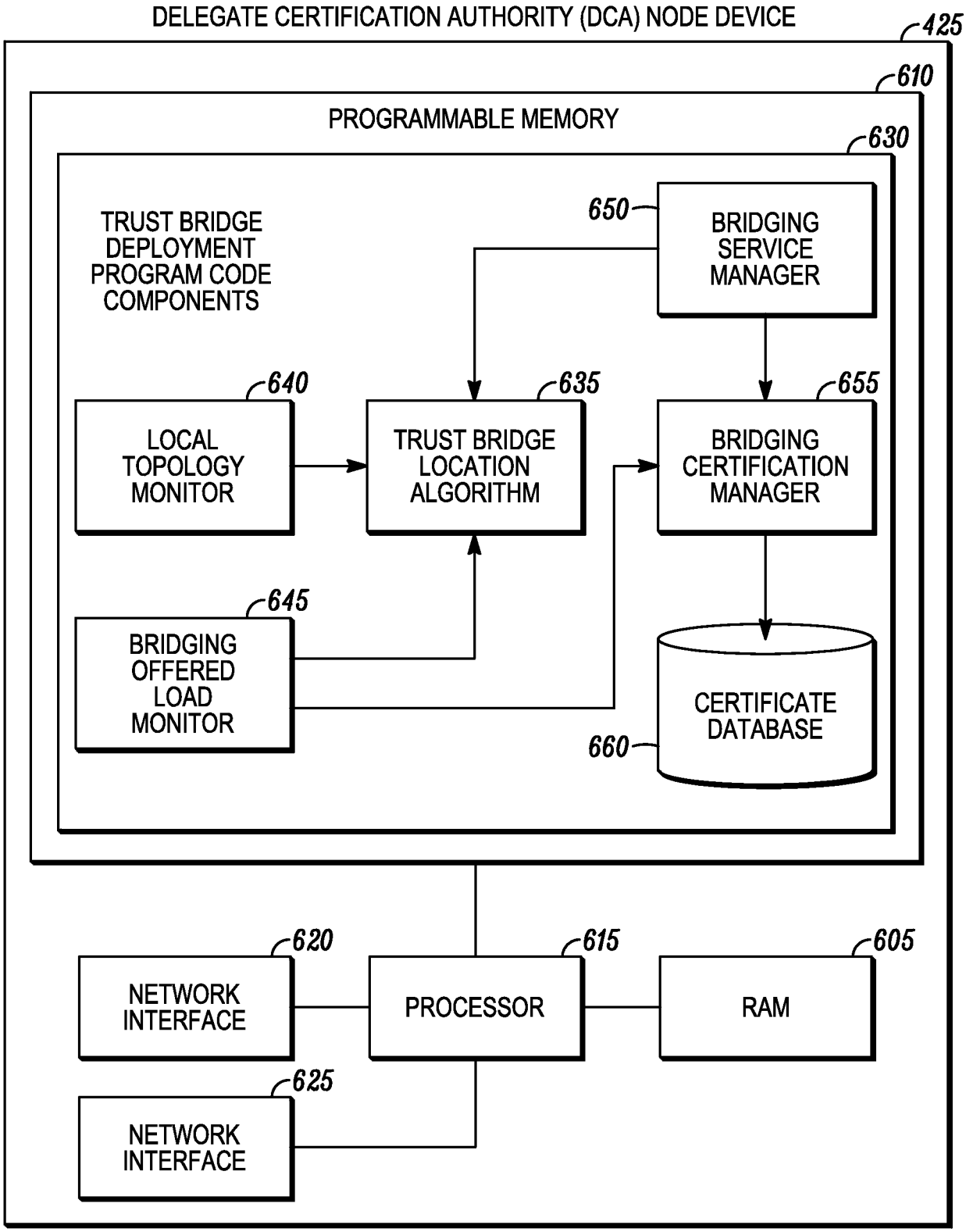

DELEGATE CERTIFICATION AUTHORITY (DCA) NODE DEVICE
425
610
PROGRAMMABLE MEMORY
630
TRUST BRIDGE DEPLOYMENT PROGRAM CODE COMPONENTS
650
BRIDGING SERVICE MANAGER
640
LOCAL TOPOLOGY MONITOR
635
TRUST BRIDGE LOCATION ALGORITHM
655
BRIDGING CERTIFICATION MANAGER
645
BRIDGING OFFERED LOAD MONITOR
CERTIFICATE DATABASE
660
620
NETWORK INTERFACE
615
PROCESSOR
605
RAM
625
NETWORK INTERFACE

FIG. 6

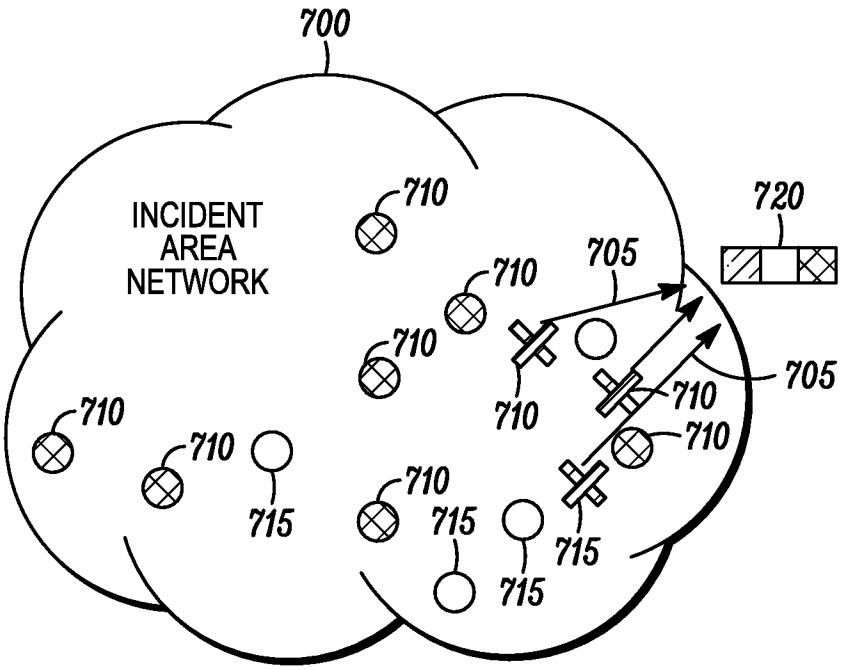

700
INCIDENT AREA NETWORK
710
720
705
715

FIG. 7

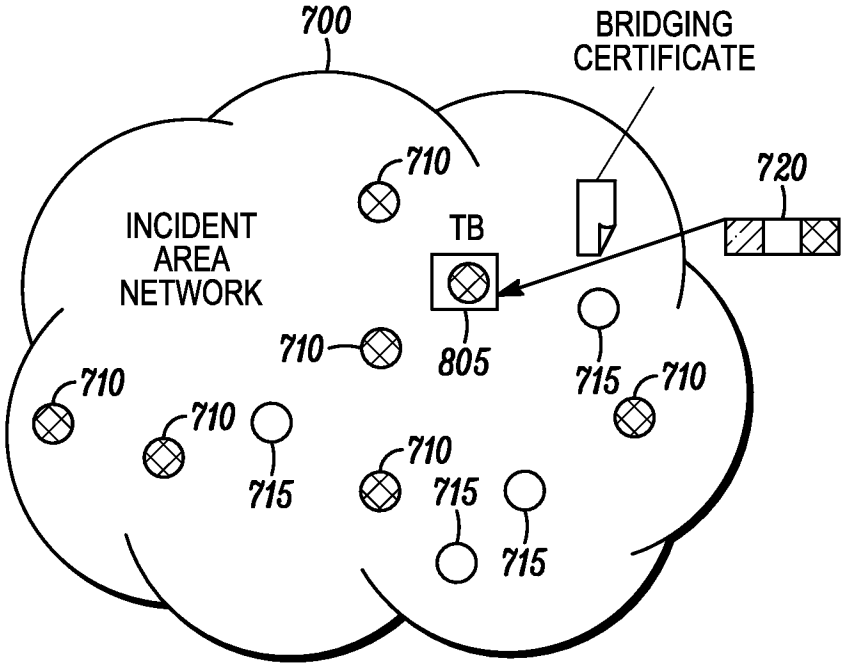

700
BRIDGING CERTIFICATE
INCIDENT AREA NETWORK
TB
805
710
720
715

FIG. 8

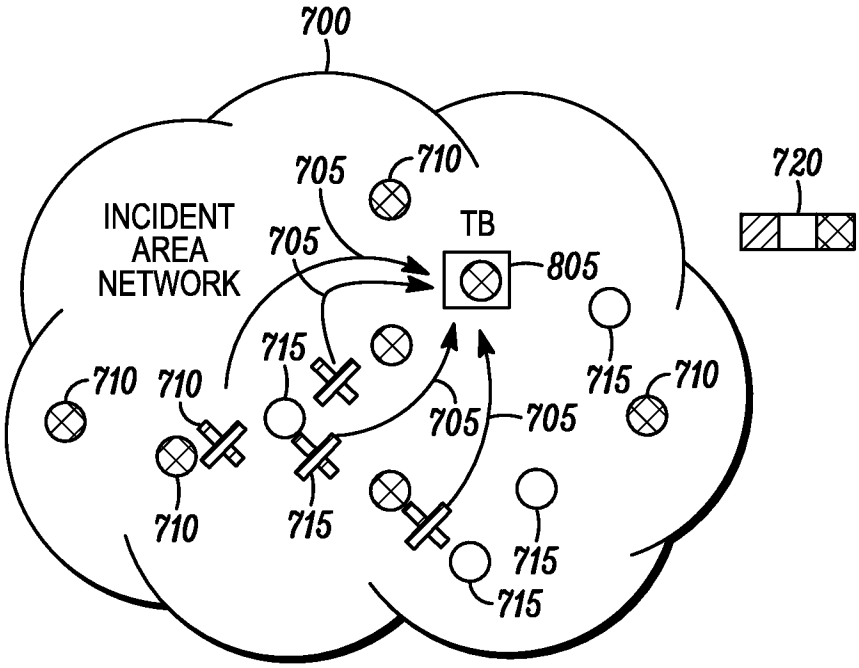

700
INCIDENT AREA NETWORK
TB
805
705
710
715
720

FIG. 9

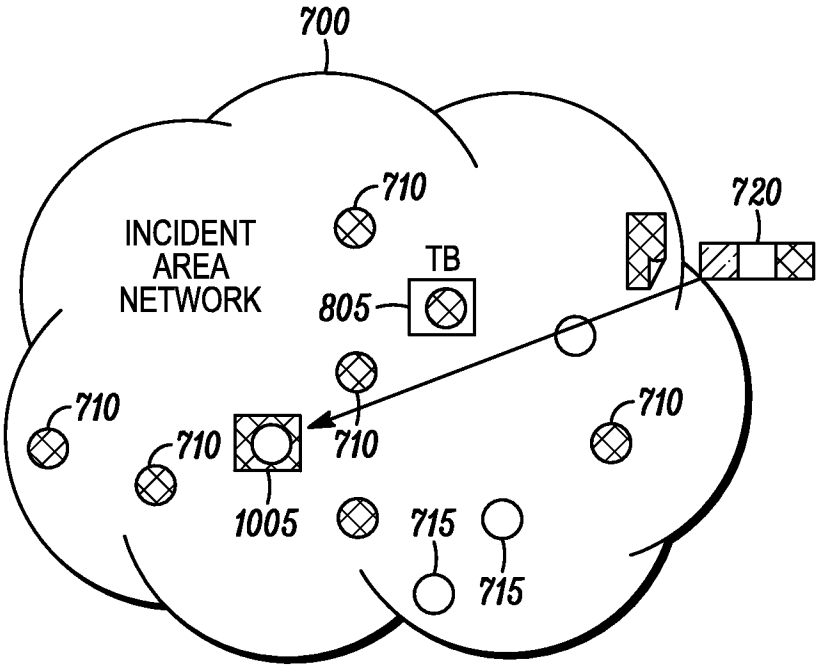

700
INCIDENT AREA NETWORK
TB
805
710
715
720
1005

FIG. 10

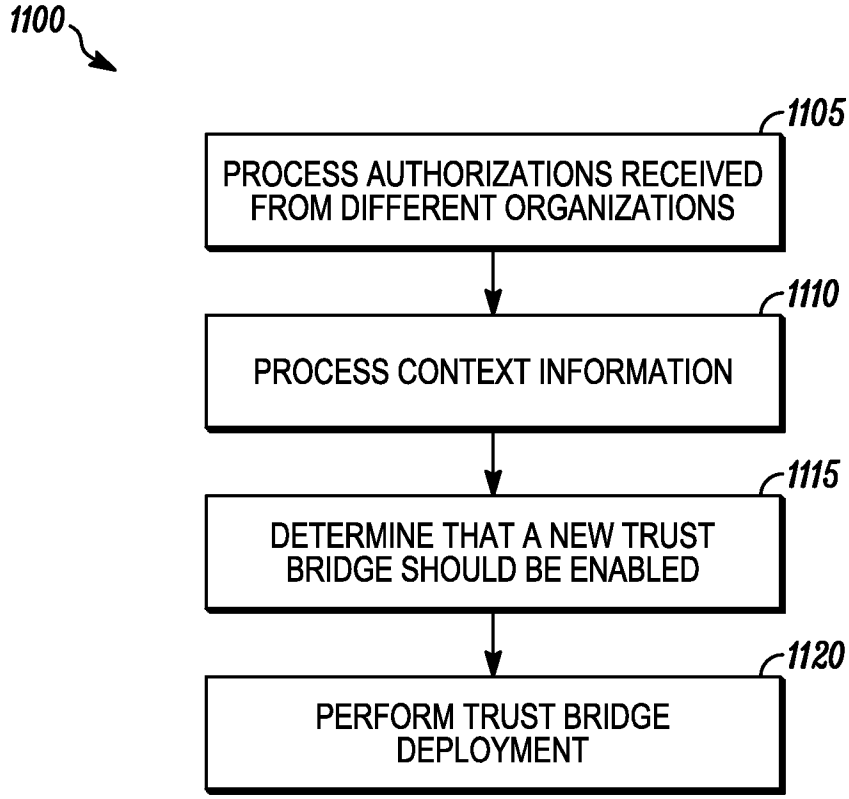

1100
1105
PROCESS AUTHORIZATIONS RECEIVED FROM DIFFERENT ORGANIZATIONS
1110
PROCESS CONTEXT INFORMATION
1115
DETERMINE THAT A NEW TRUST BRIDGE SHOULD BE ENABLED
1120
PERFORM TRUST BRIDGE DEPLOYMENT

FIG. 11

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2009/039054

A. CLASSIFICATION OF SUBJECT MATTER
INV. 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)
H04L G06F

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, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ZHENGPING WU, ALFRED C. WEAVER: "Using Web Service Enhancements to Bridge Business Trust Relationships" DEPARTMENT OF COMPUTER SCIENCE UNIVERSITY OF VIRGINIA, 1 November 2006 (2006-11-01), pages 1-8, XP002536183 PST 2006, Markham, Ontario, Canada page 3, paragraph 3.1 - page 4, paragraph 3.3	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
9 July 2009	21/07/2009

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	Figiel, Barbara

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2009/039054

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ALTERMAN P: "The US Federal PKI and the Federal Bridge Certification Authority" COMPUTER NETWORKS, ELSEVIER SCIENCE PUBLISHERS B.V., AMSTERDAM, NL, vol. 37, no. 6, 1 December 2001 (2001-12-01), pages 685-690, XP004324410 ISSN: 1389-1286 the whole document	1-20
A	US 2008/046716 A1 (EASTLAKE DONALD E [US] ET AL) 21 February 2008 (2008-02-21) paragraph [0022]; figure 4 paragraph [0025] - paragraph [0026]	1,14

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2009/039054

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008046716 A1	21-02-2008	NONE	