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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 June 2014 (19.06.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/092534 A1

(51) International Patent Classification:
H04W 84/18 (2009.01) *H04L 29/08* (2006.01)
H04L 29/06 (2006.01) *G06F 9/50* (2006.01)

(21) International Application Number:
PCT/MY2013/000230

(22) International Filing Date:
5 December 2013 (05.12.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI 2012005356 11 December 2012 (11.12.2012) MY

(71) Applicant: **MIMOS BERHAD** [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY).

(72) Inventors: **POH, Geong Sen**; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **MOHD AMRIL, Nurman Mohd Nazir**; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY).

(74) Agent: **MIRANDAH, Patrick**; Patrick Mirandah Co. (Malaysia) SDN BHD, Suite 3B-19-3 Plaza Sentral, Jalan Stesen Sentral 5, 50470 Kuala Lumpur (MY).

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

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

Declarations under Rule 4.17:

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

[Continued on next page]

(54) Title: A SYSTEM AND METHOD FOR PEER-TO-PEER ENTITY AUTHENTICATION WITH NEAREST NEIGHBOURS CREDENTIAL DELEGATION

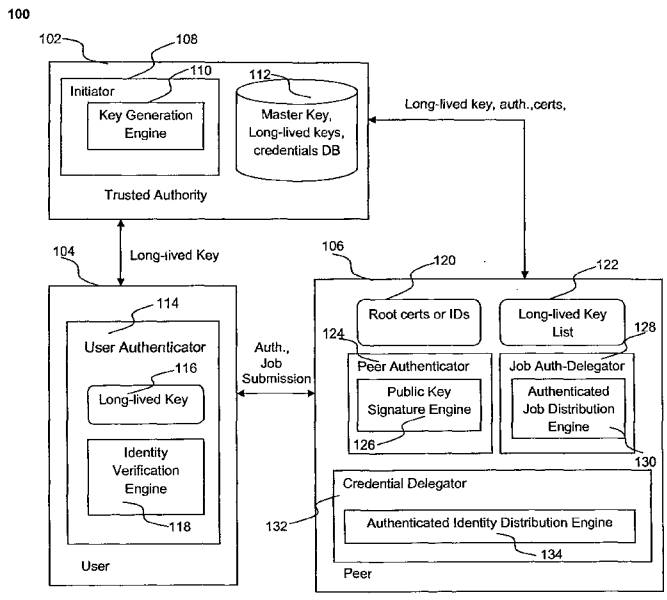


FIG. 1.0

(57) Abstract: A system and method for peer-to-peer entity authentication with nearest neighbours credential delegation is provided by using a hybrid approach of pre-shared symmetric keys on the user level and PKI on the peer level. The system includes an Initiator module (108) within a Trusted Authority (102); said Initiator module (108) is configured for registering users and peers, generating and distributing pre-shared keys to users and peers, wherein user submits job request and obtains processed results and a peer is at least a virtual machine; an User Authenticator module (114) configured for mutually authenticating users and peers through pre-shared keys and creating at least one session key for secure communication; a Peer Authenticator module (124) configured for mutually authenticating at least two peers through public key signature scheme and creating a session key for secure communication; a Credential Delegator module (132) configured for matching, retrieving and providing authentication credential of user not in the peer list to other peers, and further providing user's secret key transport; and a Job-Authentication-Delegator module (128) configured for matching, authenticating and providing authentication credential for delegating jobs to peer with applications suitable for processing jobs. The hybrid authentication approach and authenticated credential generation permits flexible peer discovery for direct submission of jobs.

WO 2014/092534 A1

— *of inventorship (Rule 4.17(iv))*

Published:

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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

A SYSTEM AND METHOD FOR PEER-TO-PEER ENTITY AUTHENTICATION WITH NEAREST NEIGHBOURS CREDENTIAL DELEGATION

FIELD OF INVENTION

The present invention relates to a system and method for peer-to-peer entity authentication with nearest neighbours credential delegation. In particular, the present invention provides for hybrid authentication approach and authenticated credential generation which permits flexible host discovery and authentication for direct submission of jobs.

BACKGROUND ART

Current architecture for virtualized environments in a cloud system does not provide mechanisms to verify authenticity of users and peers, job requests, and mutual authentication between peers. On the other hand, existing cloud authentication mechanism relies on centralized management infrastructure. Therefore, existing cloud authentication mechanism is not suitable in a virtual peer-to-peer environment as virtual peers are not centralized.

In current centralized cloud, all users and cloud hosts are registered to the front-end in a centralized architecture. In a peer-to-peer case, how do users and cloud hosts authenticate with one another in a decentralized environment without a centralized authority? Similarly, in centralized cloud, the cloud front-end initiates virtual machine provisioning to a particular cloud host that matches the user's specification. All cloud hosts are under the control of a centralized front-end. In decentralized peer-to-peer cloud, there is no single entity that controls and maintains information of all the cloud hosts. How can one be sure that incoming request (i.e., virtual machine provisioning request) and outgoing results from an entity are authentic?

These are the two main issues that the present invention addresses.Generally, in the existing cloud system, authentication and verification of users in a cloud is provided using Secure Shell (SSH). The user simply logs in to the front-end host via SSH. Once the user is authenticated by the front-end host, he or she can start to request virtual

machines. The front-end will then use the user credential to login to a scheduled cloud host via SSH. The user then SSH directly into the VM using the information provided by the front end. These steps are repeated each time a user requests for a virtual machines.

Another related existing mechanism, while not for the cloud system but towards peer-to-peer network is the United States Patent No. 7,899,188 B2, hereby denoted as US 188 Patent. It relates to authenticating peers in a peer-to-peer network, particularly for mobile devices. US 188 Patent provides entity authentication in a peer-to-peer setting by utilizing a symmetric key that is further used to generate a public key pair based in user identity as compared to the present invention which utilizes a hybrid approach of pre-shared symmetric keys on client level and PKI (public key infrastructure) on the host level. The said US 188 Patent exemplifies a system strictly for peer-to-peer authentication whereby no pre-shared key is required as compared to the present invention which utilizes hybrid authentication approach and authenticated credential generation which permits host discovery for direct submission of jobs.

Similar to the above, the United States Patent No. 7,127,613 B2, hereby denoted as US 613 Patent, also provides secure mechanism under peer-to-peer networking, but particularly to a system and method for secure exchange of messages and other data between peers in a peer-to-peer environment. In US 613 Patent, entity authentication is provided only on user level authentication through public key schemes. The peer-to-peer system is strictly for peer-to-peer authentication through generation of session keys and does not utilize hybrid authentication approach and authenticated credential generation which permits host discovery for direct submission of jobs as provided in the present application.

Also, Celesti et al. in their paper entitled "Three-Phase Cross-Cloud Federation Model: The Cloud SSO Authentication" proposed a peer-to-peer network environment, particularly, to a super peer based peer-to-peer network system, which is capable of providing a high-reliability service through secure user authentication, and a peer authentication method. In their proposal, entity authentication is provided by verifying authentication of user and peer through authentication information and public key infrastructure (PKI) of a user and a peer. It does not provide for user and job delegations

as provided in the present invention. It exemplifies a peer-to-peer system which is strictly for peer-to-peer authentication through generation of session keys and does not utilize hybrid authentication approach and authenticated credential generation which permits host discovery for direct submission of jobs as provided in the present application.

5

The subject matter claimed herein is not limited to embodiments that solve any disadvantages or that operate only in environments such as those described above. Rather, this background is only provided to illustrate one exemplary technology area where some embodiments described herein may be practiced.

SUMMARY OF INVENTION

The present invention relates to a system and method for peer-to-peer entity authentication with nearest neighbours credential delegation. In particular, the present invention provides for hybrid authentication approach and authenticated credential generation which permits flexible host discovery and authentication for direct submission of jobs.

One aspect of the present invention provides a system for peer-to-peer entity authentication with nearest neighbours credential delegation. The system comprising at least one Initiator module (108) within a Trusted Authority (102); said Initiator module (108) is configured for registering users and peers, generating and distributing pre-shared keys to users and peers, wherein user submits job request and obtains processed results and a peer is at least a virtual machine; at least one User Authenticator module (114) configured for mutually authenticating users and peers through pre-shared keys and creating at least one session key for secure communication; at least one Peer Authenticator module (124) configured for mutually authenticating at least two peers through public key signature scheme and creating at least one session key for secure communication; at least one Credential Delegator module (132) configured for matching, retrieving and providing authentication credential of user not in the peer list to other peers, and further providing user's secret key transport; and at least one Job-Authentication-Delegator module (128) configured for matching, authenticating and providing authentication credential for delegating jobs to peer with applications suitable for processing jobs.

In another aspect the invention provides a system wherein the said Initiator module (108) further comprising at least one Key Generation Engine (110) having means for generating long-term master secret key using at least one pseudo-random bit generator; generating long term secret keys using said master secret and said pseudo-random bit generator; and generating public private key pairs and digital certificates.

In yet another aspect of the invention there is provided a system wherein said User Authenticator module (114) further comprising at least one Identity Verification Engine (118) having means for generating at least one authentication token in the form of a

Message Authentication Code (MAC) containing at least a user ID and a random nonce; and computing and verifying MACs with pre-shared key.

In still another aspect of the invention there is provided a system wherein said Credential Delegator module (132) further comprising at least one Authenticated Identity Distribution Engine (134) having means for broadcasting at least one user ID by an original peer to request for an authenticated user credential which matches said user ID; verifying said request of original peer by other peers, searching and comparing said user ID with nearest neighbours lists of different peers by other peers; retrieving pre-shared key by a matching peer and encrypting the retrieved key with the public key of the original peer; signing said user ID and encrypted key by a matching peer and forwarding said user ID together with said encrypted key to said original peer; and verifying said signature, decrypting said key and verifying authenticity of user requesting job submission by said original peer.

In a further aspect of the invention there is provided a system wherein said Job-Authenticator Delegator (128) module further comprising at least one Authenticated Job Distribution Engine (130) having means for broadcasting at least one user ID and job ID by an original peer to other peers capable of processing jobs; verifying said request of original peer by other peers, matching job description in ID with capabilities of original peer by other peers; informing original peer its capability of processing said job upon determining matching peer for authentication; and verifying and informing job requestor of availability of at least one peer capable of processing said job by said original peer.

In another aspect the invention provides a method for peer-to-peer entity authentication with nearest neighbours credential delegation. The method comprising steps of registering all users and peers and generating pre-shared long lived secret keys using master secret key (202); registering peers and generating certificates for all peers (204); generating at least one authenticated user credential for mutually authenticating users and peers (206); matching, retrieving and providing authentication credential of user not in the peer list to other peers, and further providing user's secret key transport (208); matching, authenticating and providing authentication credential for delegating jobs to peer with applications suitable for processing jobs (210); and mutually authenticating at

least two peers through public key signature scheme and creating at least one session key for secure communication (212).

In a further aspect of the invention there is provided a method wherein generating at least one authenticated user credential for mutually authenticating users and peers further comprising steps of authenticating user to peer by providing user and job IDs and computing at least a MAC with a pre-shared key (302); matching peer with user ID with peer's list of nearest neighbours containing user ID and pre-shared key (304); directing to Credential Delegator module if there is no matching user ID (306); retrieving pre-shared key matching said ID by said peer and computing a MAC based on said key by said peer when user ID is available upon matching by first peer and when user ID is available upon matching steps from Credential Delegator module (308); verifying job ID and application by peer to process job when there are matching MACs (310); and allowing user to access resources and computing session key for secure communication (312) when there are available applications; else directing to Job-Authentication Delegator module when applications are not available.

In still a further aspect of the invention there is provided a method wherein matching, retrieving and providing authentication credential of user not in the peer list to other peers, and further providing user's secret key transport further comprising steps of broadcasting user ID by peer to other peers by signing user ID with freshness mechanism (402); verifying said signature by other peers (404); matching user ID with nearest neighbors list by other peers upon verification of said signature (406); directing to first time job request when user ID is not available (408); retrieving pre-shared key of said user by said peer with matching ID and encrypting said key with original host key upon availability of user ID (410); signing user ID and encrypted key by peer with matching ID and sending said signature to original peer (412); verifying said signature by original peer and return to User Authenticator module upon successful verification (414).

In yet another aspect of the invention there is provided a method wherein directing to first time job request when user ID is not available (408) further comprises steps of sending user ID to trusted authority by original peer (502); mutual verification between trusted authority and peer using MAC (504); matching user ID with its register list by trusted authority (506); directing to Credential Delegator module if there is no matching

user ID (508); encrypting long-lived shared key using shared key with peer by trusted authority when user ID is available (510); and sending encrypted shared key to peer and return to User Authenticator module (512).

In another aspect of the invention there is provided a method wherein matching, authenticating and providing authentication credential for delegating jobs to peer with applications suitable for processing jobs further comprises steps of broadcasting user and job IDs by peer to other peer by generating at least one signature on job ID with freshness mechanism (602); verifying signature by other peers (604); matching job ID with list of applications by other peers upon successful verification of signature (606); signing job ID by peer with matching application sending said job ID to original peer when matching jobs are available (608);verifying signature by original peers (610); and informing user by original peer on peer having capability to process said jobs (612).

In yet another aspect the invention provides a method wherein mutually authenticating at least two peers through public key signature scheme and creating at least one session key for secure communication further comprises steps of agreeing on authentication and freshness mechanism by peers (702); first peer authenticating second peer by computing at least one credential token which is at least a digital signature using at least one private key (704); verifying said signature by second peer (706); said second peer authenticating to first peer by computing a credential token which is at least a digital signature using a private key (708); said first peer verifying said signature (710); and mutual authentication between said first peer and said second peer and computing at least one session key for subsequent secure communication (712).

The present invention consists of features and a combination of parts hereinafter fully described and illustrated in the accompanying drawings, it being understood that various changes in the details may be made without departing from the scope of the invention or sacrificing any of the advantages of the present invention.

BRIEF DESCRIPTION OF ACCOMPANYING DRAWINGS

To further clarify various aspects of some embodiments of the present invention, a more particular description of the invention will be rendered by references to specific embodiments thereof, which are illustrated in the appended drawings. It is appreciated that these drawings depict only typical embodiments of the invention and are therefore not to be considered limiting of its scope. The invention will be described and explained with additional specificity and detail through the accompanying drawings in which:

FIG. 1.0 illustrates the system of an embodiment of the invention.

FIG. 2.0 is a flowchart illustrating the method for peer-to-peer entity authentication with nearest neighbours credential delegation.

FIG. 3.0 is a flowchart illustrating the system flow of User Authenticator module.

FIG. 4.0 is a flowchart illustrating the system flow of Credential Delegator module.

FIG. 5.0 is a flowchart illustrating the system flow of first time job request.

FIG. 6.0 is a flowchart illustrating the system flow of Job-Authentication-Delegator module.

FIG. 7.0 is a flowchart illustrating the system flow of Peer Authenticator module.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention provides a system and method for peer-to-peer entity authentication with nearest neighbours credential delegation. In particular, the present invention provides for hybrid authentication approach and authenticated credential generation which permits flexible host discovery for direct submission of jobs for authentication.

Hereinafter, this specification will describe the present invention according to the preferred embodiments. It is to be understood that limiting the description to the preferred embodiments of the invention is merely to facilitate discussion of the present invention and it is envisioned without departing from the scope of the appended claims.

Referring to FIG 1.0, the system (100) according to an embodiment of the invention is illustrated. The system (100) includes an Initiator module (108) within a Trusted Authority (102); said Initiator module (108) is configured for registering users and peers, generating and distributing pre-shared keys to users and peers, wherein user submits job request and obtains processed results and a peer is at least a virtual machine. The Initiator module (108) is in communication with an User Authenticator module (114) wherein the User Authentication module is configured for mutually authenticating users and peers through pre-shared keys and creating at least one session key for secure communication. A Peer Authenticator module (124) is provided and is configured for mutually authenticating at least two peers through public key signature scheme and creating at least one session key for secure communication. A Credential Delegator module (132) is also provided and configured for matching, retrieving and providing authentication credential of user not in the peer list to other peers, and further providing user's secret key transport. A Job-Authentication-Delegator module (128) is also provided. This is configured for matching, authenticating and providing authentication credential for delegating jobs to peer with applications suitable for processing jobs.

A more detailed description of the Initiator module (108) may be seen within the system architecture of FIG. 2.0. More particularly, the Initiator module (108) includes a Key Generation Engine (110) for generating long-term master secret key using at least one pseudo-random bit generator; generating long term secret keys using said master secret

and said pseudo-random bit generator; and generating public private key pairs and digital certificates. The User Authenticator module (114) further comprising an Identity Verification Engine (118) having means for generating at least one authentication token in the form of a Message Authentication Code (MAC) containing at least a user ID and a random nonce; and computing and verifying MACs with pre-shared key.

The Credential Delegator module (132) generally includes an Authenticated Identity Distribution Engine (134) having means for broadcasting at least one user ID by an original peer to request for an authenticated user credential which matches said user ID; verifying said request of original peer by other peers, searching and comparing said user ID with nearest neighbours lists of different peers by other peers; retrieving pre-shared key by a matching peer and encrypting the retrieved key with the public key of the original peer; signing said user ID and encrypted key by a matching peer and forwarding said user ID together with said encrypted key to said original peer; and verifying said signature, decrypting said key and verifying authenticity of user requesting job submission by said original peer.

The Job-Authenticator Delegator (128) module further comprising an Authenticated Job Distribution Engine (130), The Authenticated Job Distribution Engine (130) is configured for broadcasting at least one user ID and job ID by an original peer to other peers capable of processing jobs; verifying said request of original peer by other peers, matching job description in ID with capabilities of original peer by other peers; informing original peer its capability of processing said job upon determining matching peer for authentication; and verifying and informing job requestor of availability of at least one peer capable of processing said job by said original peer.

Referring to FIGs. 2 through 7, an embodiment of the methodology (200) of the invention is illustrated. Generally, the invention includes the steps of registering all users and peers and generating pre-shared long lived secret keys using master secret key (202); registering peers and generating certificates for all peers (204); generating at least one authenticated user credential for mutually authenticating users and peers (206); matching, retrieving and providing authentication credential of user not in the peer list to other peers, and further providing user's secret key transport (208); matching, authenticating and providing authentication credential for delegating jobs to peer with

applications suitable for processing jobs (210); and mutually authenticating at least two peers through public key signature scheme and creating at least one session key for secure communication (212).

The step of generating at least one authenticated user credential for mutually authenticating users and peers further includes authenticating user to peer by providing user and job IDs and computing at least a MAC with a pre-shared key (302); matching peer with user ID with peer's list of nearest neighbours containing user ID and pre-shared key (304); directing to Credential Delegator module if there is no matching user ID (306); retrieving pre-shared key matching said ID by said peer and computing a MAC based on said key by said peer when user ID is available upon matching by first peer and when user ID is available upon matching steps from Credential Delegator module (308); verifying job ID and application by peer to process job when there are matching MACs (310); and allowing user to access resources and computing session key for secure communication (312) when there are available applications; else directing to Job-Authentication-Delegator module when applications are not available.

The step of matching, retrieving and providing authentication credential of user not in the peer list to other peers, and further providing user's secret key transport further includes broadcasting user ID by peer to other peers by signing user ID with freshness mechanism (402); verifying said signature by other peers (404); matching user ID with nearest neighbors list by other peers upon verification of said signature (406); directing to first time job request when user ID is not available (408); retrieving pre-shared key of said user by said peer with matching ID and encrypting said key with original host key upon availability of user ID (410); signing user ID and encrypted key by peer with matching ID and sending said signature to original peer (412); verifying said signature by original peer and return to User Authenticator module upon successful verification (414).

The step of directing to first time job request when user ID is not available (408) further includes sending user ID to trusted authority by original peer (502); mutual verification between trusted authority and peer using MAC (504); matching user ID with its register list by trusted authority (506); directing to Credential Delegator module if there is no matching user ID (508); encrypting long-lived shared key using shared key with peer by

trusted authority when user ID is available (510); and sending encrypted shared key to peer and return to User Authenticator module (512).

The step of matching, authenticating and providing authentication credential for delegating jobs to peer with applications suitable for processing jobs further includes broadcasting user and job IDs by peer to other peer by generating at least one signature on job ID with freshness mechanism (602); verifying signature by other peers (604); matching job ID with list of applications by other peers upon successful verification of signature (606); signing job ID by peer with matching application sending said job ID to original peer when matching jobs are available (608); verifying signature by original peers (610); and informing user by original peer on peer having capability to process said jobs (612).

The step of mutually authenticating at least two peers through public key signature scheme and creating at least one session key for secure communication further includes agreeing on authentication and freshness mechanism by peers (702); first peer authenticating second peer by computing at least one credential token which is at least a digital signature using at least one private key (704); verifying said signature by second peer (706); said second peer authenticating to first peer by computing a credential token which is at least a digital signature using a private key (708); said first peer verifying said signature (710); and mutual authentication between said first peer and said second peer and computing at least one session key for subsequent secure communication (712).

The present invention provides for peer-to-peer entity authentication with nearest neighbours credential delegation by utilizing hybrid approach of the pre-shared symmetric keys on the client level and the public key infrastructure (PKI) of the host level. In addition, the present invention provides for hybrid authentication approach and authenticated credential generation which permits flexible host discovery for direct submission of jobs for authentication.

Unless the context requires otherwise or specifically stated to the contrary, integers, steps or elements of the invention recited herein as singular integers, steps or elements clearly encompass both singular and plural forms of the recited integers, steps or elements.

Throughout this specification, unless the context requires otherwise, the word "comprise", or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated step or element or integer or group of steps or elements or integers, but not the exclusion of any other step or element or integer or group of steps, elements or integers. Thus, in the context of this specification, the term "comprising" is used in an inclusive sense and thus should be understood as meaning "including principally, but not necessarily solely".

It will be appreciated that the foregoing description has been given by way of illustrative example of the invention and that all such modifications and variations thereto as would be apparent to persons of skill in the art are deemed to fall within the broad scope and ambit of the invention as herein set forth.

CLAIMS

1. A system (100) for peer-to-peer entity authentication with nearest neighbours credential delegation, the system comprising:

at least one Initiator module (108) within a Trusted Authority (102); said Initiator module (108) is configured for registering users and peers, generating and distributing pre-shared keys to users and peers, wherein user submits job request and obtains processed results and a peer is at least a virtual machine;

at least one User Authenticator module (114) configured for mutually authenticating users and peers through pre-shared keys and creating at least one session key for secure communication;

at least one Peer Authenticator module (124) configured for mutually authenticating at least two peers through public key signature scheme and creating at least one session key for secure communication;

at least one Credential Delegator module (132) configured for matching, retrieving and providing authentication credential of user not in the peer list to other peers, and further providing user's secret key transport; and

at least one Job-Authentication-Delegator module (128) configured for matching, authenticating and providing authentication credential for delegating jobs to peer with applications suitable for processing jobs characterized in that

the at least one Initiator module (108) within a Trusted Authority (102) further comprising at least one Key Generation Engine (110) having means for:

generating long-term master secret key using at least one pseudo-random bit generator;

generating long term secret keys using said master secret and said pseudo-random bit generator; and

generating public private key pairs and digital certificates;

the at least one Credential Delegator module (132) further comprising at least one Authenticated Identity Distribution Engine (134) having means for:

broadcasting at least one user ID by an original peer to request for an authenticated user credential which matches said user ID;

verifying said request of original peer by other peers, searching and comparing said user ID with nearest neighbours lists of different peers by other peers;

retrieving pre-shared key by a matching peer and encrypting the retrieved key with the public key of the original peer;

signing said user ID and encrypted key by a matching peer and forwarding said user ID together with said encrypted key to said original peer; and

verifying said signature, decrypting said key and verifying authenticity of user requesting job submission by said original peer; and

the Job-Authenticator Delegator (128) module further comprising at least one Authenticated Job Distribution Engine (130) having means for:

broadcasting at least one user ID and job ID by an original peer to other peers capable of processing jobs;

verifying said request of original peer by other peers, matching job description in ID with capabilities of original peer by other peers;

informing original peer its capability of processing said job upon determining matching peer for authentication; and

verifying and informing job requestor of availability of at least one peer capable of processing said job by said original peer.

2. A system (104) according to Claim 1, wherein said User Authenticator module (114) further comprising at least one Identity Verification Engine (118) having means for:

generating at least one authentication token in the form of a Message Authentication Code (MAC) containing at least a user ID and a random nonce; and

computing and verifying MACs with pre-shared key.

3. A method (200) for peer-to-peer entity authentication with nearest neighbours credential delegation, the method comprising steps of:

registering all users and peers and generating pre-shared long lived secret keys using master secret key (202);

registering peers and generating certificates for all peers (204);

generating at least one authenticated user credential for mutually authenticating users and peers (206);

matching, retrieving and providing authentication credential of user not in the peer list to other peers, and further providing user's secret key transport (208);

matching, authenticating and providing authentication credential for delegating jobs to peer with applications suitable for processing jobs (210); and

mutually authenticating at least two peers through public key signature scheme and creating at least one session key for secure communication (212)

characterized in that

matching, retrieving and providing authentication credential of user not in the peer list to other peers, and further providing user's secret key transport further comprising steps of:

broadcasting user ID by peer to other peers by signing user ID with freshness mechanism (402);

verifying said signature by other peers (404);

matching user ID with nearest neighbors list by other peers upon verification of said signature (406);

directing to first time job request when user ID is not available (408);

retrieving pre-shared key of said user by said peer with matching ID and encrypting said key with original host key upon availability of user ID (410);

signing user ID and encrypted key by peer with matching ID and sending said signature to original peer (412);

verifying said signature by original peer and return to User Authenticator module upon successful verification (414);

matching, authenticating and providing authentication credential for delegating jobs to peer with applications suitable for processing jobs further comprises steps of:

broadcasting user and job IDs by peer to other peer by generating at least one signature on job ID with freshness mechanism (602);

verifying signature by other peers (604);

matching job ID with list of applications by other peers upon successful verification of signature (606);

signing job ID by peer with matching application sending said job ID to original peer when matching jobs are available (608);

verifying signature by original peers (610); and

informing user by original peer on peer having capability to process said jobs (612).

4. A method (300) according to Claim 3, wherein generating at least one authenticated user credential for mutually authenticating users and peers further comprising steps of:

authenticating user to peer by providing user and job IDs and computing at least a MAC with a pre-shared key (302);

matching peer with user ID with peer's list of nearest neighbours containing user ID and pre-shared key (304);

directing to Credential Delegator module if there is no matching user ID (306);

retrieving pre-shared key matching said ID by said peer and computing a MAC based on said key by said peer when user ID is available upon matching by first peer and when user ID is available upon matching steps from Credential Delegator module (308);

verifying job ID and application by peer to process job when there are matching MACs (310); and

allowing user to access resources and computing session key for secure communication (312) when there are available applications; else directing to Job-Authentication-Delegator module when applications are not available.

5. A method (500) according to Claim 3, wherein directing to first time job request when user ID is not available (408) further comprises steps of:

sending user ID to trusted authority by original peer (502);

mutual verification between trusted authority and peer using MAC (504);

matching user ID with its register list by trusted authority (506);

directing to Credential Delegator module if there is no matching user ID (508);

encrypting long-lived shared key using shared key with peer by trusted authority when user ID is available (510); and

sending encrypted shared key to peer and return to User Authenticator module (512).

6. A method according to Claim 3, wherein mutually authenticating at least two peers through public key signature scheme and creating at least one session key for secure communication further comprises steps of:

agreeing on authentication and freshness mechanism by peers (702);

first peer authenticating second peer by computing at least one credential token which is at least a digital signature using at least one private key (704);

verifying said signature by second peer (706);

said second peer authenticating to first peer by computing a credential token which is at least a digital signature using a private key (708);

said first peer verifying said signature (710); and

mutual authentication between said first peer and said second peer and computing at least one session key for subsequent secure communication (712).

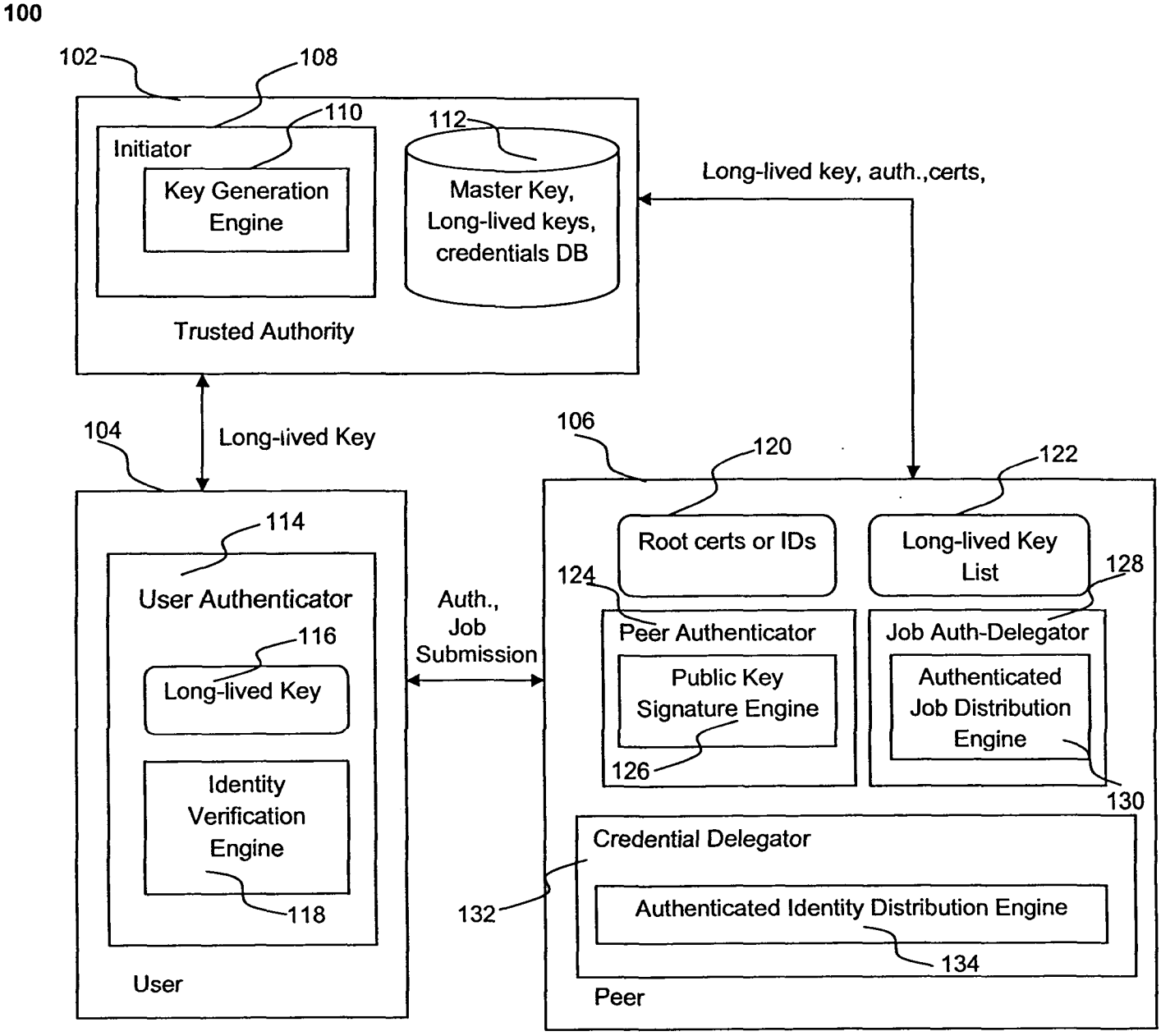

100
102
108
110
112
Initiator
Key Generation Engine
Master Key, Long-lived keys, credentials DB
Trusted Authority
Long-lived key, auth.,certs,
104
Long-lived Key
106
120
122
114
User Authenticator
116
Long-lived Key
Identity Verification Engine
118
User
Auth., Job Submission
Root certs or IDs
Long-lived Key List
124
128
Peer Authenticator
Public Key Signature Engine
126
Job Auth-Delegator
Authenticated Job Distribution Engine
130
Credential Delegator
132
Authenticated Identity Distribution Engine
134
Peer

FIG. 1.0

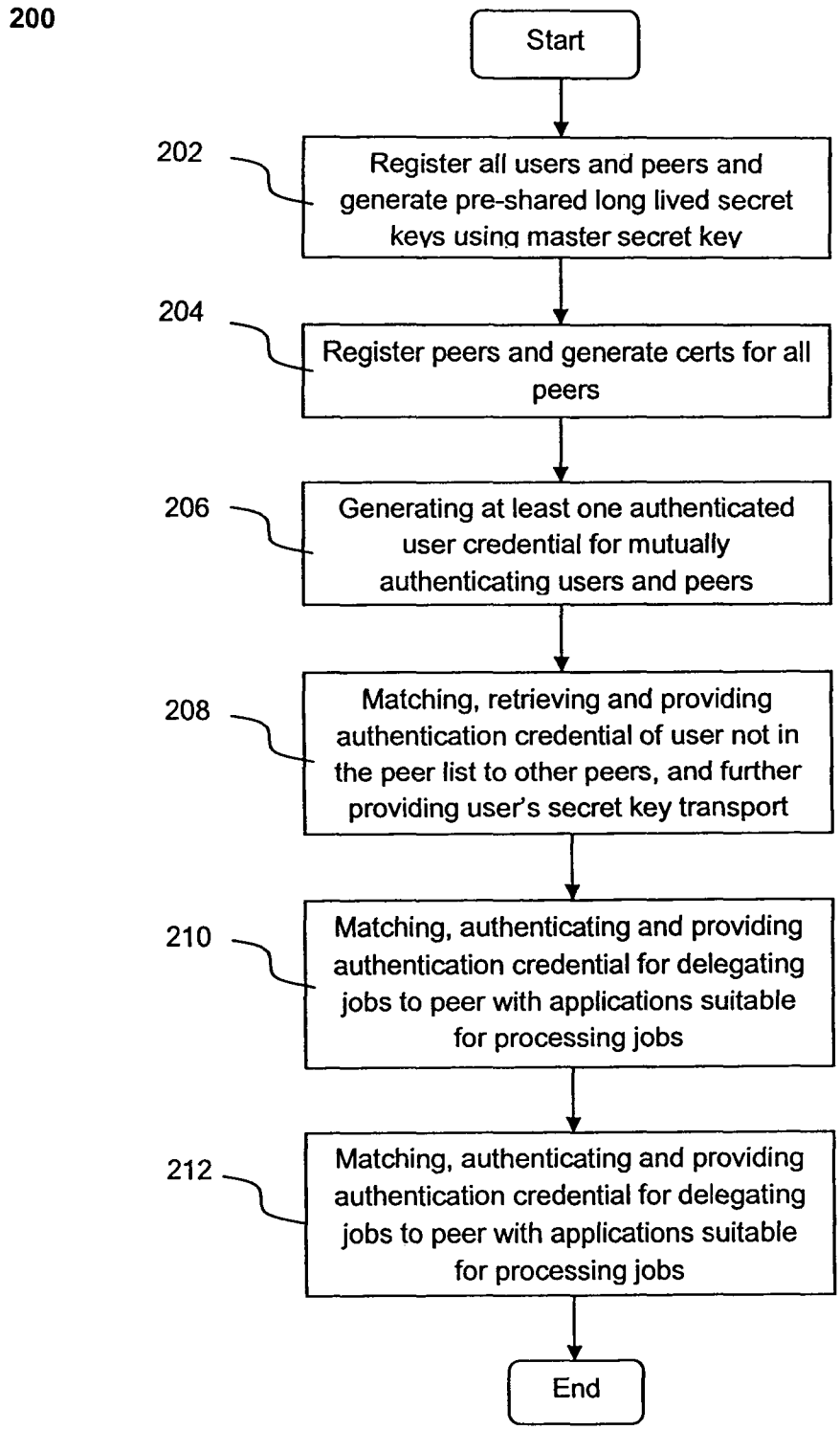
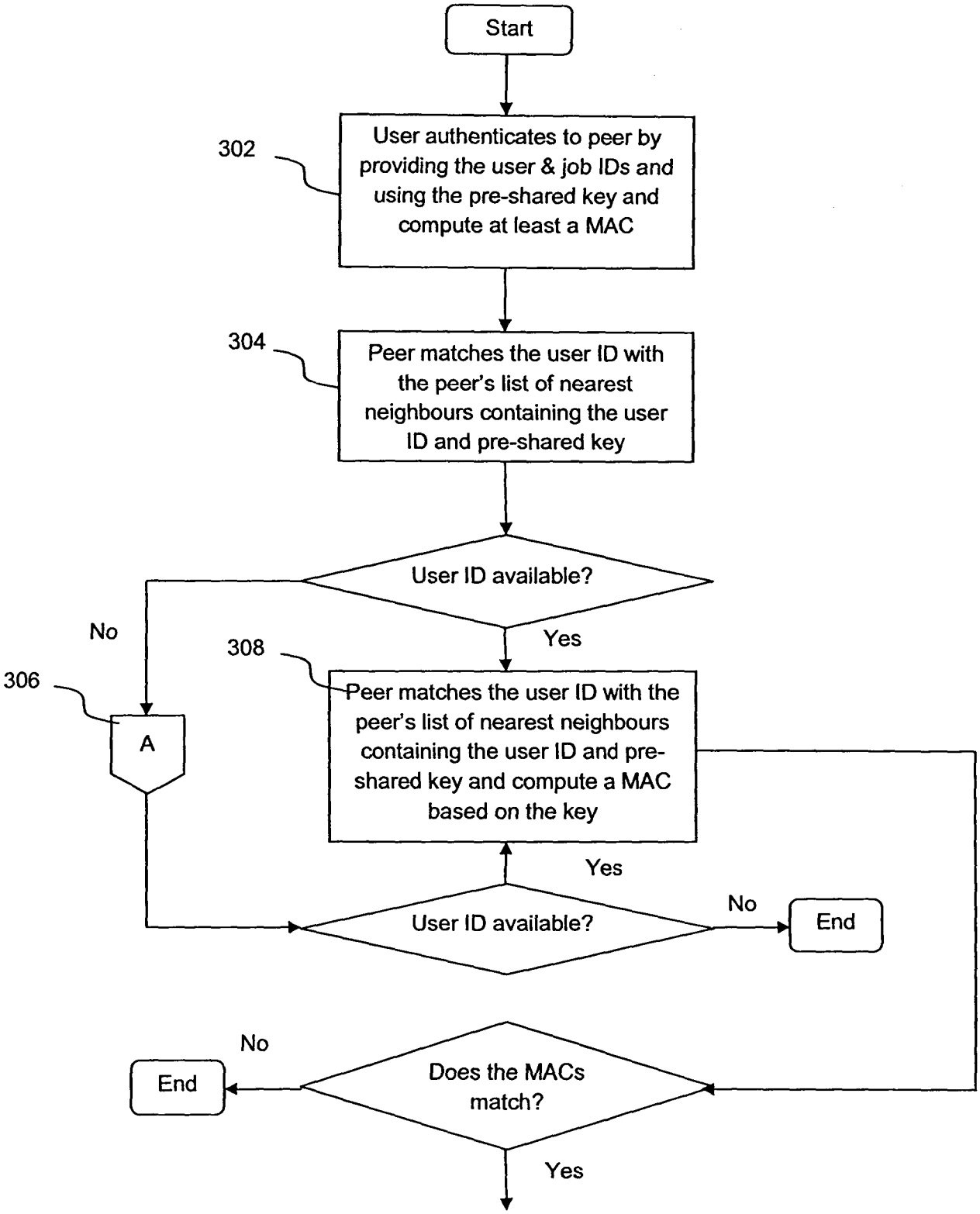

200
Start
202
Register all users and peers and generate pre-shared long lived secret keys using master secret key
204
Register peers and generate certs for all peers
206
Generating at least one authenticated user credential for mutually authenticating users and peers
208
Matching, retrieving and providing authentication credential of user not in the peer list to other peers, and further providing user's secret key transport
210
Matching, authenticating and providing authentication credential for delegating jobs to peer with applications suitable for processing jobs
212
Matching, authenticating and providing authentication credential for delegating jobs to peer with applications suitable for processing jobs
End

FIG. 2.0

300


Start
302
User authenticates to peer by providing the user & job IDs and using the pre-shared key and compute at least a MAC
304
Peer matches the user ID with the peer's list of nearest neighbours containing the user ID and pre-shared key
User ID available?
No
Yes
306
A
308
Peer matches the user ID with the peer's list of nearest neighbours containing the user ID and pre-shared key and compute a MAC based on the key
Yes
User ID available?
No
End
No
End
Does the MACs match?
Yes

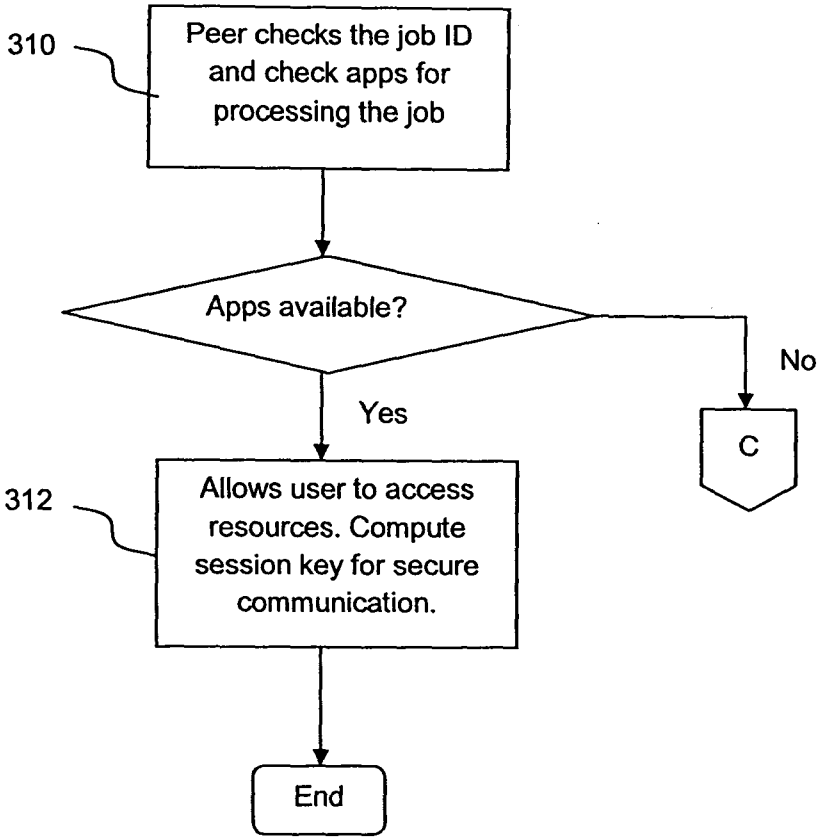
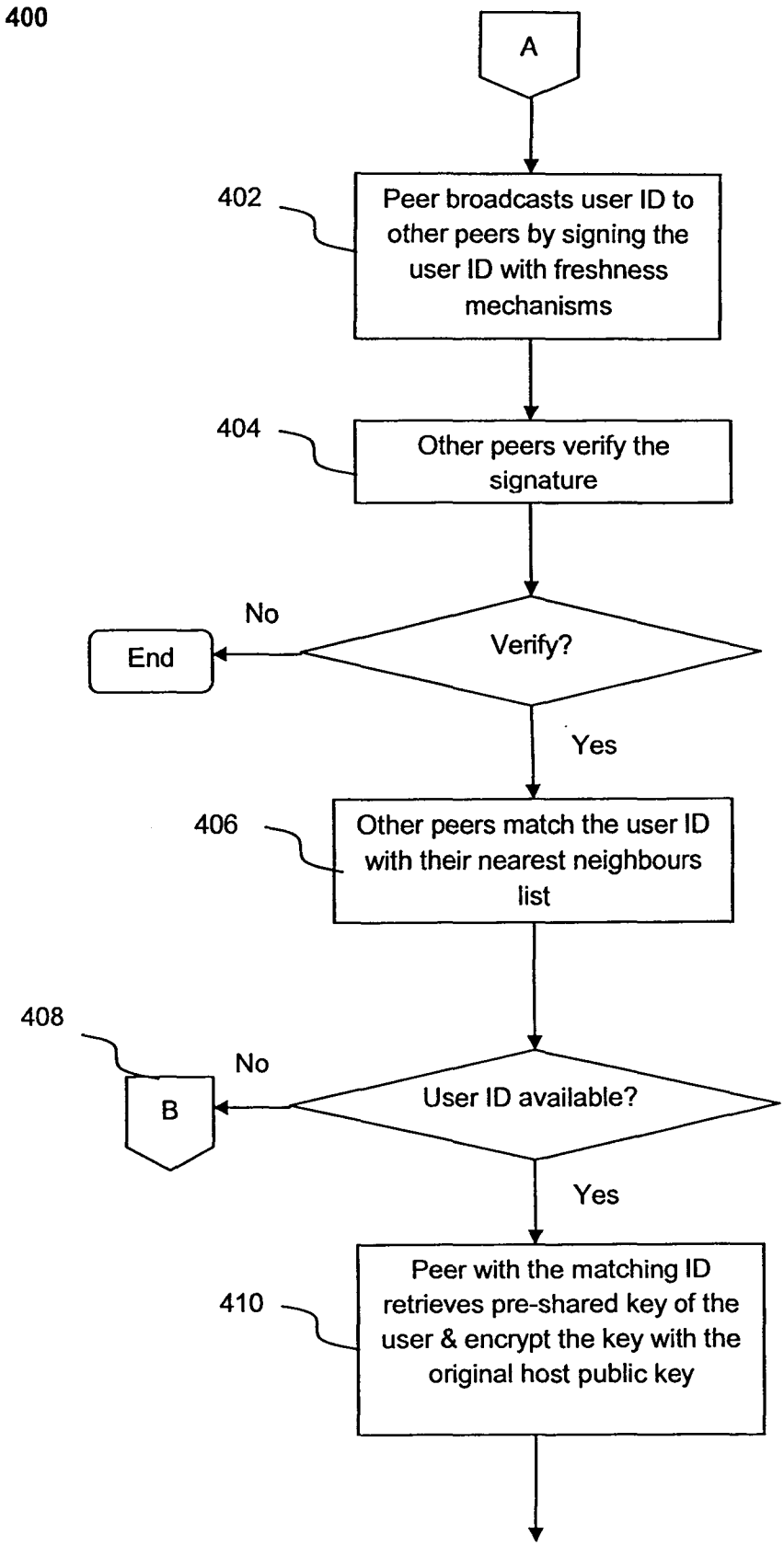

310
Peer checks the job ID and check apps for processing the job
Apps available?
No
C
Yes
312
Allows user to access resources. Compute session key for secure communication.
End

FIG. 3.0


400
A
402
Peer broadcasts user ID to other peers by signing the user ID with freshness mechanisms
404
Other peers verify the signature
No
End
Verify?
Yes
406
Other peers match the user ID with their nearest neighbours list
408
No
B
User ID available?
Yes
410
Peer with the matching ID retrieves pre-shared key of the user & encrypt the key with the original host public key

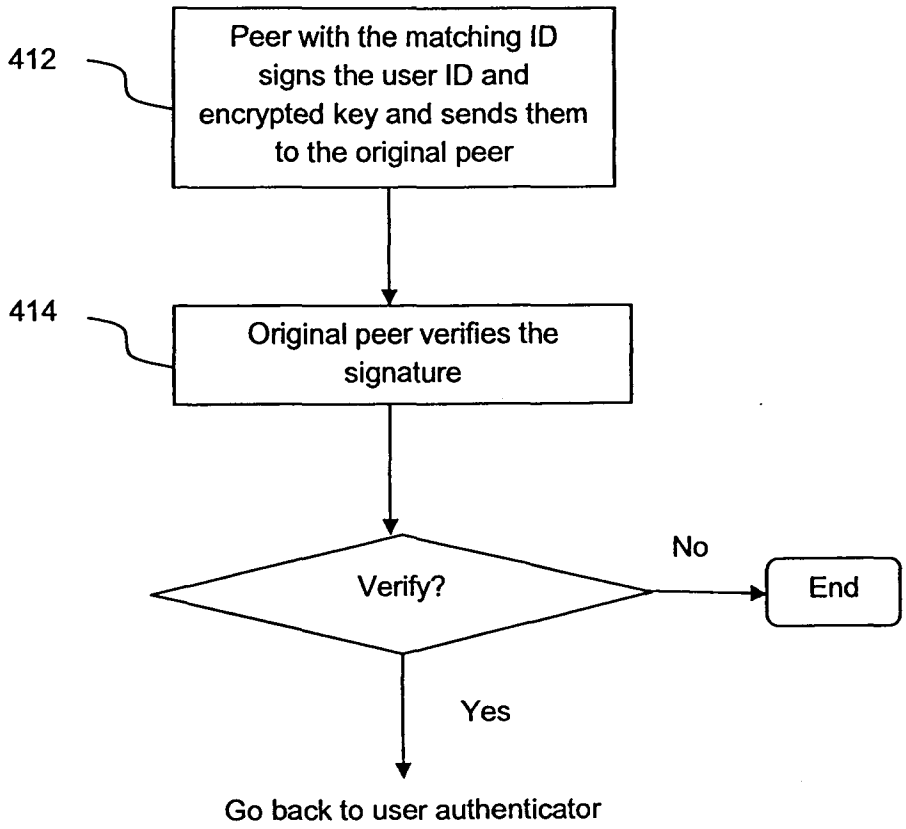

412
Peer with the matching ID signs the user ID and encrypted key and sends them to the original peer
414
Original peer verifies the signature
Verify?
No
End
Yes
Go back to user authenticator

FIG. 4.0

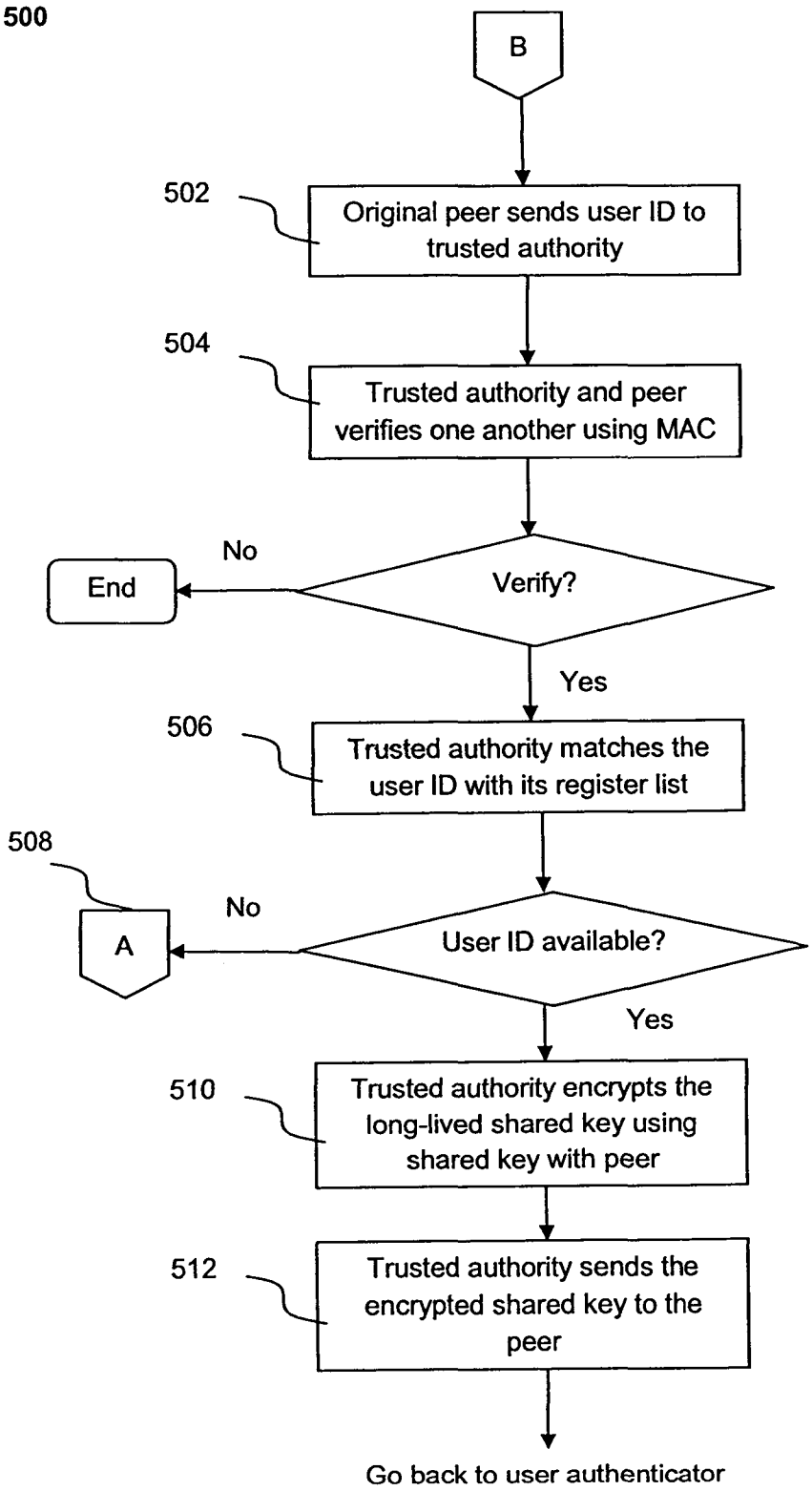

500
B
502
Original peer sends user ID to trusted authority
504
Trusted authority and peer verifies one another using MAC
Verify?
No
End
Yes
506
Trusted authority matches the user ID with its register list
508
User ID available?
No
A
Yes
510
Trusted authority encrypts the long-lived shared key using shared key with peer
512
Trusted authority sends the encrypted shared key to the peer
Go back to user authenticator

FIG. 5.0

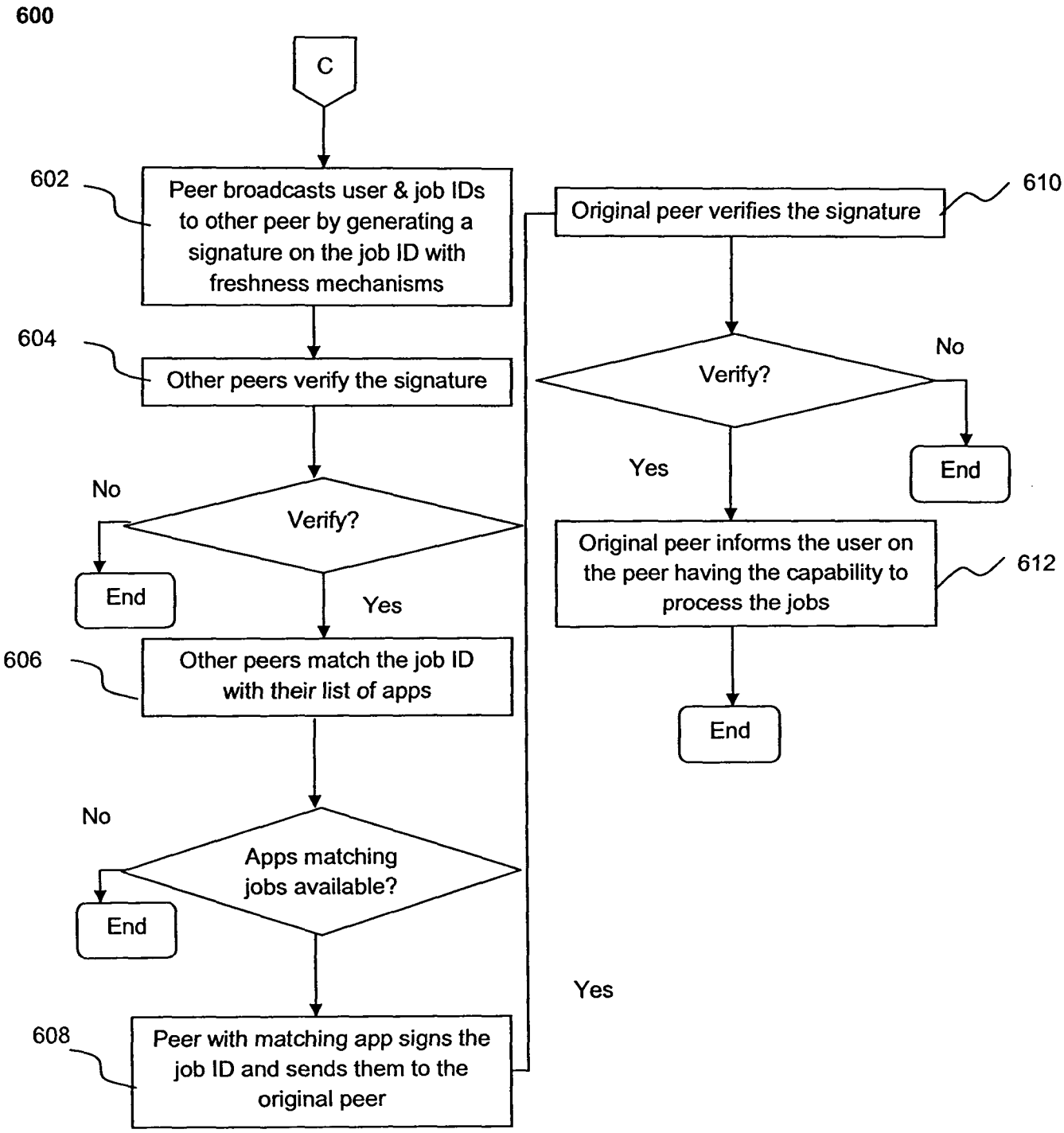

600
C
602
Peer broadcasts user & job IDs to other peer by generating a signature on the job ID with freshness mechanisms
604
Other peers verify the signature
No
Verify?
End
Yes
606
Other peers match the job ID with their list of apps
No
Apps matching jobs available?
End
Yes
608
Peer with matching app signs the job ID and sends them to the original peer
Original peer verifies the signature
610
No
Verify?
End
Yes
Original peer informs the user on the peer having the capability to process the jobs
612
End

FIG. 6.0

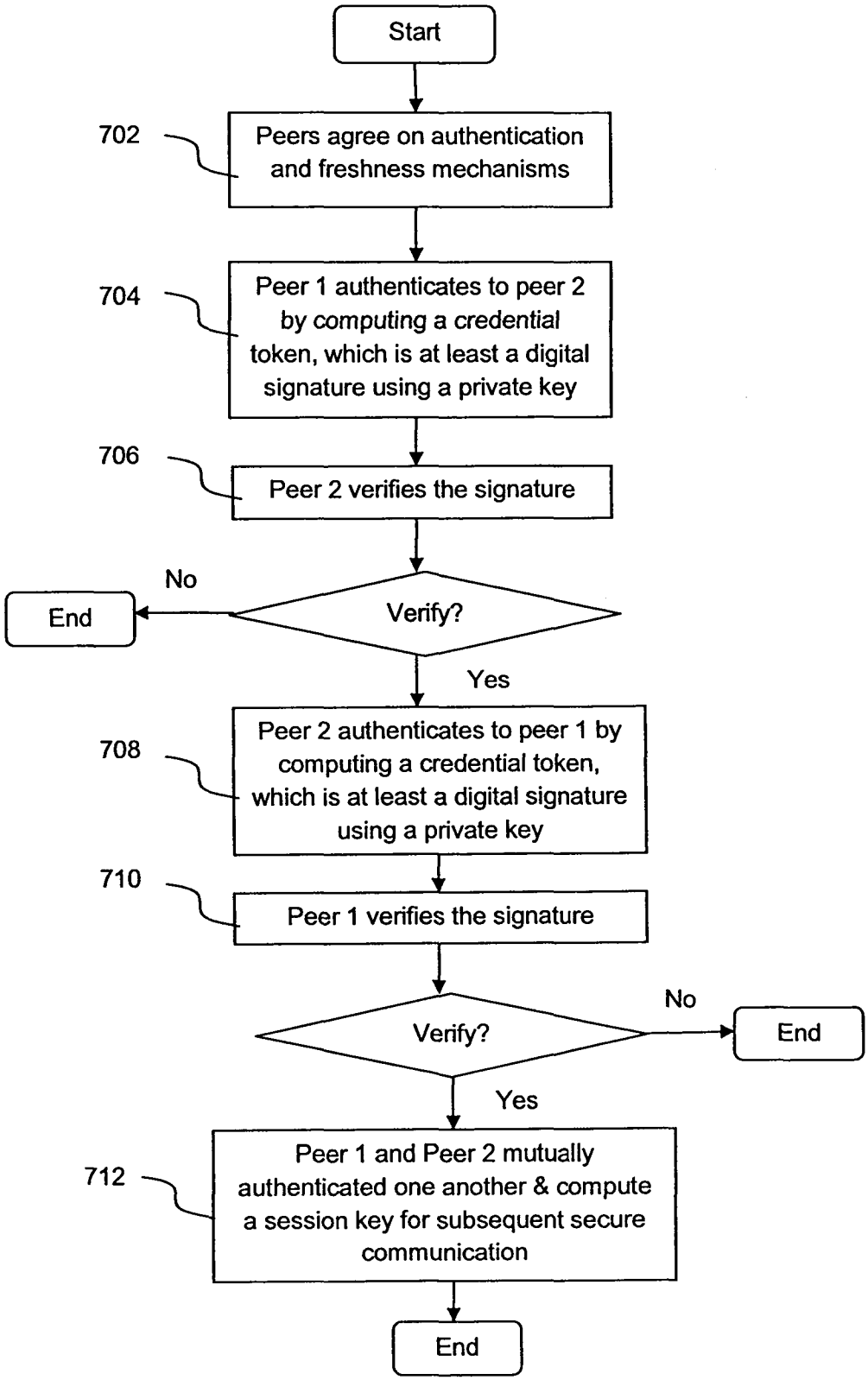

700
Start
702
Peers agree on authentication and freshness mechanisms
704
Peer 1 authenticates to peer 2 by computing a credential token, which is at least a digital signature using a private key
706
Peer 2 verifies the signature
Verify?
No
End
Yes
708
Peer 2 authenticates to peer 1 by computing a credential token, which is at least a digital signature using a private key
710
Peer 1 verifies the signature
Verify?
No
End
Yes
712
Peer 1 and Peer 2 mutually authenticated one another & compute a session key for subsequent secure communication
End

FIG. 7.0

INTERNATIONAL SEARCH REPORT

International application No
PCT/MY2013/000230

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W84/18 H04L29/06 H04L29/08 G06F9/50
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W 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 practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2008/313715 A1 (NARDONE MASSIMO [FI] ET AL) 18 December 2008 (2008-12-18) paragraphs [0025] - [0028], [0038] figures 2,4	1-6
A	EP 2 056 563 A1 (ALCATEL LUCENT [FR]) 6 May 2009 (2009-05-06) paragraphs [0008], [0015]; figure 1	1-6
A	US 2006/072148 A1 (KOVNAT LARRY A [US] ET AL) 6 April 2006 (2006-04-06) paragraph [0018]; figures 2,6	1-6

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 May 2014	21/05/2014

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	Pajatakis, Emmanouil

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/MY2013/000230

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008313715 A1	18-12-2008	US 2008313715 A1	18-12-2008
		US 2013007844 A1	03-01-2013
EP 2056563 A1	06-05-2009	CN 101431529 A	13-05-2009
		EP 2056563 A1	06-05-2009
		ES 2394107 T3	21-01-2013
		JP 5000763 B2	15-08-2012
		JP 2011503936 A	27-01-2011
		KR 20100057701 A	31-05-2010
		US 2009119747 A1	07-05-2009
		WO 2009059895 A1	14-05-2009
US 2006072148 A1	06-04-2006	NONE	