(12) STANDARD PATENT (11) Application No. **AU 2007240567 B2**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
Peer-to-peer contact exchange

(51) International Patent Classification(s)
G06F 15/16 (2006.01) ***H04L 9/30*** (2006.01)
G06F 17/00 (2006.01)

(21) Application No: **2007240567** (22) Date of Filing: **2007.04.23**

(87) WIPO No: **WO07/124180**

(30) Priority Data

(31) Number	(32) Date	(33) Country
11/408,894	**2006.04.21**	**US**

(43) Publication Date: **2007.11.01**
(44) Accepted Journal Date: **2011.07.21**

(71) Applicant(s)
Microsoft Corporation

(72) Inventor(s)
Sidhu, Gursharan S.;Singhal, Sandeep K.;Horton, Noah

(74) Agent / Attorney
Davies Collison Cave, 1 Nicholson Street, Melbourne, VIC, 3000

(56) Related Art
US 2005/0010794
US 6782103
US 6671804
EP 1473899
US 2001/0019609
US 2004/0064693

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 November 2007 (01.11.2007)

PCT

(10) International Publication Number
WO 2007/124180 A3

(51) International Patent Classification:
G06F 15/16 (2006.01) *H04L 9/30* (2006.01)
G06F 17/00 (2006.01)

(21) International Application Number:
PCT/US2007/010092

(22) International Filing Date: 23 April 2007 (23.04.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/408,894 21 April 2006 (21.04.2006) US

(71) Applicant *(for all designated States except US)*: **MICROSOFT CORPORATION** [US/US]; One Microsoft Way, Redmond, Washington 98052-6399 (US).

(72) Inventors: **SIDHU, Gursharan S.**; c/o Microsoft Corporation, International Patents, One Microsoft Way, Redmond, Washington 98052-6399 (US). **HORTON, Noah**; c/o Microsoft Corporation, International Patents, One Microsoft Way, Redmond, Washington 98052-6399 (US). **SINGHAL, Sandeep K.**; c/o Microsoft Corporation, International Patents, One Microsoft Way, Redmond, Washington 98052-6399 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, 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, 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, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

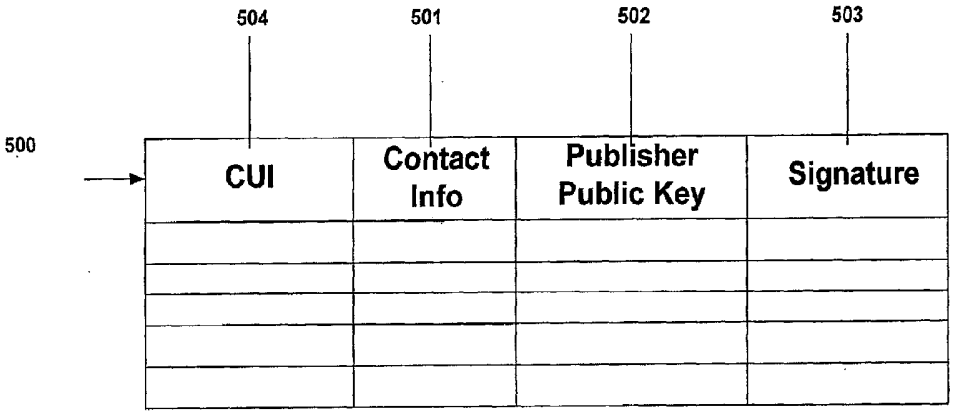
Declarations under Rule 4.17:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
13 December 2007

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: PEER-TO-PEER CONTACT EXCHANGE



(57) Abstract: A system may publish authenticated contact information in a publicly available index store, retrieve the contact information, and validate it. The claimed method and system may provide a client-based, server optional approach to publishing. The publicly available index store may be a distributed hash table used in a peer-to-peer network. The system may be used in other secure directory service applications where a server may not be available or where server trust may be minimal.

WO 2007/124180 A3

C:\NRPortbl\DCC\MKA\3654474_1.DOC-15/06/2011

2007240567 21 Jun 2011

PEER-TO-PEER CONTACT EXCHANGE

Background

[0001] Directory services may typically be provided using a network server. In order to utilize the directory services, a user may be required to connect to the server and have a user account in order to access the directory service. Additionally, the user may have to trust the server to provide data integrity and data authentication. If the directory service is intended for a smaller group of connected entities, for example an ad hoc network, then creating and setting up a directory server for that ad hoc network may be inefficient. For example, ad hoc networks may typically be transient in nature, and the cost of setting up a dedicated server for short durations and for a small number of users may be too costly, due to administrator time, equipment resource capacity (some server must be reallocated or added), and user time (user may be involved in account creation and setup). Moreover, while server based systems may be common, new serverless systems such as peer-to-peer networks, may provide greater flexibility in creating ad hoc networks because they may not require a dedicated server to facilitate communications. However, to enable secure communications over these ad hoc networks using existing encryption processes, a directory service may be required to facilitate public key exchange that does not rely on a server based model.

[0001A] It is desired, therefore, to provide a method of using a publicly available index store for a secure publication system, a computer system, or a memory storage device on a first node having computer-executable instructions for performing operations that alleviate one or more of the above difficulties, or at least provide a useful alternative.

Summary

[0001B] In accordance with the present invention, there is provided a method of using a publicly available index store for a secure publication system, the method comprising:

configuring a first computing device to be a publisher of contact information corresponding to the publisher, wherein:

the contact information is required to be known by both the publisher and another node to enable an initial establishment of a secure connection between the

2007240567 21 Jun 2011

another node and the publisher, and the contact information targeted for retrieval by only a user of the contact information;

the first computing device includes a first memory, a first processing unit, and first computer-executable instructions stored in the first memory and executable by the first processing unit to publish the contact information;

at the publisher:

providing a first cryptographically unique identifier that is statistically unique to a public key of the publisher;

obtaining a second cryptographically unique identifier that is statistically unique to a public key of the user of the contact information;

appending the second cryptographically unique identifier to the first cryptographically unique identifier to form a combination key;

creating a publisher signature by signing the contact information with a publisher private key;

creating a single record corresponding to the contact information, wherein the single record includes and is indexed by the combination key, and wherein the single record includes the publisher public key, the publisher signature, and all of the contact information corresponding to the publisher; and

inserting the record into a publicly available index store;

configuring a second computing device to be the user of the contact information, the second computing device including a second memory, a second processing unit, and second computer-executable instructions stored in the second memory and executable by the second processing unit to use the contact information to establish a secure connection with the publisher; and

at the user:

obtaining the first cryptographically unique identifier;

retrieving the single record from the publicly available index store based on the combination key;

determining whether the first cryptographically unique identifier relates to the publisher public key included in the single record;

2007240567 21 Jun 2011

determining whether the contact information is signed by a private key corresponding to the publisher public key included in the single record;

establishing the secure connection with the publisher using at least a portion of the single record upon determining the first cryptographically unique identifier relates to the publisher public key included in the single record and the contact information is signed by the private key corresponding to the publisher public key included in the single record; and

refusing to establish the secure connection with the publisher upon determining the first cryptographically unique identifier does not relate to the publisher public key included in the single record or the contact information is not signed by the private key corresponding to the publisher public key included in the single record,

wherein the publisher and the user are different nodes in a peer-to-peer network.

[0001C] The present invention also provides a computer system comprising:

a plurality of peer nodes forming a peer-to-peer network;

a distributed hash table of the peer-to-peer network;

a first peer node from the plurality of peer nodes, the first peer node configured to:

publish contact information corresponding to the first peer node wherein the contact information is required to be known by both the first peer node and a second peer node from the plurality of peer nodes to enable an initial establishment of a secure connection between the first peer node and the second peer node, and the contact information targeted for retrieval by only the second peer node,

create a first cryptographically unique identifier that is statistically unique to a public key of the first peer node,

create a signature by signing the contact information with a private key of the first peer node,

obtain a second cryptographically unique identifier that is statistically unique to a public key of the second peer node,

append the second cryptographically unique identifier to the first cryptographically unique identifier to form a combination key,

2007240567 21 Jun 2011

create a single record corresponding to the contact information, wherein the single record includes and is indexed by the combination key, and wherein the single record includes the public key of the first peer node, the signature, and all of the contact information corresponding to the first peer node; and

insert the single record into the distributed hash table; and

the second peer node from the plurality of peer nodes, the second peer node configured to:

obtain the first cryptographically unique identifier;

retrieve the single record from the distributed hash table based on the combination key,

determine whether the first cryptographically unique identifier relates to the public key of the first peer node included in the single record,

determine whether the contact information is signed by a private key corresponding to the public key of the first peer node included in the single record,

determine whether the contact information has an expected format and syntax,

establish a secure connection with the first peer node using at least a portion of the single record upon determining:

the -first cryptographically unique identifier relates to the public key of the first peer node included in the single record,

the contact information is signed by the private key corresponding to the public key of the first peer node included in the single record, and

the contact information has the expected format and syntax; and

refuse to establish the secure connection with the first peer node upon determining:

the-first cryptographically unique identifier does not relate to the public key of the first peer node included in the single record,

the contact information is not signed by the private key corresponding to the public key of the first peer node included in the single record, or

the contact information has an unexpected format or syntax.

2007240567 21 Jun 2011

[0001D] The present invention also provides a memory storage device on a first node having computer-executable instructions for performing operations comprising:

receiving a second cryptographically unique identifier corresponding to a second node;

retrieving an entry from an index store based on a combination key, the combination key including a first cryptographically unique identifier corresponding to the first node appended to the second cryptographically unique identifier corresponding to the second node, wherein:

the entry contains a complete set of contact information corresponding to the second node and a public key corresponding to the second node;

the entry further contains the combination key and is indexed by the combination key;-

the complete set of contact information is required to be known by both the first node and the second node to enable an initial establishment of a secure connection between the first node and the second node;

the complete set of contact information and the public key corresponding to the second node are together signed by a private key corresponding to the public key corresponding to the second node; and

the entry was previously entered into the index store by the second node;

determining whether the second cryptographically unique identifier relates to the public key corresponding to the second node;

determining whether the complete set of contact information and the public key corresponding to the second node are signed by the private key corresponding to the second node;

establishing the secure connection between the first node and the second node using at least a portion of the entry upon determining the second cryptographically unique identifier relates to the public key corresponding to the second node included in the entry and the contact information is signed by the private key corresponding to the public key corresponding to the second node included in the entry; and

refusing to establish the secure connection between the first and the second node upon determining the second cryptographically unique identifier does not relate to the

2007240567 21 Jun 2011

public key corresponding to the second node included in the entry or the contact information is not signed by the private key corresponding to the public key corresponding to the second node included in the entry,

wherein the first node and the second node are different nodes in a peer-to-peer network.

[0002] In accordance with some embodiments of the present invention, a system may publish authenticated contact information in a publicly available index store. The system may also provide a method of retrieving the contact information and validating it. The method and system may be client based, with a server being optional. The publicly available index store may be a distributed hash table used in a peer-to-peer network. The system may be used in other secure directory service applications where a server may not be available or where server trust may be minimal.

[0003] In one embodiment, the system may be used as a general message publishing system. In another embodiment, the system may be used to provide selective publication in which a posted record may only be retrieved and read by an intended recipient.

Drawings

[0003A] Some embodiments of the present invention are hereinafter described, by way of example only, with reference to the accompanying drawings, wherein:

[0004] Figure 1 illustrates a block diagram of a computing system that may operate in accordance with some embodiments of the present invention;

[0005] Figure 2 illustrates a general peer-to-peer network;

[0006] Figure 3 illustrates a general director server and service;

[0007] Figure 4 illustrates a distributed hash table;

[0008] Figure 5 illustrates a record used in an embodiment of the present invention;

[0009] Figure 6 illustrates a publishing process embodiment;

[0010] Figure 7 illustrates a retrieval process embodiment;

[0011] Figure 8 illustrates a modified record containing a duration parameter;

2007240567 21 Jun 2011

[0012] Figure 9 illustrates an another validation process using a duration parameter;

[0013] Figure 10 illustrates a modified record for selective publication;

[0014] Figure 11 illustrates a publishing process embodiment for selective publication; and

[0015] Figure 12 illustrates a retrieval process embodiment for selective publication.

Description

[0016] Although the following text sets forth a detailed description of numerous different embodiments, the detailed description is to be construed as exemplary only and does not describe every possible embodiment since describing every possible embodiment would be impractical, if not impossible. Numerous alternative embodiments could be implemented, using either current technology or technology developed after the filing date of this patent, which would still fall within the scope of the claims.

[0017] It should also be understood that, unless a term is expressly defined in this patent using the sentence "As used herein, the term '_____' is hereby defined to mean..." or a similar sentence, there is no intent to limit the meaning of that term, either expressly or by implication, beyond its plain or ordinary meaning, and such term should not be interpreted to be limited in scope based on any statement made in any section of this patent (other than the language of the claims). To the extent that any term recited in the claims at the end of this patent is referred to in this patent in a manner consistent with a single meaning, that is done for sake of clarity only so as to not confuse the reader, and it is not intended that such claim term be limited, by implication or otherwise, to that single meaning.

[0018] Figure 1 illustrates an example of a suitable computing system environment 100 on which a system for the claimed method and apparatus may be implemented. The computing system environment 100 is only one example of a suitable computing environment and is not intended to suggest any limitation as to the scope of use or functionality of the method and apparatus of the claims. Neither should the computing environment 100 be interpreted as having any dependency or requirement relating to any

2007240567 21 Jun 2011

one component or combination of components illustrated in the exemplary operating environment 100.

[0019] The method and apparatus are operational with numerous other general purpose or special purpose computing system environments or configurations. Examples of well known computing systems, environments, and/or configurations that may be suitable for use with the methods or apparatus of the claims include, but are not limited to, personal computers, server computers, hand-held or laptop devices, multiprocessor systems, microprocessor-based systems, set top boxes, programmable consumer electronics, network PCs, minicomputers, mainframe computers, distributed computing environments that include any of the above systems or devices, and the like.

[0020] The method and apparatus may be described in the general context of computer-executable instructions, such as program modules, being executed by a computer. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. The methods and apparatus may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote computer storage media including memory storage devices.

[0021] With reference to Figure 1, an exemplary system for implementing the claimed method and apparatus includes a general purpose computing device in the form of a computer 110. Components of computer 110 may include, but are not limited to, a processing unit 120, a system memory 130, and a system bus 121 that couples various system components including the system memory to the processing unit 120. The system bus 121 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. By way of example, and not limitation, such architectures include Industry Standard Architecture (ISA) bus, Micro Channel Architecture (MCA) bus, Enhanced ISA (EISA) bus, Video Electronics Standards Association (VESA) local bus, and Peripheral Component Interconnect (PCI) bus also known as Mezzanine bus.

2007240567 21 Jun 2011

[0022] Computer 110 typically includes a variety of computer readable media. Computer readable media may be any available media that may be accessed by computer 110 and includes both volatile and nonvolatile media, removable and non-removable media. By way of example, and not limitation, computer readable media may comprise computer storage media and communication media. Computer storage media includes both volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules or other data. Computer storage media includes, but is not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical disk storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which may be used to store the desired information and which may accessed by computer 110. Communication media typically embodies computer readable instructions, data structures, program modules or other data in a modulated data signal such as a carrier wave or other transport mechanism and includes any information delivery media. The term "modulated data signal" means a signal that has one or more of its characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media includes wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, RF, infrared and other wireless media. Combinations of the any of the above should also be included within the scope of computer readable media.

[0023] The system memory 130 includes computer storage media in the form of volatile and/or nonvolatile memory such as read only memory (ROM) 131 and random access memory (RAM) 132. A basic input/output system 133 (BIOS), containing the basic routines that help to transfer information between elements within computer 110, such as during start-up, is typically stored in ROM 131. RAM 132 typically contains data and/or program modules that are immediately accessible to and/or presently being operated on by processing unit 120. By way of example, and not limitation, Figure 1 illustrates operating system 134, application programs 135, other program modules 136, and program data 137.

[0024] The computer 110 may also include other removable/non-removable, volatile/nonvolatile computer storage media. By way of example only, Figure 1 illustrates a hard disk drive 140 that reads from or writes to non-removable, nonvolatile magnetic media, a magnetic disk drive 151 that reads from or writes to a removable, nonvolatile magnetic disk 152, and an optical disk drive 155 that reads from or writes to a removable, nonvolatile optical disk 156 such as a CD ROM or other optical media. Other removable/non-removable, volatile/nonvolatile computer storage media that may be used in the exemplary operating environment include, but are not limited to, magnetic tape cassettes, flash memory cards, digital versatile disks, digital video tape, solid state RAM, solid state ROM, and the like. The hard disk drive 141 is typically connected to the system bus 121 through a non-removable memory interface such as interface 140, and magnetic disk drive 151 and optical disk drive 155 are typically connected to the system bus 121 by a removable memory interface, such as interface 150.

[0025] The drives and their associated computer storage media discussed above and illustrated in Figure 1, provide storage of computer readable instructions, data structures, program modules and other data for the computer 110. In Figure 1, for example, hard disk drive 141 is illustrated as storing operating system 144, application programs 145, other program modules 146, and program data 147. Note that these components may either be the same as or different from operating system 134, application programs 135, other program modules 136, and program data 137. Operating system 144, application programs 145, other program modules 146, and program data 147 are given different numbers here to illustrate that, at a minimum, they are different copies. A user may enter commands and information into the computer 20 through input devices such as a keyboard 162 and pointing device 161, commonly referred to as a mouse, trackball or touch pad. Other input devices (not

illustrated) may include a microphone, joystick, game pad, satellite dish, scanner, or the like. These and other input devices are often connected to the processing unit 120 through a user input interface 160 that is coupled to the system bus, but may be connected by other interface and bus structures, such as a parallel port, game port or a universal serial bus (USB). A monitor 191 or other type of display device is also connected to the system bus 121 via an interface, such as a video interface 190. In addition to the monitor, computers may also include other peripheral output devices such as speakers 197 and printer 196, which may be connected through an output peripheral interface 190.

[0026] The computer 110 may operate in a networked environment using logical connections to one or more remote computers, such as a remote computer 180. The remote computer 180 may be a personal computer, a server, a router, a network PC, a peer device or other common network node, and typically includes many or all of the elements described above relative to the computer 110, although only a memory storage device 181 has been illustrated in Figure 1. The logical connections depicted in Figure 1 include a local area network (LAN) 171 and a wide area network (WAN) 173, but may also include other networks. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets and the Internet.

[0027] When used in a LAN networking environment, the computer 110 is connected to the LAN 171 through a network interface or adapter 170. When used in a WAN networking environment, the computer 110 typically includes a modem 172 or other means for establishing communications over the WAN 173, such as the Internet. The modem 172, which may be internal or external, may be connected to the system bus 121 via the user input interface 160, or other appropriate mechanism. In a networked environment, program modules depicted relative to the computer 110, or portions thereof, may be stored in the remote memory storage device. By way of example, and not limitation, Figure 1 illustrates remote application programs 185 as residing on memory device 181. It will be appreciated that the network connections illustrated are exemplary and other means of establishing a communications link between the computers may be used.

[0028] Peer-to-peer (P2P) systems employ a network of nodes that communicate with each other in a decentralized manner, e.g., without the aid of a central server. Each node (e.g., an application or a device) in the peer-to-peer network may communicate with another node on

the network through a direct connection, or each node may communicate indirectly using one or more intermediate nodes to relay communications to an intended node.

[0029] Figure 2 illustrates a high-level depiction of a P2P system 200. The system 200 includes a collection of peer entities (202-212). The peer entities (202-212) may be personal computer devices that are coupled together via a network or combination of networks. Figure 2 illustrates an example in which each peer entity (202-212) is connected to all other peer entities (202-212). In other cases, one or more peer entities (202-212) may be connected to other peer entities (202-212) via one or more intermediary participants (202-212). However, in order to provide secure communication on a peer-to-peer network, secure connections between peer nodes may first need to be established.

[0030] Connection security may be based on a symmetric key encryption process, as may be commonly known in the art. In order to implement this encryption security, however, peer entities may need to first exchange certificates and/or public keys which enable a secure connection to be initially established. In some existing systems, such as that illustrated in Figure 3, this exchange may be facilitated using a central directory server 300 where users 301, 302, 303 may post their certificates 304, 305, 306 and/or public keys on the directory server 300. A directory service 307 may be a database table containing records 308 of certificates and/or public keys indexed under a username or other identifier used as a key 309. A user capable of connecting to the directory server 300 and allowed access to the directory service 307 may lookup a target user using the target user's identifier, and obtain the target user's corresponding public key. This approach may require connectivity to the server 300, explicit signup with the directory server 300, and trust in the directory server 300. Furthermore, someone must incur the cost of hosting such as server. When a user 303 is connecting from a remote location, Internet connectivity 310 may additionally be required. The server signup process may involve user accounts that are used to promote trust in the directory server 300. For example, if any user could access the server 300, the server 300 may be viewed as more susceptible to compromise, especially if security information is being posted and exchanged, such as public keys. Further, creating a directory server for an ad hoc, temporary network may be impractical because of the transient nature of these networks and the difficulty in setting up a directory server. A possible workaround for an ad hoc peer-to-peer network may be to exchange public keys via email or via an off network process, such as physically sending or mailing a diskette containing a certificate/public key to a target

2007240567 21 Jun 2011

member. This may enable the peer entities to establish server independent, secure links. However, this may be cumbersome and error-prone.

[0031] The server-independent indexing process may use a serverless index store, such as a distributed hash table (DHT) 400 illustrated in Figure 4. This distributed hash table 400 may be maintained over a group of peer entities 401-404 that form a peer-to-peer network 405. The entries in a distributed hash table may be logically divided or grouped using, for example, a hash function. The hash function may clump records together in some organized manner, thereby making retrieval more efficient. A DHT may have two primary properties: 1) distribution of a table (e.g., table 400), across a plurality of nodes (e.g., nodes 401-404); and 2) a routing mechanism (not shown) that provides a method for publishing and retrieving records. The routing mechanism and distribution may be managed by an overlay protocol such as Chord, PNRP, Pastry, Tapestry, etc. While a DHT may be used to provide an index store in accordance with an embodiment of the claims, it is emphasized that any index store which may be easily accessed by a group of peer entities may be used, including server-based indices. In the case of a server-based indices, the claimed system may reduce the level of trust required from the server alone because the claimed system may provide the necessary level of security for an unsecured index store.

[0032] The server-independent indexing process may use a particular record format, as illustrated in Figure 5. Figure 5, illustrates that a publisher may post to the index store a record 500 containing contact information 501, the publisher's public key 502 and a signature 503 of the contact information using the publisher's private key. Alternatively, the signature may be for a combination of the contact information and public key. This record may be indexed by a record key 504. In one embodiment, the key 504 of the record may be a cryptographically unique identifier (CUI). A CUI may have two primary properties. First, the CUI may be statistically unique and second, the CUI may correspond to a particular user public key, such as the publisher public key 502. Similar to common database indexing schemes, a record key may need to be unique to prevent duplicate entity entries. Accordingly, a CUI may be one that is derived such that there is a high probability that it is unique for a particular situation or application. For example, in a peer group of only a few members, the CUI may be statistically unique if the probability that a cryptographically unique identifier may be derived from the same member public key is unlikely for the group size.

[0033] The CUI may be derived from a public key using an algorithm, such as a hash or encryption algorithm. The CUI may be verified to correspond or match with its public key using the algorithm. In one embodiment, the CUI may be used to represent a longer user identifier, such as a public key, in a shorter more user manageable form such as the peer names used in a P2P system described in U.S. Patent Application No. 10/882079, entitled "Callsigns."

[0034] The record of Figure 5 may be used to publish contact information to an index store, such as the DHT 400 of Figure 4. The CUI key 504 may be used to locate each record 500 and retrieve the contact information 501 and public key 502. In this embodiment, the published information may be public, i.e., the published information may not be encrypted, except for the signatures. However, other embodiments described below may encrypt portions of the published information. Also, while this embodiment illustrates using a record 500 to facilitate public key 502 exchange, it is emphasized that the system may be used in any application in which a unique message publication may be used. For example, instead of contact information 501, any message may be posted against a user CUI 504.

[0035] Figure 6 illustrates a general publishing process in accordance with an embodiment of the claims. Using an algorithm such as a hash function, a CUI may be generated for a given user's public key 601. It is important to note that whatever algorithm may be used, that the CUI may be verified to correspond to the public key that was used to generate it. A record of the contact information, or other message data, and publisher's public key may be constructed 602 and the contact information and/or publisher's public key may be signed by the publisher's private key 603 (which may correspond to the public key). The record, including the contact information, the public key and the signature may be inserted 604 into a publicly available index. The record may be indexed by the CUI corresponding to the publisher public key.

[0036] Figure 7 illustrates a retrieval process in accordance with an embodiment of the claims. A user desiring to connect with a second peer may obtain the CUI of the second peer 701. The CUI may be obtained out of band either through email or off network process (e.g., snail mail, verbal communication, business card, etc.). The CUI may then be used to lookup up a record mapped to the CUI in the index store 702. As discussed above, a record may include a key, some message information (contact information), and a signature.

[0037] The user may then query the index store to retrieve a record based on the CUI 703. Once the CUI is retrieved, the CUI may be verified using the public key contained in the record to ensure that they correspond to each other 704. This process block may be used to verify that the record corresponds to the CUI. The CUI may be made statistically unique to the public key in any number of ways. In one embodiment, the peer communication system may pre-establish a common mapping process, for example using a recognized hash function. This initial verification process helps to ensure that the record may indeed correspond to the given CUI.

[0038] If the CUI maps properly, then the signature of the record may then be used to determine whether the signature is signed by a corresponding private key of the publisher 705. This may authenticate the message by providing evidence that the message originated from the publisher, as it may be assumed that the publisher owns the private key corresponding to the public key used for the encryption.

[0039] If the record/message is properly signed, a message format and/or syntax check 706 may then be performed on the contact information of the record. This may be used, for example, to ensure that the message was not hacked to match the signature. While providing a hacked message to match an encrypted signature may be statistically difficult, it may not be impossible. Hacking, however, may result in a message that does not conform to intended or expected format. Thus, a first check of the message may be made to determine whether the message format complies with an expected format. For example, where contact information is communicated, the contact information may require a ten character format. If the record format does not provide this ten character format, then someone or something may have tampered with the message 711.

[0040] Alternatively, or in addition, the semantics of the message may be checked. For example, the contact information may be limited to a list of options and specific relations between those options. Therefore, if the format requires two entries, and the first entry is related to the second entry (semantics) and they do not match this expected format, then someone or something may have tampered with the message 711.

[0041] If all of the verifications processes 704, 705, 706 have been completed successfully, then the record may be authentic and subsequently used 707, for example, the public key may be used to establish communication links. If any of the verification steps 704,705, 706 fails,

then someone or something may have been tampered with the message 711. In the case of a public key exchange system, a connection may be refused.

[0042] In another embodiment illustrated in Figure 8, a duration parameter 801 may be included with the record 800. This duration parameter 801 may correspond to a level of encryption used in the authentication process described. For example, the encryption level may correspond to the strength of the encryption used to generate the public/private key pairs used in the claimed system. If the encryption strength is high, then the duration may be long and vice versa. The duration parameter 801 may indicate a duration of validity for the record. Thus, the duration parameter 801 may be used in the retrieval process as illustrated in Figure 9. Figure 9 illustrates the same process of Figure 7, with the addition of block 909, where the duration 901 indicated by the duration parameter 801 is checked to determine whether the duration has expired. If the duration parameter 801 is expired, then the record may be compromised 911. Otherwise the record may be valid 907.

[0043] Figures 10-12 illustrates another embodiment where selective publication may be used to allow a first user to publish data that only a targeted second user may retrieve. In this selective publication embodiment, a record 1001, as illustrated in Figure 10, may be used. The record 1001 may include a key 1002 that is formed from the combination of two CUIs 1003, 1004. The first CUI 1003 may be associated with a first user while the second CUI 1004 may be associated with a second user. The combination may be formed by simply appending the second CUI to the first CUI. This record may include a message portion 1005 and a duration parameter 1006. The message 1005 may contain data on a publisher's contact information, publisher public key, and a signature.

[0044] Figure 11 illustrates a selective publishing process using the record 1001 of Figure 10. A publisher could derive his CUI from a public key 1101, obtain a CUI of a selected recipient 1102, construct the message 1103, sign the message using the publisher's private key 1104 and insert the message into an index based 1105 on the CUI combination key 1101. Additionally, the message may be encrypted 1106 using the intended recipient's public key.

[0045] Figure 12 illustrates a retrieval process for a selective publication process that is similar to Figure 7 with the addition of blocks 1201, 1202, 1203. A recipient wishing to retrieve a published record may first obtain the CUI of the publisher 1201 and then lookup a record in the index store under the combined CUI key 1202. In a further enhanced embodiment, the message may be encrypted using a public key of the recipient. Thus, only

the recipient may decrypt the intended data. After the recipient retrieves the message using the CUI combination key 1202, the recipient may use its private key to first decrypt the record 1203, after which the process of verification and validation follows that of Figure 7. In this selective publication embodiment, the recipient's public key (used to encrypt the record) may be determined from the recipient CUI, which the publisher used to create the combination key.

[0046] In another enhancement of the above embodiment, the key may be a group public key, which is owned by a group of peers. In this embodiment, any member of the group may lookup a record under the group public key and perform the authentication process. The group of users may have access to the record and may be specifically targeted for receipt of a posted message.

[0047] It should be emphasized that while the specific embodiments described above may be associated with a public key exchange directory, the contact information may represent other data. For example, instead of contact information, the record may be a generic message posting. Thus, the claimed system may be used as a general publication system over any publicly accessible index store. The claimed system may also be used to provide directory services other than public key lookup. The claimed system enables existing distributed index stores, such as distributed hash tables, to function as secured directory services work without relying on a server.

[0048] Additionally, the claimed system may be used on existing server based directories where the server security may be minimal, thereby requiring the authentication process provided by the claimed system. In ad hoc systems such as peer groups and peer-to-peer networks, a serverless process of public key publication and retrieval may make the creation of such networks more efficient by reducing the need for a hosted, dedicated server to provide the directory service. The claimed method and system may also minimize user involvement because the public/private key encryption process may eliminate the need for a user to explicitly sign on to a server.

2007240567 21 Jun 2011

[0049] Throughout this specification and claims which follow, unless the context requires otherwise, the word "comprise", and variations such as "comprises" and "comprising", will be understood to imply the inclusion of a stated integer or step or group of integers or steps but not the exclusion of any other integer or step or group of integers or steps.

[0050] The reference in this specification to any prior publication (or information derived from it), or to any matter which is known, is not, and should not be taken as an acknowledgment or admission or any form of suggestion that that prior publication (or information derived from it) or known matter forms part of the common general knowledge in the field of endeavour to which this specification relates.

2007240567 21 Jun 2011

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A method of using a publicly available index store for a secure publication system, the method comprising:

configuring a first computing device to be a publisher of contact information corresponding to the publisher, wherein:

the contact information is required to be known by both the publisher and another node to enable an initial establishment of a secure connection between the another node and the publisher, and the contact information targeted for retrieval by only a user of the contact information;

the first computing device includes a first memory, a first processing unit, and first computer-executable instructions stored in the first memory and executable by the first processing unit to publish the contact information;

at the publisher:

providing a first cryptographically unique identifier that is statistically unique to a public key of the publisher;

obtaining a second cryptographically unique identifier that is statistically unique to a public key of the user of the contact information;

appending the second cryptographically unique identifier to the first cryptographically unique identifier to form a combination key;

creating a publisher signature by signing the contact information with a publisher private key;

creating a single record corresponding to the contact information, wherein the single record includes and is indexed by the combination key, and wherein the single record includes the publisher public key, the publisher signature, and all of the contact information corresponding to the publisher; and

inserting the record into a publicly available index store;

configuring a second computing device to be the user of the contact information, the second computing device including a second memory, a second processing unit, and second computer-executable instructions stored in the second memory and executable by

2007240567 21 Jun 2011

the second processing unit to use the contact information to establish a secure connection with the publisher; and

at the user:

obtaining the first cryptographically unique identifier;

retrieving the single record from the publicly available index store based on the combination key;

determining whether the first cryptographically unique identifier relates to the publisher public key included in the single record;

determining whether the contact information is signed by a private key corresponding to the publisher public key included in the single record;

establishing the secure connection with the publisher using at least a portion of the single record upon determining the first cryptographically unique identifier relates to the publisher public key included in the single record and the contact information is signed by the private key corresponding to the publisher public key included in the single record; and

refusing to establish the secure connection with the publisher upon determining the first cryptographically unique identifier does not relate to the publisher public key included in the single record or the contact information is not signed by the private key corresponding to the publisher public key included in the single record,

wherein the publisher and the user are different nodes in a peer-to-peer network.

2. The method of claim 1, further comprising:

determining, by the second computing device, whether the contact information has an expected format and syntax;

establishing the secure connection with the publisher using the at least the portion of the single record upon determining the contact information is determined to have the expected format and syntax; and

refusing to establish the secure connection with the publisher upon determining the contact information has an unexpected format or syntax.

2007240567 21 Jun 2011

3. The method of claim 1 or 2, wherein the index store is one of a distributed hash table and a directory server.

4. The method of any one of claims 1 to 3, wherein the first cryptographically unique identifier is derived from the public key of the user using a hash function.

5. The method of any one of claims 1 to 4, wherein the single record further includes a duration parameter that is proportional to an encryption strength.

6. The method of claim 5, further comprising at the second computing device:

establishing the secure connection with the publisher using the at least the portion of the single record upon determining that a duration indicated by the duration parameter has not expired; and

refusing to establish the secure connection with the publisher upon determining that the duration indicated by the duration parameter has expired.

7. The method of any one of claims 1 to 6, wherein the first cryptographically unique identifier comprises a group public key.

8. The method of any one of claims 1 to 7, wherein establishing the secure connection with the publisher using the at least the portion of the single record comprises establishing the secure connection with the publisher using the publisher public key included in the single record.

9. The method of any one of claims 1 to 8, further comprising:

at the publisher, encrypting the contact information using the public key of the user; and

at the user, decrypting the contact information using a private key of the user.

10. A method of using a publicly available index store for a secure publication system, substantially as hereinbefore described with reference to the accompanying drawings.

2007240567 21 Jun 2011

11. A memory storage device on a first node having computer-executable instructions for performing the method of any one of claims 1 to 10.

12. A computer system comprising:

a plurality of peer nodes forming a peer-to-peer network;

a distributed hash table of the peer-to-peer network;

a first peer node from the plurality of peer nodes, the first peer node configured to:

publish contact information corresponding to the first peer node wherein the contact information is required to be known by both the first peer node and a second peer node from the plurality of peer nodes to enable an initial establishment of a secure connection between the first peer node and the second peer node, and the contact information targeted for retrieval by only the second peer node,

create a first cryptographically unique identifier that is statistically unique to a public key of the first peer node,

create a signature by signing the contact information with a private key of the first peer node,

obtain a second cryptographically unique identifier that is statistically unique to a public key of the second peer node,

append the second cryptographically unique identifier to the first cryptographically unique identifier to form a combination key,

create a single record corresponding to the contact information, wherein the single record includes and is indexed by the combination key, and wherein the single record includes the public key of the first peer node, the signature, and all of the contact information corresponding to the first peer node; and

insert the single record into the distributed hash table; and

the second peer node from the plurality of peer nodes, the second peer node configured to:

obtain the first cryptographically unique identifier;

retrieve the single record from the distributed hash table based on the combination key,

2007240567 21 Jun 2011

determine whether the first cryptographically unique identifier relates to the public key of the first peer node included in the single record,

determine whether the contact information is signed by a private key corresponding to the public key of the first peer node included in the single record,

determine whether the contact information has an expected format and syntax,

establish a secure connection with the first peer node using at least a portion of the single record upon determining:

the -first cryptographically unique identifier relates to the public key of the first peer node included in the single record,

the contact information is signed by the private key corresponding to the public key of the first peer node included in the single record, and

the contact information has the expected format and syntax; and

refuse to establish the secure connection with the first peer node upon determining:

the-first cryptographically unique identifier does not relate to the public key of the first peer node included in the single record,

the contact information is not signed by the private key corresponding to the public key of the first peer node included in the single record, or

the contact information has an unexpected format or syntax.

13. The system of claim 12, wherein the contact information is encrypted using a public key of the second peer node and the contact information is decrypted using a private key of the second peer node.

14. The system of claim 12 or 13, wherein the single record further includes a duration parameter, wherein the duration parameter is proportional to the strength of an encryption algorithm used to generate the public key of the first peer node and the private key corresponding to the public key of the first peer node.

2007240567 21 Jun 2011

15. The system of claim 14, wherein the second peer node is configured to:

establish the secure connection with the first peer node using the at least the portion of the single record upon determining that a duration indicated by the duration parameter has not expired; and

refuse to establish the secure connection with the first peer node upon determining that the duration indicated by the duration parameter has expired.

16. A memory storage device on a first node having computer-executable instructions for performing operations comprising:

receiving a second cryptographically unique identifier corresponding to a second node;

retrieving an entry from an index store based on a combination key, the combination key including a first cryptographically unique identifier corresponding to the first node appended to the second cryptographically unique identifier corresponding to the second node, wherein:

the entry contains a complete set of contact information corresponding to the second node and a public key corresponding to the second node;

the entry further contains the combination key and is indexed by the combination key;

the complete set of contact information is required to be known by both the first node and the second node to enable an initial establishment of a secure connection between the first node and the second node;

the complete set of contact information and the public key corresponding to the second node are together signed by a private key corresponding to the public key corresponding to the second node; and

the entry was previously entered into the index store by the second node;

determining whether the second cryptographically unique identifier relates to the public key corresponding to the second node;

2007240567 21 Jun 2011

determining whether the complete set of contact information and the public key corresponding to the second node are signed by the private key corresponding to the second node;

establishing the secure connection between the first node and the second node using at least a portion of the entry upon determining the second cryptographically unique identifier relates to the public key corresponding to the second node included in the entry and the contact information is signed by the private key corresponding to the public key corresponding to the second node included in the entry; and

refusing to establish the secure connection between the first and the second node upon determining the second cryptographically unique identifier does not relate to the public key corresponding to the second node included in the entry or the contact information is not signed by the private key corresponding to the public key corresponding to the second node included in the entry,

wherein the first node and the second node are different nodes in a peer-to-peer network.

17. The memory storage device of claim 16, further comprising:

determining whether the complete set of contact information has an expected format and syntax;

establishing the secure connection between the first node and the second node using the at least the portion of the single record upon determining the complete set of contact information has the expected format and syntax; and

refusing to establish the secure connection between the first node and the second node upon determining the complete set of contact information has an unexpected format or syntax.

18. The memory storage device of claim 16 or 17, further comprising determining whether a duration parameter of the entry has expired.

19. The memory storage device of claim 18, wherein a duration indicated by the duration parameter is proportional to a level of encryption used to generate the public key

2007240567 21 Jun 2011

corresponding to the second node included in the entry and the private key corresponding to the second node.

20. The memory storage device of any one of claims 16 to 19, wherein the complete set of contact information is encrypted using a public key of a computer associated with the second cryptographically unique identifier, and wherein the complete set of contact information is decrypted using a private key corresponding to the first node.

21. The system of any one of claims 12 to 20, wherein the second peer node establishes the secure connection with the first peer node using the public key of the first peer node included in the single record.

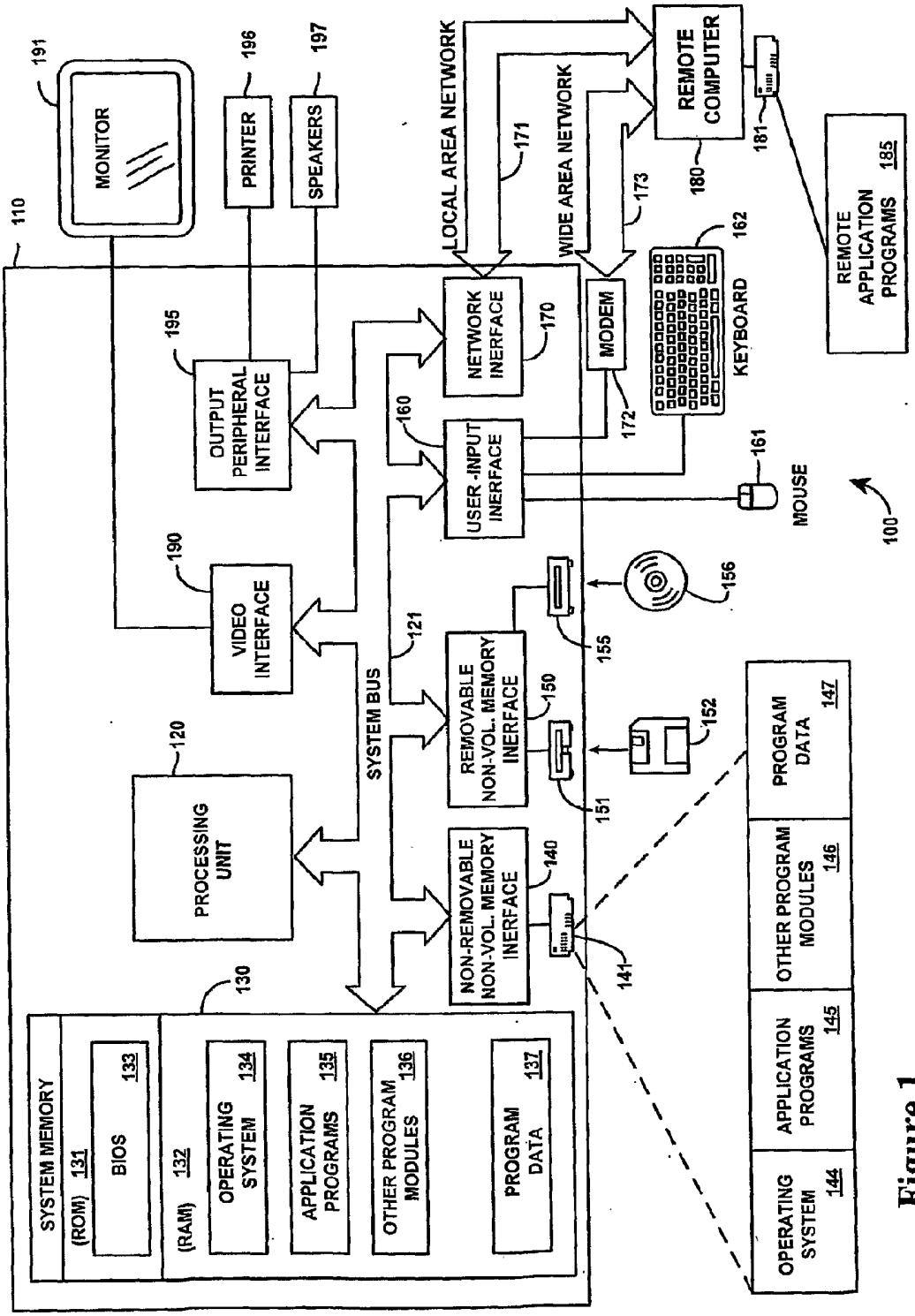

MONITOR
191
PRINTER
196
SPEAKERS
197
110
LOCAL AREA NETWORK
171
WIDE AREA NETWORK
173
REMOTE COMPUTER
180
181
REMOTE APPLICATION PROGRAMS 185
KEYBOARD
162
MODEM
172
NETWORK INERFACE
170
OUTPUT PERIPHERAL INTERFACE
195
USER -INPUT INERFACE
160
MOUSE
161
100
VIDEO INTERFACE
190
156
155
SYSTEM BUS
121
REMOVABLE NON-VOL. MEMORY INERFACE
150
152
151
PROCESSING UNIT
120
NON-REMOVABLE NON-VOL. MEMORY INERFACE
140
141
PROGRAM DATA
147
OTHER PROGRAM MODULES
146
APPLICATION PROGRAMS
145
OPERATING SYSTEM
144
SYSTEM MEMORY
(ROM) 131
BIOS 133
(RAM) 132
OPERATING SYSTEM 134
APPLICATION PROGRAMS 135
OTHER PROGRAM MODULES 136
PROGRAM DATA 137
130

Figure 1

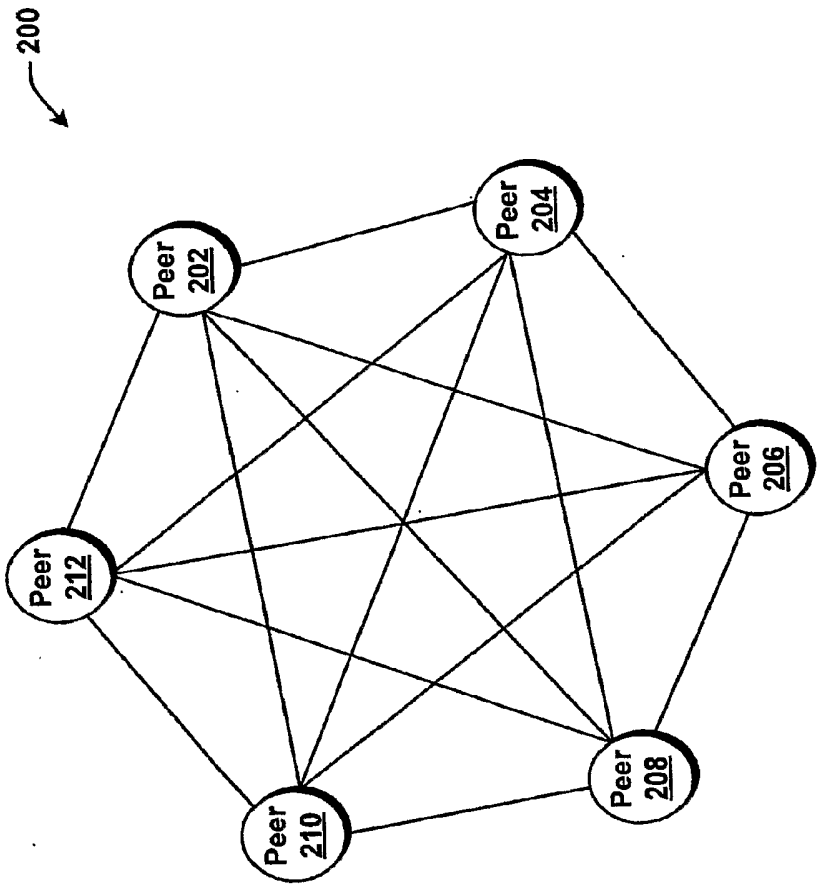


Figure 2

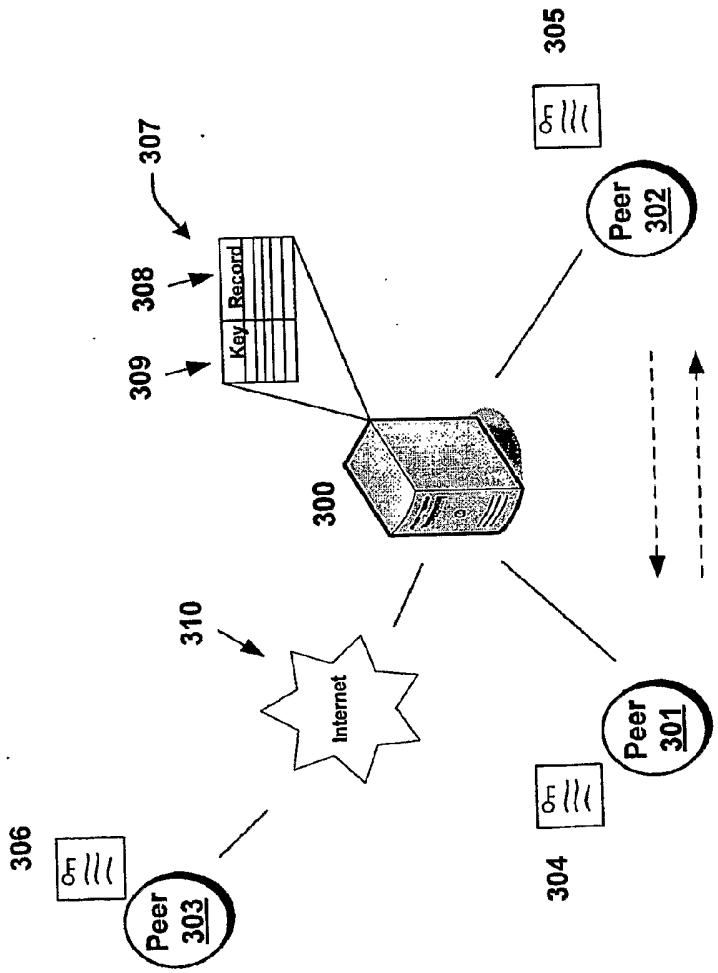

307
308
309
Key
Record
300
305
Peer 302
310
Internet
Peer 301
306
Peer 303
304

Figure 3

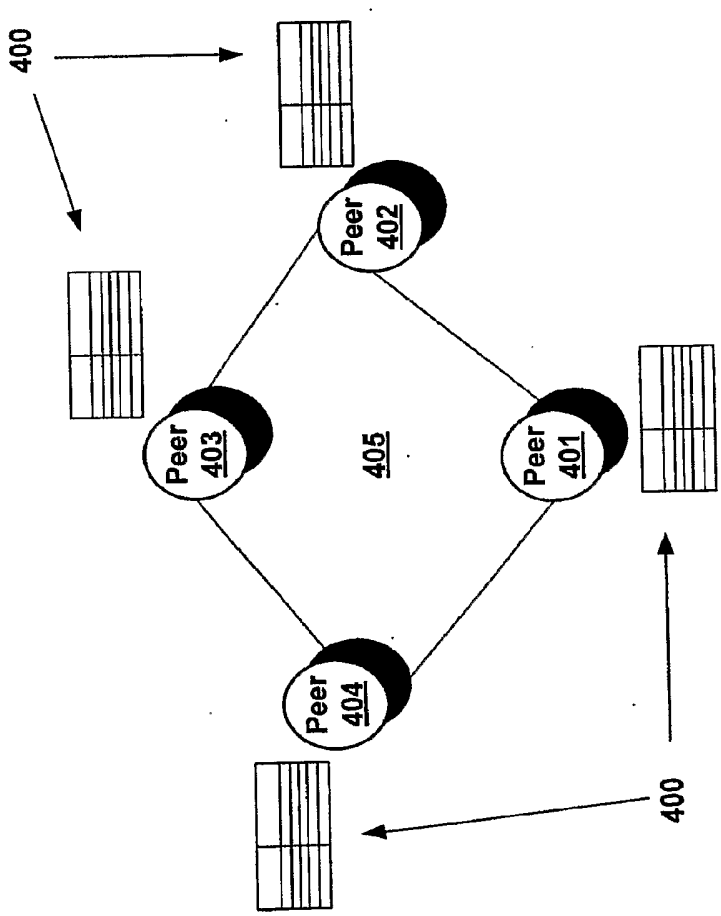


Figure 4

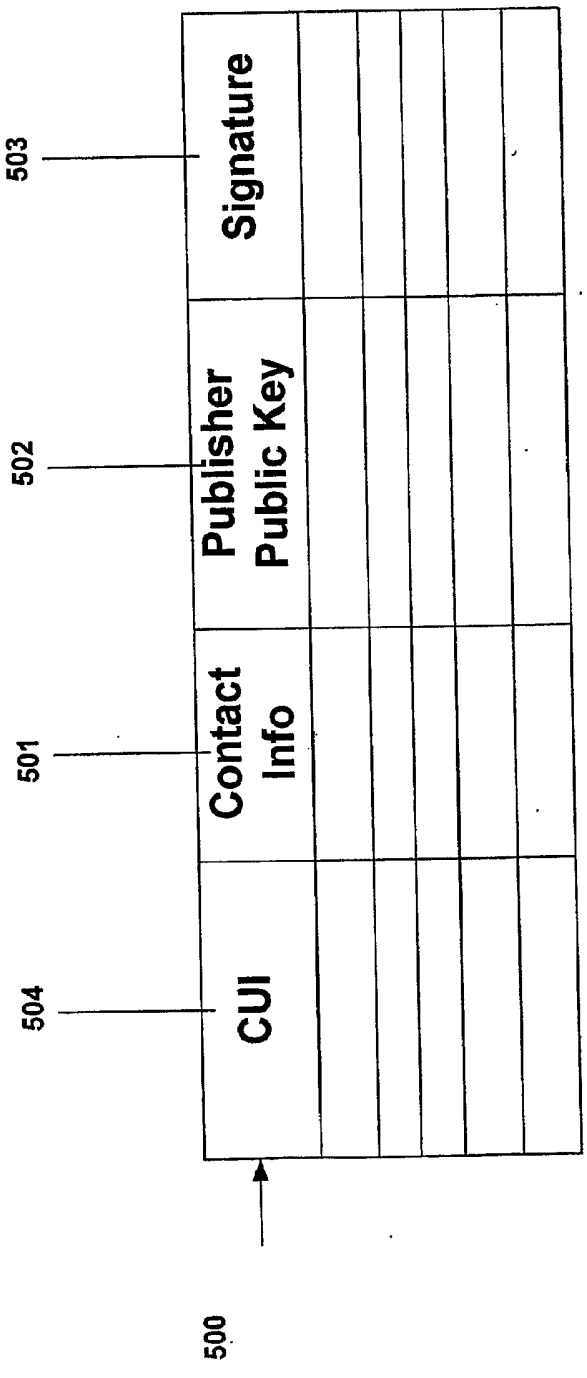

503
Signature
502
Publisher Public Key
501
Contact Info
504
CUI
500

Figure 5

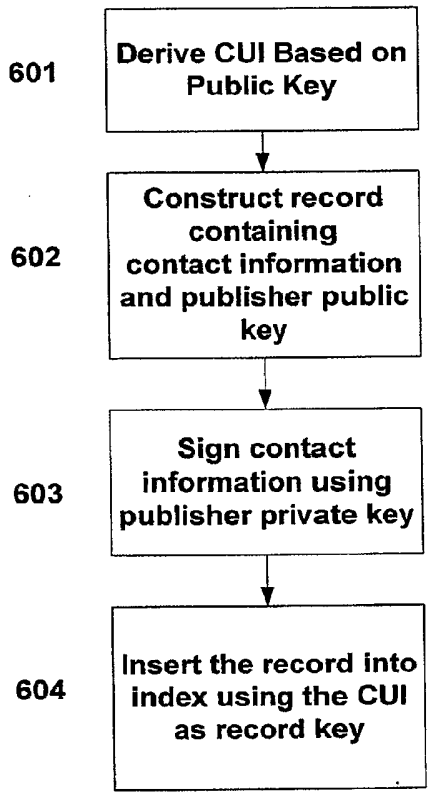

601
Derive CUI Based on Public Key
602
Construct record containing contact information and publisher public key
603
Sign contact information using publisher private key
604
Insert the record into index using the CUI as record key

Figure 6

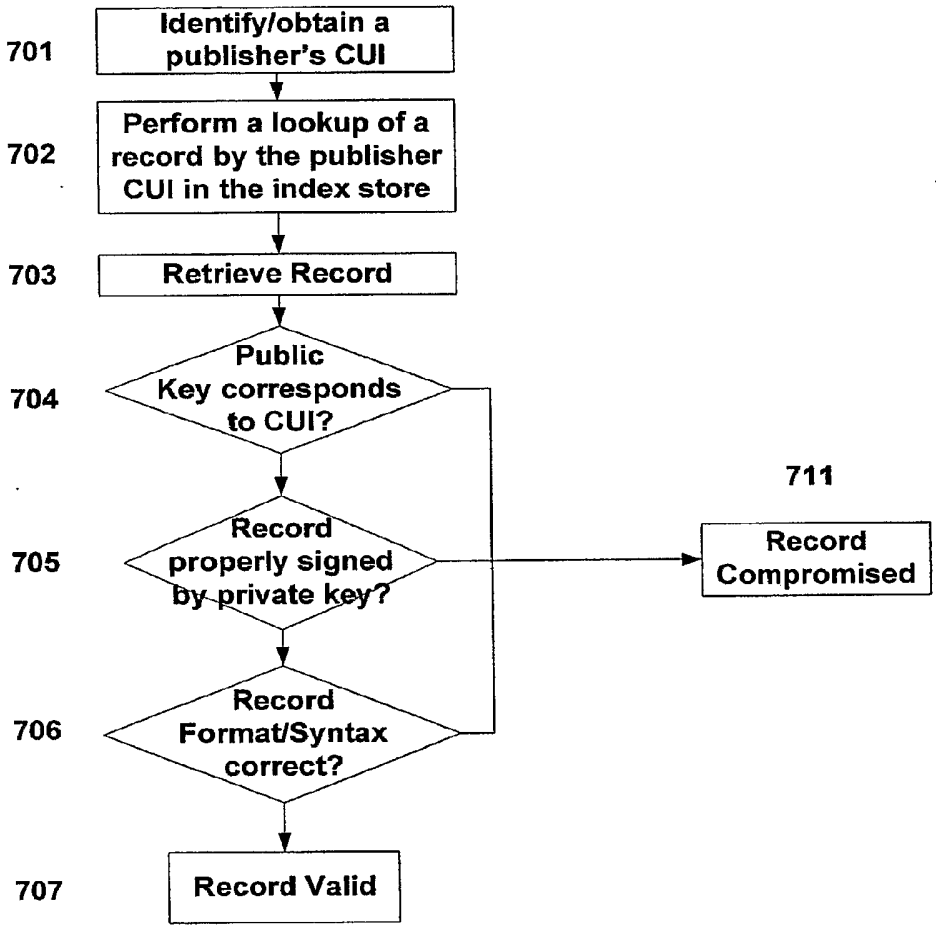

701
Identify/obtain a publisher's CUI
702
Perform a lookup of a record by the publisher CUI in the index store
703
Retrieve Record
704
Public Key corresponds to CUI?
705
Record properly signed by private key?
706
Record Format/Syntax correct?
707
Record Valid
711
Record Compromised

Figure 7

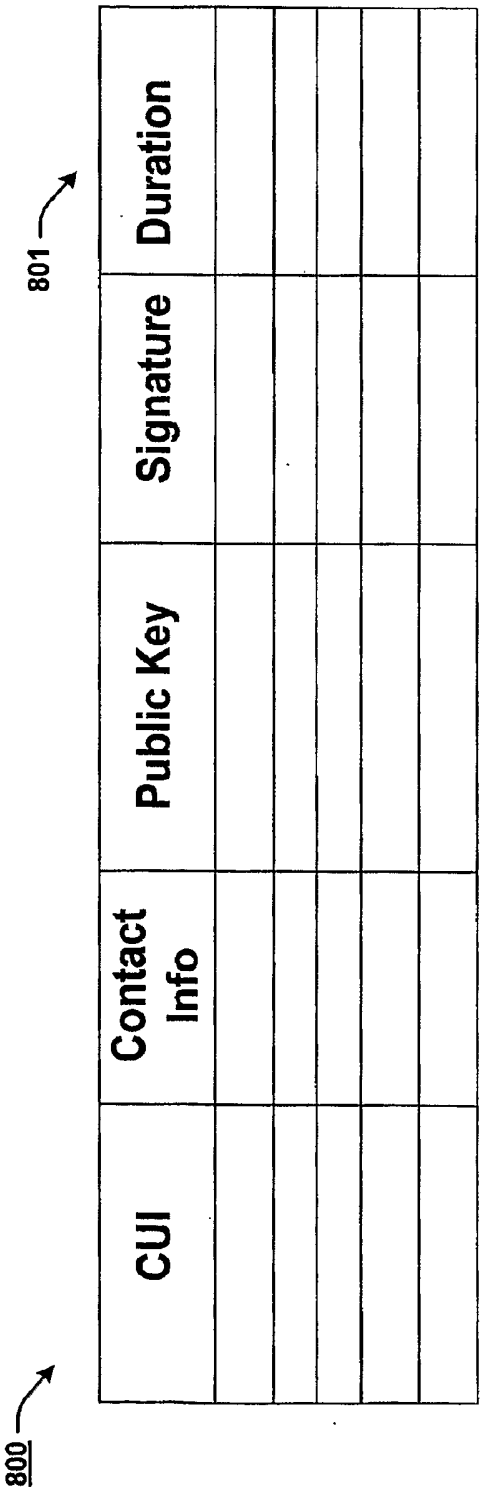


Figure 8

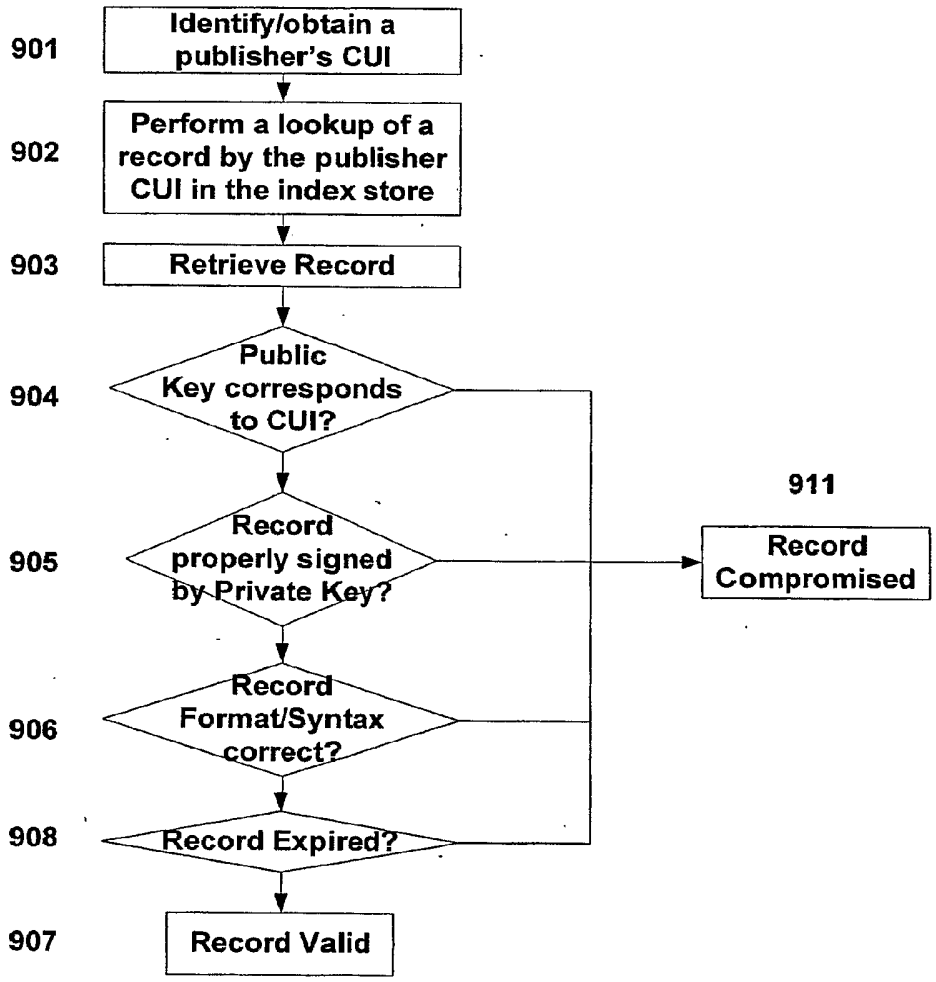

901
Identify/obtain a publisher's CUI
902
Perform a lookup of a record by the publisher CUI in the index store
903
Retrieve Record
904
Public Key corresponds to CUI?
905
Record properly signed by Private Key?
911
Record Compromised
906
Record Format/Syntax correct?
908
Record Expired?
907
Record Valid

Figure 9

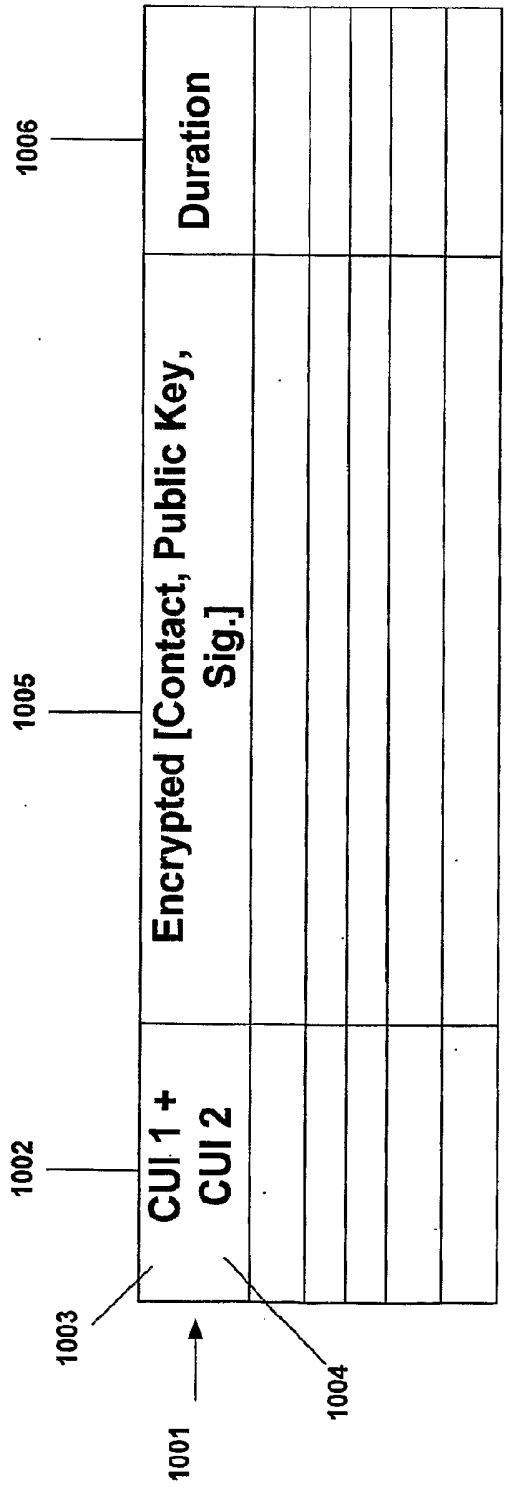

1006
Duration
1005
Encrypted [Contact, Public Key, Sig.]
1002
CUI 1 + CUI 2
1003
1004
1001

Figure 10

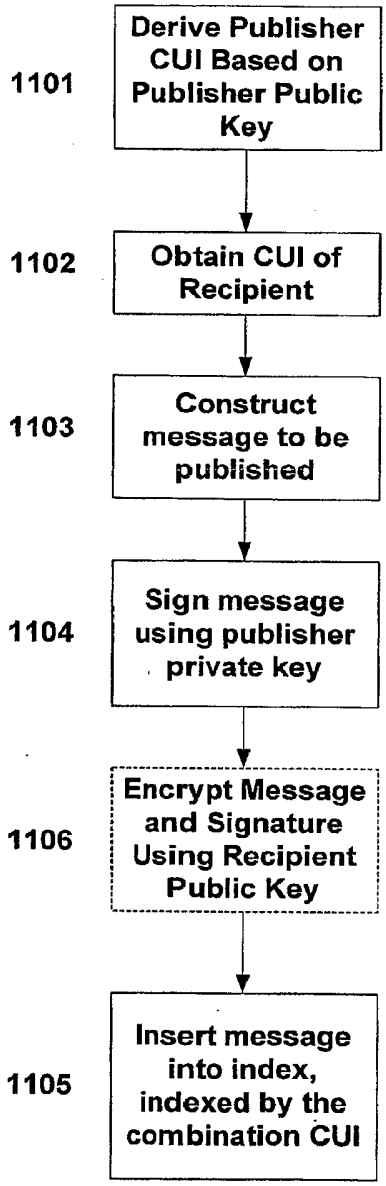

1101
Derive Publisher CUI Based on Publisher Public Key
1102
Obtain CUI of Recipient
1103
Construct message to be published
1104
Sign message using publisher private key
1106
Encrypt Message and Signature Using Recipient Public Key
1105
Insert message into index, indexed by the combination CUI

Figure 11

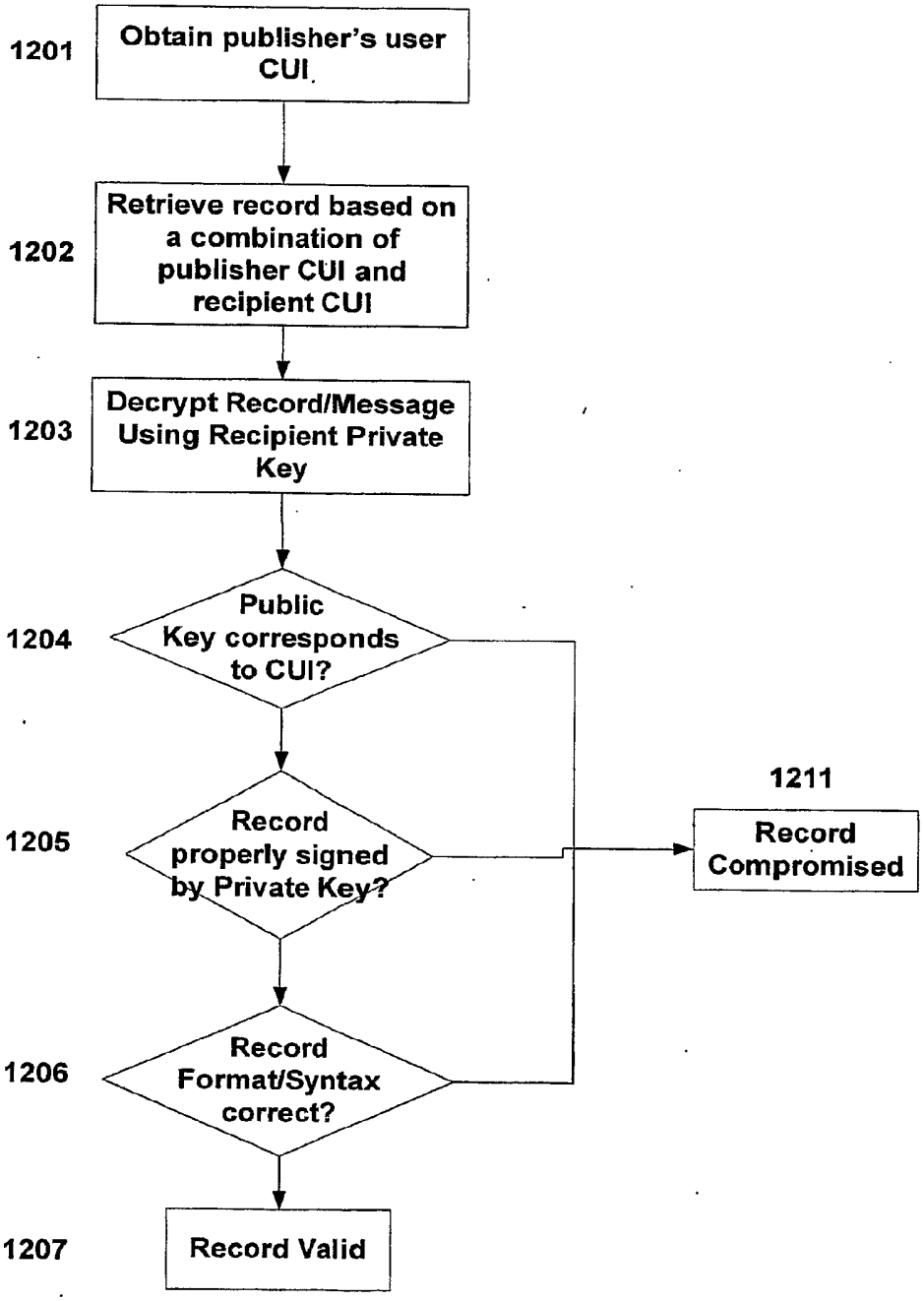

1201
Obtain publisher's user CUI
1202
Retrieve record based on a combination of publisher CUI and recipient CUI
1203
Decrypt Record/Message Using Recipient Private Key
1204
Public Key corresponds to CUI?
1205
Record properly signed by Private Key?
1206
Record Format/Syntax correct?
1207
Record Valid
1211
Record Compromised

Figure 12