



(51) International Patent Classification:

H04L 9/32 (2006.01) **G06F 21/00** (2006.01)
H04L 29/06 (2006.01)

(21) International Application Number:

PCT/FI2010/050517

(22) International Filing Date:

17 June 2010 (17.06.2010)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

20095685 17 June 2009 (17.06.2009) FI

(71) Applicant (for all designated States except US): **VALTION TEKILLINEN TUTKIMUSKESKUS** [FI/FI];
Vuorimiehentie 3, FI-02044 Vtt (FI).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **JUHOLA, Arto** [FI/FI]; Ratalaaksonkuja 5 C 10, FI-02760 Espoo (FI).
RAATIKAINEN, Pertti [FI/FI]; Klemetintie 1, FI-01690 Vantaa (FI).

(74) Agent: **IPR PARTNERS OY**; Bulevardi 2-4, FI-00120 Helsinki (FI).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ,

CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, 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, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— 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))

(54) Title: METERING UNIT FOR UNDENIABLE SERVICE MANAGEMENT AND A RELATED METHOD

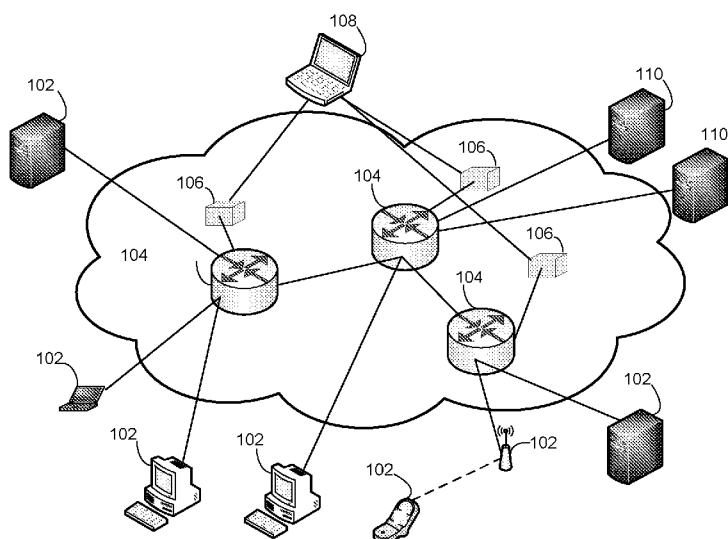


Fig. 1

(57) Abstract: A metering unit, functionally connectable to a router, and related method for monitoring and processing the data passed through a router, wherein the metering unit, internal or external device of the router, is capable of undeniably verifying outcomes of performed actions, actualizations of delivered services and/or current configurations. In addition, the metering unit is advantageously capable of monitoring and collecting the information of the network topology, such as the locations of its own and the elements nearby it in the network topology.

METERING UNIT FOR UNDENIABLE SERVICE MANAGEMENT AND A RELATED METHOD

FIELD OF THE INVENTION

5 This invention relates generally to communications networks. More particularly the present invention is directed to an undeniable service management platform for a packet switching network and a method for undeniably verifying outcomes of performed actions, actualizations of delivered services and/or presence of configurations.

10

BACKGROUND OF THE INVENTION

Today a packet switching network, such as the Internet, which is an aggregate of multiple smaller networks, may have countless of users throughout the world. In addition to email, packets transferred on the Internet may include various other
15 forms of data like video streaming data and bi-directional voice communications, for instance.

The importance and the usage of the Internet are rapidly changing as enhanced techniques including different broadband methods offer more possibilities to exploit more advanced applications. Accordingly, e-commerce is growing fast; it has been
20 estimated that product sales in online shops totaled \$146.4 billion in the United States in 2006, for example, whereupon the importance of the e-commerce is increasing year by year. Another example is provided by the e-services that the governments of several countries and enterprises offer to citizens and customers, respectively, for doing business in the Internet. For example, electronic voting is
25 already possible e.g. in Estonia and will also be introduced in many other countries in the near future.

However, the increased possibilities to do business in Internet have also brought on new security concerns. For example, frauds, identity thefts and phishing are some examples of today's threats in the Internet. Protecting confidential information is a
30 customary business requirement, and in many cases also an ethical and/or legal requirement. Demands for the successful fulfillment of the legal requirements will

be on the increase when the Internet solutions replace critical solutions, such as the above-mentioned voting. For instance, European Union has given a directive on the retention of identifying information that shall be saved for even two years. The responsibility to retain the identifying information may be left to the providers of
5 publicly available electronic communications services or of public communications networks.

The verification of the level of service management, the accuracy of configurations or the actualization of services or management actions is not always simple to accomplish. Because of outsourcing and third parties service management of the
10 Internet has spread causing difficulties in verifying the above-mentioned security issues. Nevertheless, preserving the trust of the subscribers or other users and the various governments in the disjointed and controlled environment requires clear and undeniable verifiability of deviations, i.e. who did what and when.

US 2006150153 A1 discloses a method for verifying digital objects by creating a
15 unique digital fingerprint. The creation of the fingerprint is done inside a terminal device and stored along with the object. The verification method can be used to validate that the digital object has not been semantically altered, despite the restructuring or reformatting of the object.

US 2005286535 A1 discloses methods for verifying consumer equipment that is
20 connected to a packet switched network. Information is hashed to generate a first hash value. Also the information in a memory of the consumer equipment is hashed in order to generate a second hash value. After that, the first hash value and the second hash value are compared to generate a verification indication for the consumer equipment. The Quality of Service for information packets that are
25 communicated with the consumer equipment through the packet switched network is controlled based on the verification indication.

SUMMARY OF THE INVENTION

The objective of the present invention is to at least alleviate one or more of the
30 aforesaid defects related to the prior art solutions what comes to the authentication of service management.

- The objective is met by a metering unit, a system and a related method for monitoring and processing the data passed, or to be passed, through a router or through other data emitting and/or forwarding entity. The metering, or “monitoring”, unit according to an embodiment of the present invention, physically being either an internal or external to the router, is advantageously capable of undeniably verifying the outcomes of performed actions, actualizations of delivered services and/or configurations. In addition, the metering unit is preferably capable of monitoring and/or collecting the network topology information, such as the locations of its own and the elements near it in the network topology.
- 10 Accordingly, in one aspect a metering unit functionally connectable to a router comprises a processing means for executing instructions and processing data, a storage means for storing data, and a transceiver for receiving and transmitting data, said metering unit further comprising one or more secured entities, such as trusted platform modules (TPM), for verifying, such as signing, data in the metering unit, the metering unit being configured to
- 15 obtain information related to the data passed through the router, such as a piece of the passed data or other information representing the passed data, and contextual information, such as identifying information, data transfer direction information, metering unit configuration information, local time stamp information, and/or network topology information,
- 20 obtain a cryptographic digest, such as a hash, for the information related to the data passed through the router and optionally to at least part of the contextual information,
- 25 obtain a non-repudiable data item, such as a time stamp, from a trusted third party, such as a trusted time stamp server, relative to cryptographic digest and optionally to at least part of the contextual information, and
- 30 to construct undeniable information and store it in the storage means, said undeniable information comprising the cryptographic digest, the contextual information, the non-repudiable data item, and verification information, such as a signature, based on verifying at least one of said digest, contextual information, and non-repudiable data item by the secured entity.

In one embodiment, all three elements, i.e. digest, contextual information and the non-repudiable data item, are verified. In another embodiment, only selected one or two of these elements are verified. Instead of all contextual information, only part of it may be verified.

- 5 According to another aspect of the present invention, a method for generating undeniable information, to be performed by a metering unit, comprises:
- obtaining information related to data passed through a router and to be verified, such as a piece of the passed data or other information representing the passed data, and contextual information, such as data transfer direction information, metering unit configuration information, local time stamp information, and/or network topology information,
 - obtaining a cryptographic digest, such as a hash, for the information related to the data passed through the router and optionally to at least part of the contextual information,
 - 15 - obtaining a non-repudiable data item, such as a time stamp, from a trusted third party, such as a trusted time stamp server, relative to cryptographic digest and optionally to at least part of the contextual information,
 - verifying, such as signing, at least one of said digest, contextual information, and non-repudiable data item by the secured entity,
 - 20 - constructing undeniable information, said undeniable information comprising cryptographic digest, the contextual information, the non-repudiable data item, and verification information, such as a signature, and
 - storing said undeniable information.

25 In a further aspect, a system for generating undeniable information comprises a metering unit and at least one trusted third party for providing a non-repudiable data item. Additionally, the system may further comprise a network management system for controlling said metering unit.

In one embodiment, which may be executed as a stand-alone or supplementary solution, a method for verifying locations and configurations of a metering unit and

one or more elements in the network, to be performed by the metering unit, comprises:

- obtaining information related to the configuration and location of the metering unit in the network topology,
 - 5 - verifying information related to the configuration and location of the metering unit in the network topology,
 - storing the obtained and verified information related to the configuration and location of the metering unit,
 - obtaining information related to one or more elements nearby the metering unit in
10 the network topology,
 - verifying the obtained information related to the one or more elements nearby the metering unit in the network topology, and
 - storing the obtained and verified information related to the one or more elements nearby the metering unit in the network topology.
- 15 Distance and/or nearness may be determined embodiment-specifically. Distance/nearness may refer to physical distance/nearness and/or logical distance/nearness. For example, distance/nearness may be determined utilizing at least one item selected from the group consisting of: element's network address or at least part thereof, transfer delay (one-way or roundtrip), geographical location
20 (e.g. coordinates), and number of hops. Differences between the addresses or locations of two entities may be then used for determining the distance/nearness between them, for instance. The associated decision logic may apply fixed and/or dynamic threshold values. Accordingly, nearby elements relative to the metering unit may be determined.
- 25 In one embodiment the metering unit may be configured to obtain ((through monitoring, for instance, the related parameter(s) such as the applied digest function) and verify its configuration(s) and location in the network topology. The verification may be performed by obtaining the non-repudiable data item from a trusted third party and/or by using the secured entity of the metering unit for signing
30 the undeniable information consisting of configuration and location information and the non- repudiable data item.

In another embodiment the metering unit may also be configured to obtain information related to the elements near it, according to predetermined criterion or criteria, in the network topology by using various one or more techniques.

5 In a further, possibly supplementary, embodiment the metering unit may be configured to monitor and store the data (or at least part or indication thereof) passed through the router and the identifying information thereof. A cryptographic digest calculation may be performed for the data, or the hash or corresponding function's outcome for the data may be obtained by some other way. The non-repudiable data item may be obtained from the trusted third party. The undeniable
10 information about the data passed through the router may be constructed by verifying with secured entity selected information as described herein in connection with various embodiments. The undeniable information may be then stored in the memory.

15 In a further embodiment one or more network elements, including the metering unit itself, are verified by using the trusted platform module (TPM) technique.

In one embodiment the cryptographic digest (function) calculation of data (e.g. bit stream) may be performed to adequate parts of the data (stream).

The utility of the present invention arises from plurality of issues. The invention provides an effortless way for retain identifying information and undeniably verify
20 the outcomes of performed actions, actualizations of delivered services and/or presence/nature of current configurations. Embodiments of the invention may also alleviate difficulties related to invoicing. Reliable verification of that the transmitted data has passed through the router may be made, according to the present invention, independent of operators or service providers. While retaining the identifying
25 information required by e.g. the authorities, the metering units can be utilized by a network operator for invoicing services on Internet traffic terms without using a heavy connection set-up managed by the operator. The suggested procedure may further prevent the "man-in-the-middle" -type of misuse of the network resources and services. Moreover, the reliability of the data traffic may be generally leveraged
30 when it is possible to undeniably track the device and point of time where e.g. a transmission error has occurred.

In this text "data passed through the router" or "passed data" refers to any kind of data transferred via the router, such as data packets and data stream. The transferred

data may be for example email data, image data, voice data, audio and/or video stream to name a few.

The expression “identifying information” refers to any kind of information included in the transferred data that can be utilized as such or together with other information to identify data traffic.

The expression “trusted third party” may refer to one or more entities, such as a timestamping authority and/or a certificate authority, which provide(s) required trusted information.

Furthermore, the expression “non-repudiable data item” may refer herein to a piece of data, such as a time stamp relative to the receiving time of a cryptographic digest (by e.g. a time-stamp service), preferably signed and/or otherwise verified such that the correctness and advantageously creation time of which cannot be disputed. For example, the data item may include a time stamp with a signature covering e.g. the cryptographic digest, the associated time indication and optional further elements.

In this text “cryptographic digest function” refers to a selected function, such as a hash function, generated about the data passed through the router by using a selected, preferably complex-to-hack, algorithm. The intent of this preferably substantially one-way (irreversible) function is to generate what in this document is called a “cryptographic digest”, that is, an unique identification of the source data, based on the essential property of the cryptographic digest function that guarantees (with a reasonable probability, taking into account the state-of-the-art) that no other piece of data will provide the same cryptographic digest when used as an input to the cryptographic digest function.

Still, the expression “undeniable information” refers herein at least to the data that the metering unit obtains and at least partially verifies by utilizing the secured entity.

Further, the expression “contextual information” may refer herein to identifying information, data transfer direction information, metering unit configuration information, time (stamp) information and/or network topology information.

In this text the expression “network resource” refers to whatever is obtained and/or controlled over the network.

Various embodiments of the present invention are disclosed in the dependent claims.

BRIEF DESCRIPTION OF THE DRAWINGS

5 Next the invention will be described in more detail with reference to the following drawings:

Fig. 1 illustrates an example of a network and the location of the metering unit in the network topology.

Fig. 2 shows a block diagram of internals of the metering unit in accordance with an embodiment of the present invention.

10 Fig. 3 illustrates a flow diagram of an embodiment of a method for generating undeniable information according to the present invention.

Fig. 4a illustrates a rough flow diagram of the operation of the metering unit according to one embodiment thereof.

15 Fig. 4b illustrates a flow diagram of an embodiment of a method for verifying configuration and the location of the metering unit.

Fig. 4c illustrates a flow diagram of an embodiment of a method for collecting information about the network topology.

DETAILED DESCRIPTION OF THE EMBODIMENTS

20 Figure 1 illustrates an example of a network and the location of the metering unit in the network topology. Figure 1 is no way meant to be precise representation of the network architecture, but only to serve as a rough example of possible elements in the network and their mutual functional connections. User (terminal) and network devices 102 are connected in the networks via different access points such as base
25 stations, WLAN access points, and/or routers 104 (several of such functionalities may also be integrated with a single physical apparatus), and the routers 104 are typically connected with several other routers of a number of networks. A metering unit 106, according to an embodiment of the present invention, is functionally connectable to one router 104, i.e. the metering unit 106 can either be integrated in a

- router 104 or it can be an external device or, in some cases, the metering unit 106 can even be physically distributed. The router is an element that forwards data between the sender and recipient thereof. The router may be located in a network, or a border of two or more (sub-)networks, and connect the multiple networks together, for example. The metering unit 106 may monitor one or more routers 104. Generally, the trusted third party 110 is a network device, e.g. a server, to which the metering unit 106 connects via the network, whereas the control means 108 may be directly connected to the metering unit 106. Alternatively, the (remote) control means 108 is connected to the metering unit 106 via the network.
- 10 The network, wherein the metering unit operates, may be a private or a public packet switching network or a part of a larger network or other type of a communications network having at least one router in it. The connections to the network and/or within the network may be implemented in a wired, such as fiber optics or cable, and/or wireless manner, such as radio waves, micro waves and infrared waves, for example. The user (terminal) and network devices 102 being at least functionally connected to a router 104 may include any type of devices typically used in the network, such as PC's, laptops, mobile devices, servers, hosts, etc., to name a few. Furthermore, the data transferred in the network may be located in packets or it may be multimedia data transferred as a stream of packets.
- 20 The control and/or the configuration of the metering unit, as well as reading and/or transfer of the stored data from the storage means of the metering unit, can be provided with one or more remote control means 108, such as a network management system dedicated or an integrated part of a larger whole. The remote control means 208 can be any type of separate device capable for connecting to the metering unit 106 and it may contain a user interface for controlling the metering unit 106. Instead or in addition to the separate device, the metering unit 106 may also comprise a user interface providing possibility to directly control and/or configure the metering unit. In this case, the user interface may comprise a display or a connector to an external display, and keyboard/keypad or other applicable control input means (e.g. touch screen or voice control input, or separate keys/buttons/knobs) configured so as to provide the user of the metering unit 106 with practicable data visualization and metering unit control means.

Moreover, the metering unit obtains the non-repudiable data item from a trusted third party 110, which can be one or more entities, such as timestamping authority

or certificate authority. Generally, the trusted third party is a service external of the metering unit, more generally, the trusted third party is accessible via the network as the other user and network devices. The trusted third party is normally an authority or an instance approved by an authority, e.g. a reliable timestamp can be obtained
5 from French postal service. Usually, the used trusted third parties are such that the acquiring of the non-repudiable data item is performed fast enough, e.g. within a few seconds. Distributed or multiple trusted third parties as well as several trusted third party servers/services can also be used to eliminate (as far as possible) the need to trust any single trusted third party stakeholder/system. That will further
10 increase the reliability and reduce the vulnerability of timestamps. Alternatively, the metering unit could itself comprise an entity for providing non-repudiable data items. Typically, the non-repudiable data item includes accurate time reference data, for example a timestamp, which is utilized to unquestionably define a certain point of time.

15 With the reference to Figure 2, an embodiment of the metering unit in accordance with the present invention comprises a processing means 202, a storage means 204, one or more transceivers 206, a control means 208, one or more secured entities 210 and, optionally, one or more additional logic blocks 212.

At first, the control means 208 is a local internal counterpart to the external control
20 means 108 in Fig. 1. The control means 208 may contain, for example, local execution logic of the remote control means for implementing the instructions by the remote control means.

Still, the processing means 202 comprises at least one processor, such as one or more microprocessors, micro-controllers, DSP's (digital signal processor),
25 programmable logic chips, etc., or any desired combination thereof. In addition, the processor may comprise a plurality of cooperating processors or sub-processors. The processing means 202 is configured to execute the code stored in a storage means 204, which may imply processing instructions and data relative to the metering unit functionalities of the present invention and optionally other
30 functionalities, such as OS related functionalities, I/O-related functionalities, and other applications. In addition, the processing means 202 controls the secured entity 210, as well as the additional logic blocks 212.

Furthermore, the storage means 204 may be divided between one or more physical memory chips or other memory elements, and it may comprise code, e.g. in a form of a computer program/application for the metering unit, and other data. Moreover, the storage means 204 may further include other storage media, such as a preferably detachable memory card, a floppy disc, a CD-ROM, fixed storage medium such as hard drive. The storage means 204 may be non-volatile, e.g. ROM, PROM, EEPROM or flash memory, and/or volatile, e.g. RAM, by nature.

Moreover, the transceiver 206, complying with predetermined wired or wireless technology, for communication primarily with the router the metering unit is connected to and, in addition to that, with other devices such as network devices and separate devices, for example the control means of the metering unit. The transceiver can be a device that has both transmitting and receiving capabilities or the transceiver may consist of a separate transmitter and receiver. While having more than one transceiver in the metering unit, some of transceivers can be implemented for wired network, for example converting electrical pulses to light and vice versa, and the other can be implemented for wireless network technology, such as GSM, UMTS, WLAN, Bluetooth, Wimax, etc.

Furthermore, the secured entity 210 included in the metering unit is for verifying and signing the information obtained by the metering unit. The secured entity 210 may be implemented by using the trusted platform module (TPM) technique or some other technique, in which the secured entity 210 is a physical device having a unique identifier and in which the functionalities of the entity are physically secured. Usually, the secured entity has a public/private key pair, which the private key is generated within the secured entity and never exposed outside it.

The metering unit may also comprise additional logic blocks 212, such as a math block, for processing data packets. The logic blocks 212 are typically stored in the storage means 204 of the metering unit and they can be executed by the processor 202. The logic blocks, especially math blocks, can be used for the cryptographic digest function, i.e. the hash function, calculation. Several methods can be used for the hash function calculation, e.g. RIPEMD-128, RIPEMD-160 and/or SHA-2 family. Therefore, a table or other entity may be maintained for the hash function so as to confirm, with which method the cryptographic digest function has been calculated. The cryptographic digest function calculation method is advantageously changeable and the other advantageous requirements for the method are that the

calculation procedure is fast enough and the approximated crack time of the hash function should be at least as long as the required retaining time of the identifying information, e.g. about two years.

5 It is clear to a skilled person that the metering unit may, in practice, comprise numerous further functional and/or structural elements for providing various beneficial communication, processing, or other features, whereupon this disclosure is not to be constructed as limiting the presence of potential additional elements in any manner.

10 Turning to Figure 3, Figure 3 illustrates a flow diagram of the method for constructing undeniable information according to the present invention. The method for verifying and signing information with the secured entity is similar regardless of the content of the information. Thus, the verification method for every verification step in the metering unit is described herein in conjunction with Figure 3.

15 At step 302, the data that is desired to be verified is obtained. The data can be any information obtained by the metering unit: data passed through the router, information related to the network topology and/or to configuration (e.g. predetermined configuration parameters such as the used digest function, transfer speed, QoS (quality of Service settings), etc.) of the metering unit, for example. The transferred data packets or data stream may be e.g. email, image, voice, audio
20 and/or video stream. When it comes to data stream, it is divided into appropriate packets, e.g. duration of about 1-2 second, depending on the buffer length of the router. Mark bits may be added to the packets so that synchronization of the cryptographic digest functions can be performed afterwards. Moreover, the data can be obtained several ways. While data is transferred via the router, it will also
25 preferably pass through the metering unit, but in the case of the network topology and related data, for example, the metering unit may request the desired data, or the metering unit may monitor the data traffic and obtain the desired information from there.

30 Further, contextual information, such as identifying information of the data passed through the router, is obtained at the step 302. The identifying information typically comprises data traffic and location information, such as data transfer direction information, as well as information required for identifying the subscriber or the user of a network resource, e.g. the connection source, the destination information

of the packet, starting time of the transfer, the ending time of the certain network resource, etc. The other contextual information may comprise information related to the network topology and/or to configurations of the metering unit, for example, or some other related information, e.g. timestamp of the metering unit.

- 5 At step 304, the metering unit obtains the cryptographic digest for the data desired to be verified. In some embodiment the cryptographic digest is calculated in the metering unit by using an additional math block or by the secured entity. In some other embodiment the cryptographic digest is obtained by some other way. For instance, the calculation may be performed by some other element in the network,
- 10 e.g. the metering unit in the service producer's side on the network, and the cryptographic digest is passed together with the data. This is a lighter way to produce the cryptographic digest, but, however, potentially more unreliable. In addition, if a data passed through the router has a well known hash function, the hash function can be obtained instead of the cryptographic digest calculation. In
- 15 some cases the hash function of the data can be obtained from somewhere else, but the cryptographic digest may be calculated nevertheless. Yet, in an additional or alternative embodiment, the cryptographic digest function consists of the number of the data packets. On the other hand, in case the metering unit obtains information about the network topology, the cryptographic digest calculation cannot be
- 20 performed this way. In one more, either alternative or supplementary, embodiment the cryptographic digest is obtained for the contextual information or suitable parts thereof, too. This is convenient in case the contextual information is also desired to be verified by the trusted third party/parties, for instance.

- At step 306, the cryptographic digest function/functions is/are sent to a trusted third
- 25 party/parties and the signed cryptographic digest function/functions is/are returned with the non-repudiable data item/items. The non-repudiable data item is typically a timestamp indicating the exact point of time. For increasing the reliability the timestamp can be obtained from various trusted third parties.

- The undeniable information is constructed at step 308 by attaching the
- 30 cryptographic digest function and/or hash function and the non-repudiable data item as well as the contextual information to the data that is desired to be verified. In case of the data passed through the router, the data to be verified may comprise at least the suitable parts of the transferred data. If the data has well known hash function, the hash function with the identifying information might be sufficient

instead of the data. In some cases, a part of the data with the identifying information may be enough, for example, in the case of streaming data, and otherwise, the data comprises identifying information and the entire transferred data.

Next, the undeniable information is verified in the secured entity at step 310.

- 5 Typically, the desired data is verified by sending the cryptographic digest function of the data to the secured entity. Then the secured entity verifies the data by signing the cryptographic digest and/or optional further data using the private key of the secured entity and returns the signed cryptographic digest and/or optional further data back to the metering unit.
- 10 Finally, the undeniable information is stored in the memory, step 312. The memory may be the storage means of the metering unit or it may be some other external storage. In case of external storage, several metering units may employ the same storage. In one embodiment, information related to the data transferred via the router includes the transferred data itself (e.g. consumed content such as an
- 15 audiovisual representation, e.g. a movie) or at least part thereof, and is stored as such. In some embodiments, the metering unit may supervise, through background execution of a related monitoring task, for example, that multiple copies of the transferred (payload) data or part of it are not stored, for instance, if a copy is already stored in the local or remote storage to which the metering unit has access.
- 20 In that case, the metering unit may have gained a link to the stored data from the sending device and the metering unit may then optionally forward the link, e.g. within the contextual information, in conjunction with the transferred data to the next device, for example. Alternatively, the metering unit may itself generate a link to the already-stored copy of the transferred data after detecting the existence thereof. The metering unit may, for example, compare existing digests of older data
- 25 transmissions to the just determined digest of the current transmission and when a match is found, generate the link instead of storing the same transferred data once more. In case the metering unit stores the data in some external storage and/or the storage means of the metering unit, the metering unit may include a qualifier, e.g. a
- 30 link, in the transferred data to indicate to the other devices that the data has already been stored. Alternatively or additionally, the undeniable information may be transmitted for permanent storing to a network management and/or some other management or other entity associated with one or more metering units. The undeniable information may be sent e.g. as appropriate-sized blocks or immediately
- 35 after generating it.

Generally, access codes, for example, bank access codes and alike, are not stored or they are stored in encrypted form. While storing encrypted information, it is possible to store also the encryption keys so that the encrypted information is decodable afterwards.

- 5 Otherwise, the undeniable data that relates to the configuration of the metering units and the network topology is normally stored as such.

Alternatively, in other embodiment the construction and the verification of the undeniable information are performed in a different order as can be seen in Figure 3 presented with broken arrows. After obtaining the data and related contextual
10 information, at step 302, and obtaining the cryptographic digest function for the data and possibly for the contextual information or suitable part(s) thereof, at step 304, the data and/or the cryptographic digest thereof and/or the related contextual information and/or the cryptographic digest thereof are verified by using the secured entity of the metering unit, at step 310. Next, the cryptographic digest of the data
15 and/or the contextual information or the cryptographic digest thereof is sent to the trusted third party/parties, at step 306. The trusted third party/parties will return the sent data with (preferably signed) time stamp as a non-repudiable data item. Then, the undeniable information is constructed and stored, at steps 308 and 312, as described above. In one, either alternative or supplementary, embodiment the data
20 and the contextual information thereof can still be verified in the secured entity 310 after sending the aforesaid data and contextual information to the trusted third party at 306.

Turning to Figure 4a, Figure 4a illustrates a rough flow diagram of possible procedures of the metering unit in connection with an embodiment of the present
25 invention. At first, the metering unit may verify the components in it 402, i.e. the secured entity, as well as the associated configurations and/or preferably information related to its location. Next, the metering unit preferably obtains information about the network topology 404, i.e. the locations of elements nearby it in the network, and after that, the metering unit initiates the obtaining and the
30 verification of the data passed through the router 406.

Generally, the verification of one or more components in the metering unit 402 may be performed right after the metering unit is assembled to its location and optionally every time the configuration(s) of the metering unit are changed. In addition, the

metering unit may be configured to perform the verification occasionally or periodically, e.g. once in a week.

Acquisition and verification of the information related to the network topology 404 may be performed more often than the verification of the metering unit (identity and/or e.g. configuration) itself. Since the elements in the network may change frequently, although the locations of routers may be more stabile, the information concerning the network topology may expire fast. The appropriate time period for confirming the network topology may be once in a minute or on daily/weekly basis, for instance. In one embodiment the metering unit monitors the elements nearby it continually by a background run.

Respectively, the obtaining and verification of the data passed through the router 406 may be performed substantially continuously. At least functional connectability between the metering unit and the router enables the metering unit to at least monitor the transferred data. In some embodiments the transferred data may also physically pass through the metering unit.

The steps concerning the verification of the components in the metering unit is illustrated in Figure 4b. At first, the secured entity provides a certification that the particular secured entity is genuine 410. It may confirm that the used public/private key pair of the secured entity for signing is protected, too. The certificates may be verified and signed by trusted third party, typically a certificate authority.

After certification of the secured entity 410, the configuration(s) and the location information of the metering unit can be verified as described herein, for instance. In the beginning, the metering unit may obtain information related to its own location in the network topology 412. The location information can be obtained by several ways. The metering unit may utilize a link state protocol, for instance, requesting the MAC-address of the router, to which the metering unit is connected, by using a proper protocol, e.g. ARP-protocol (Address Resolution Protocol). The metering unit can also determine whether it is within a wider area, such as an intranet. The metering unit may obtain information related to its location in the network topology by detecting the network or sub-network wherein it is located. It may acquire location information by monitoring network address information of one or more other network elements, e.g. neighbouring elements, and/or of the metering unit and/or the router itself, for example. On the other hand, the identifying information

of the router that the metering unit is connected to, or of other element(s), may be entered manually to the metering unit by using the control means of the metering unit, for example.

At step 414, the metering unit verifies the information related to its configuration(s) and location in the network. At step 416, the obtained and verified information related to the location and configuration(s) of the metering unit is stored in the storage means of the metering unit.

Respectively, in Figure 4c, the information, such as location and/or configuration information, related to the elements nearby the metering unit in the network is obtained 420, for example, by inquiring/requesting the MAC-address of the elements. In some embodiment the metering unit may also require the obtained information to be verified by the secured entity of the elements. In one other, either supplementary or alternative, embodiment, the metering unit may collect information about the network topology by monitoring the IP-signaling of the elements and collecting the required information from it. Further, in some advanced embodiments, the metering unit may as well control the authenticity of the obtained information by observing the response time of the elements. For example, the response time should be short if the element is claimed to be nearby the metering unit.

Next, the obtained information about the network topology is then verified by the secured entity 422. Finally, the obtained and verified information related to the network topology is stored in the memory 424. The used memory may be the storage means of the metering unit or the metering unit may collect the network topology information to some external storage, which might be shared between several metering units and/or other devices. The stored information about the network topology can be united afterwards with the information of the other metering units and/or the network topology information collected by some other components to create a wider view of the elements in the network and a route of some particular data packet. This information is useful when tracking afterwards a precise error point of a transferred data packet.

In a preferred embodiment the method for verifying the data passed through the router is utilized while monitoring and verifying the network traffic in the aspect of SLA (Service Level Agreement). At least one metering unit according to an

embodiment of the present invention is preferably utilized to monitor input and/or output traffic of the network so as to produce undeniable information including accurate timestamp for the purposes of the SLA system.

5 In one, either supplementary or alternative, embodiment the metering unit is configured to monitor the acknowledgement traffic of the router, where at least one party in the transmission path is the router and the other(s) may be, for example, the entity that has sent the transferred data and/or the end user, who receives the transferred data. In this embodiment, the verification procedure may be accomplished after the acknowledgement information is sent and/or received by the
10 router.

The procedure of monitoring the acknowledgement traffic preferably allows the metering unit to verify faultless packets only; whereas the corrupted packets may be omitted by the metering unit or possibly some other classification procedure may be performed to them. The metering unit may be configured to delete the corrupted
15 packets completely, which induces a missing packets situation noticed in a receiving entity, for example in a host device of the end user, and which will further initiate the packets retransmission.

Furthermore, the sent and/or received acknowledgement information may be included in the contextual information of the data passed through the router. Thus,
20 the reliability of the undeniable information of performed actions and/or actualizations of delivered services is increased and afterwards it is easier to undeniably verify the functionality of the router.

The scope of the patent will be defined by the appended claims. Skilled persons will appreciate the fact that various changes and modifications may be made to the
25 explicitly disclosed embodiments and features thereof without diverging from the scope as set forth in the claims.

CLAIMS

1. A metering unit (106) functionally connectable to a router comprising a processing means (202) for executing instructions and processing data, a storage means (204) for storing data, and a transceiver (206) for receiving and transmitting data, said metering unit further comprising one or more secured entities (210), such as trusted platform modules (TMP), for verifying, such as signing, data in the metering unit, the metering unit being configured to
5 obtain information related to the data passed through the router, such as a piece of the passed data or other information representing the passed data, and contextual information, such as identifying information, data transfer direction information, metering unit configuration information, local time stamp information, and/or network topology information,
10 obtain a cryptographic digest, such as a hash, for the information related to the data passed through the router and optionally to at least part of the contextual information,
15 obtain a non-repudiable data item, such as a time stamp, from a trusted third party, such as a trusted time stamp server, relative to cryptographic digest and optionally to at least part of the contextual information, and
20 to construct undeniable information and store it in the storage means, said undeniable information comprising the cryptographic digest, the contextual information, the non-repudiable data item, and verification information, such as a signature, based on verifying at least one of said digest, contextual information, and non-repudiable data item by the secured entity.
- 25 2. A metering unit of any preceding claim, further comprising a control means (208) for controlling and/or configuring said metering unit and/or providing said undeniable information from said metering unit.
3. A metering unit of any preceding claim, wherein said metering unit is external of said router.

4. A metering unit of claim 1-2, wherein said metering unit is integrated into said router.
5. A metering unit of claim 1-2, wherein said metering unit is physically distributed among a plurality of network devices.
- 5 6. A metering unit of any preceding claim, wherein said metering unit comprises one or more logic blocks (212) for processing said collected data.
7. A metering unit of claim 6, wherein one or more of said logic blocks are configured to perform calculation of the cryptographic digest using a cryptographic digest function.
- 10 8. A metering unit of any preceding claim, wherein said cryptographic digest function for the data is executed in a device of a service provider and included in the data passed through the router.
9. A metering unit of any preceding claim, wherein said non-repudiable data item comprises a time stamp obtained from said trusted third party.
- 15 10. A metering unit of any preceding claim, wherein said information related to the data passed through the router comprises the identification information.
11. A metering unit of claim 10, wherein said information related to the data passed through the router further comprises the data passed through the router.
12. A metering unit of claim 10, wherein said information related to the data
20 passed through the router further comprises a part of the data passed through the router.
13. A metering unit of claims of any preceding claim, wherein a qualifier is included in contextual information to notify other elements in the network about the storage of the data.
- 25 14. A metering unit of any preceding claim, wherein said metering unit is configured to obtain and verify the information related to its own configurations and location in the network topology and generating the undeniable information of said obtained information.

15. A metering unit of any preceding claim, wherein said metering unit is configured to obtain and verify the information related to the locations of the elements nearby said metering unit in the network topology and generating the undeniable information of said obtained information.
- 5 16. A metering unit of any preceding claim, wherein said network elements, including the metering unit, are verified by using said secured entity/entities.
17. A metering unit of any preceding claim, wherein the metering unit is configured to monitor the acknowledgement traffic of the router.
- 10 18. A metering unit of claim 17, wherein the metering unit is configured to verify only the data in relation to which the acknowledgement information is sent and/or received by the router.
19. A metering unit of claim 17 or 18, wherein acknowledgement information is included in the contextual information of the transferred data.
- 15 20. A system for generating undeniable information comprising a metering unit (106) of any of preceding claim and at least one trusted third party (110) for providing a non-repudiable data item.
21. A system of claim 20 further comprising a network management system for controlling said metering unit.
- 20 22. A method for generating undeniable information (406), to be performed by a metering unit, comprising:
- obtaining information related to data passed through a router and to be verified, such as a piece of the passed data or other information representing the passed data, and contextual information, such as data transfer direction information, metering unit configuration information, local time stamp information, and/or network topology information (302),
- 25 -obtaining a cryptographic digest, such as a hash, for the information related to the data passed through the router and optionally to at least part of the contextual information (304),

-obtaining a non-repudiable data item, such as a time stamp, from a trusted third party, such as a trusted time stamp server, relative to cryptographic digest and optionally to at least part of the contextual information (306),

5 -verifying, such as signing, at least one of said digest, contextual information, and non-repudiable data item by the secured entity (310),

-constructing undeniable information, said undeniable information comprising cryptographic digest, the contextual information, the non-repudiable data item, and verification information, such as a signature, (308), and

-storing said undeniable information (312).

10 23. A method of claim 22, further comprising, in order to verify location and configuration of a metering unit and information related to one or more elements in the network (402, 404):

-obtaining information related to the configuration and location of the metering unit in the network topology (410, 412),

15 -verifying information related to the configuration and location of the metering unit in the network topology (414),

-storing the obtained and verified information related to the configuration and location of the metering unit (416),

20 -obtaining information related to one or more elements nearby the metering unit in the network topology (420),

-verifying the obtained information related to the one or more elements nearby the metering unit in the network topology (422), and

-storing the obtained and verified information related to the one or more elements nearby the metering unit in the network topology (424).

25 24. A method of claim 23, wherein said metering unit obtains information related to the network topology by utilizing a link state protocol.

25. A method of any of claims 23-24, wherein said metering unit obtains the information related to the elements nearby said metering unit in the network by monitoring the IP signaling of said elements.

26. A method of any of claims 23-25, wherein said metering unit requests the
5 verification for the information related to the elements nearby said metering unit in the network to be performed by the secured entity of said elements.

27. A method of any of claims 23-26, wherein said metering unit detects at least part of the information related to the elements in the network by monitoring the response time of the elements.

1/3

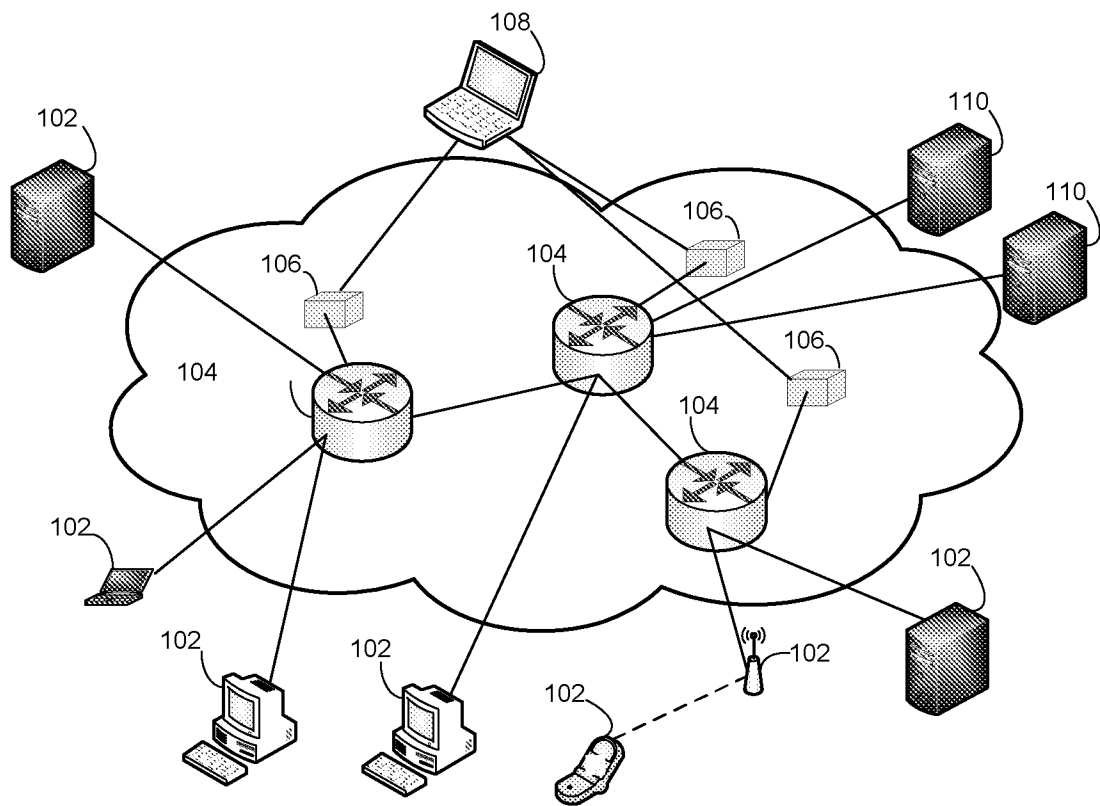


Fig. 1

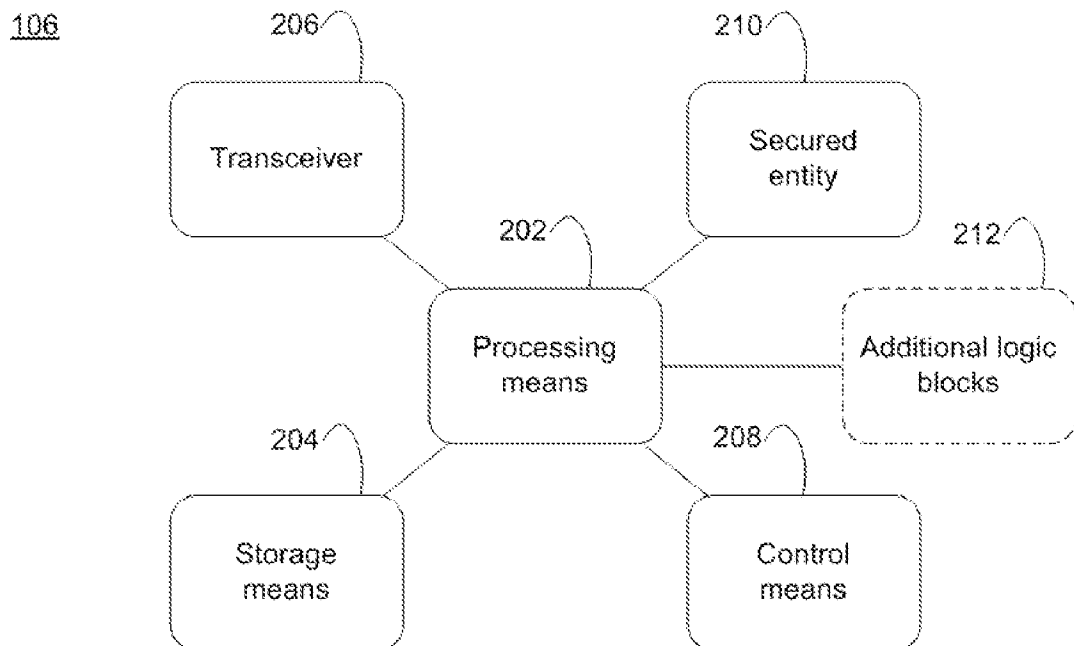


Fig. 2

2/3

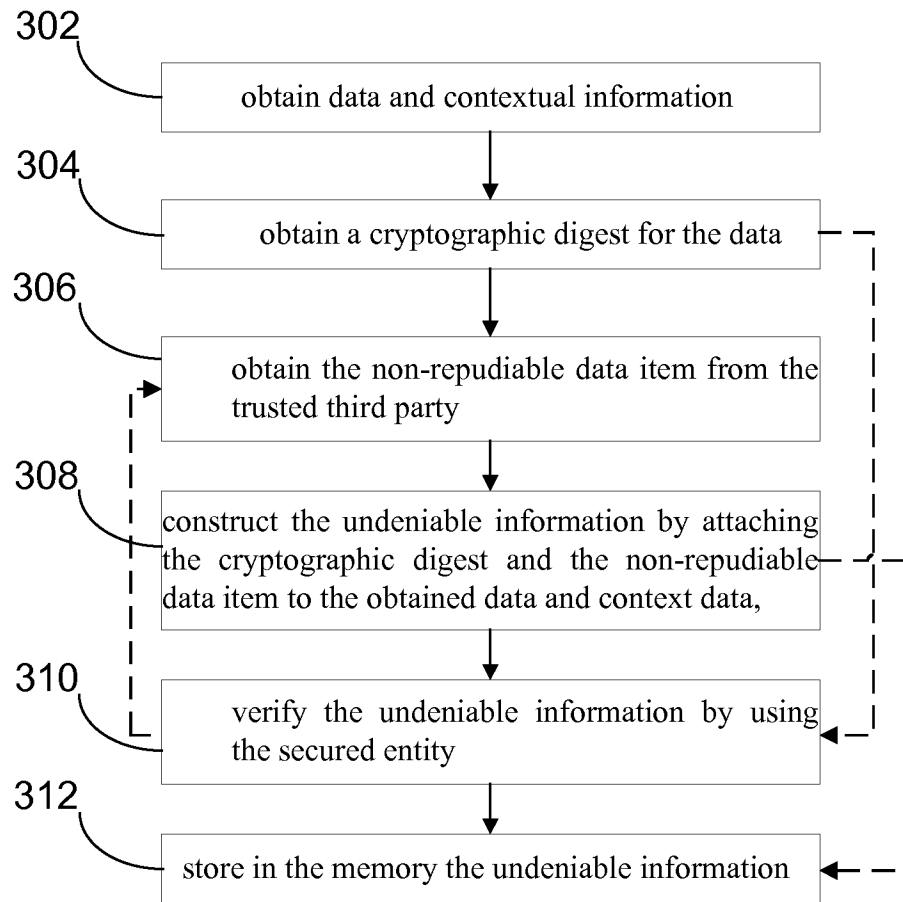


Fig. 3

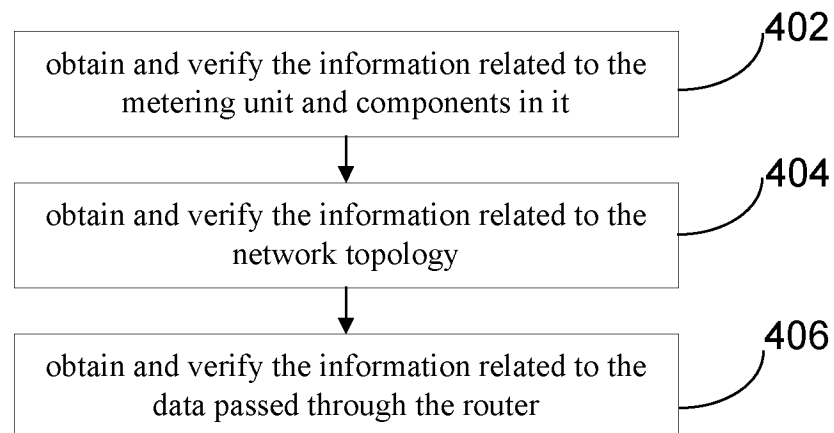
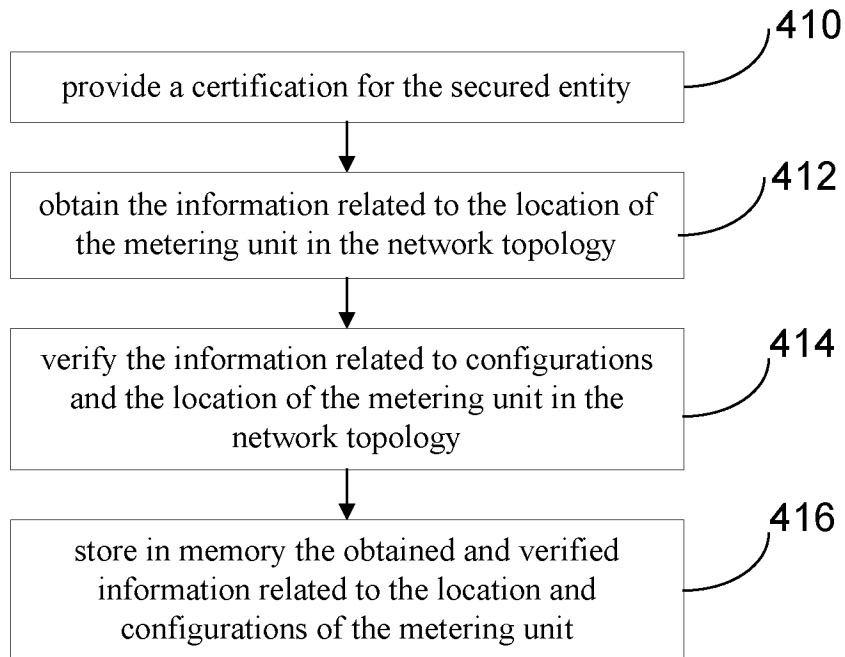
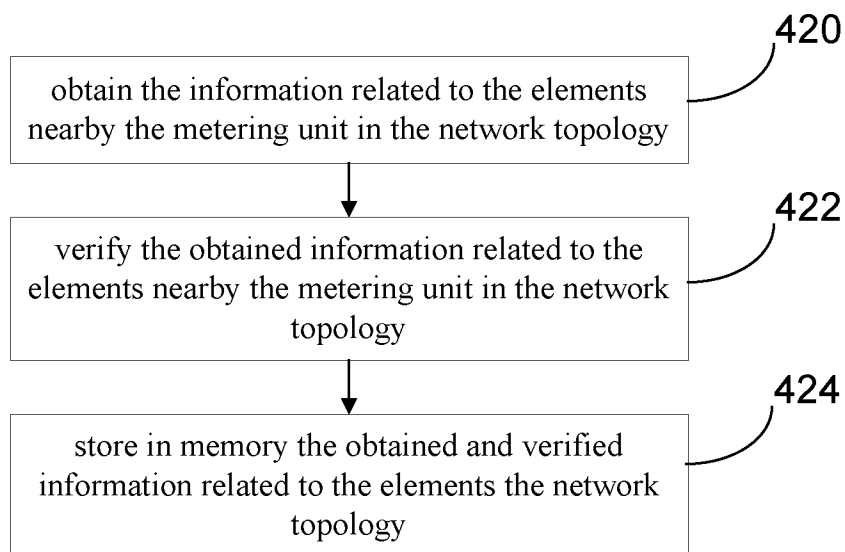


Fig. 4a

3/3

**Fig. 4b****Fig. 4c**

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI2010/050517

A. CLASSIFICATION OF SUBJECT MATTER

See extra sheet

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)

IPC: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
FI, SE, NO, DK

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI, XPAIP, XPESP, XPETSI, XPIEE, XPIETF, XPIOP, XPIPCOM, XPI3E, XPMISC, XPOAC, 3GPP, COMPENDEX, INSPEC, Google

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 101447999 A (GOLDEN VISTA BEIJING TECHNOLOG) 03 June 2009 (03.06.2009) & WPI Abstract	1-27
A	US 2009044010 A1 (HUGHES JAMES P) 12 February 2009 (12.02.2009) [0017] – [0018], Fig. 1	1-27
A	US 2007022296 A1 (CAVERLY GORDON et al.) 25 January 2007 (25.01.2007) abstract	1-27
A	EP 1228451 B1 (SIGN ON I STOCKHOLM AKTIEBOLAG) 07 August 2002 (07.08.2002) [0027] – [0029], Fig. 1	1-27

☒ 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
08 October 2010 (08.10.2010)

Date of mailing of the international search report
11 October 2010 (11.10.2010)

Name and mailing address of the ISA/FI
National Board of Patents and Registration of Finland
P.O. Box 1160, FI-00101 HELSINKI, Finland
Facsimile No. +358 9 6939 5328

Authorized officer
Jouko Berndtson
Telephone No. +358 9 6939 500

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI2010/050517

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SUNG-WOO T, et al., Modeling and Design of Notarial system supporting Secure Transactions in Electronic Commerce based on the Internet. INTERNATIONAL CONFERENCE ON INFORMATION NETWORKING [online], January 1998 [retrieved on 2010-10-05]. Retrieved from the Internet: <URL:http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=648389&userType=&tag=1>. Section 2	1-27

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/FI2010/050517

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
CN 101447999 A	03/06/2009	None	
US 2009044010 A1	12/02/2009	None	
US 2007022296 A1	25/01/2007	None	
EP 1228451 B1	07/08/2002	SE 0203745 A NO 20015975 A SE 0104066 A SE 518978 C2 WO 0133420 A1 GB 2367403 A ES 2211629T T3 EP 1383053 A2 DK 1228451T T3 DE 60007171T T2 DE 10084762T T0 CA 2409404 A1 CA 2376530 C AU 7977600 A AT 256314T T	16/12/2002 06/05/2002 22/01/2002 17/12/2002 10/05/2001 03/04/2002 16/07/2004 21/01/2004 08/03/2004 16/09/2004 16/01/2003 10/05/2001 10/12/2002 14/05/2001 15/12/2003

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2010/050517

CLASSIFICATION OF SUBJECT MATTER

Int.Cl.

H04L 9/32 (2006.01)

H04L 29/06 (2006.01)

G06F 21/00 (2006.01)