



(51) International Patent Classification:

G06F 21/33 (2013.01) H04L 29/06 (2006.01)
H04L 9/32 (2006.01)

(21) International Application Number:

PCT/EP2020/050669

(22) International Filing Date:

13 January 2020 (13.01.2020)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

201941002106 17 January 2019 (17.01.2019) IN

(71) Applicant: **NOKIA TECHNOLOGIES OY** [FI/FI];
Karakaari 7, 02610 Espoo (FI).

(72) Inventors: **AGARWAL, Vaibhav**; D1-503, Golden Palms
Apartment, K. Narayanapura, Kotanur Post, Off Hennur
Road, Bangalore 560077 (IN). **SINHA, Amit**; #10122,
Prestige Shantiniketan, ITPL Road, Bangalore 560048 (IN).
RANGANATHAN, Vidya; 80 Gokulam AICOBOO Na-
gar 18th main 2nd cross BTM 1st stage Bangalore, Karnata-
ka 560068 (IN). **SANTHIBHAVAN, Harikumar**; 376, 6th
Main, 1st Cross, NGEF Layout, Sadananda Nagar, Banga-
lore 560038 (IN). **RAJAGOPALAN, Nagaraj**; # 135, 4th
cross, AMS Layout, Vidhyaranyapura, Bangalore 560097
(IN).

(74) Agent: **NOKIA EPO REPRESENTATIVES**; Nokia
Technologies Oy, Karakaari 7, 02610 Espoo (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, BN, BR, BW, BY, BZ,
CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO,

(54) Title: NETWORK SECURITY

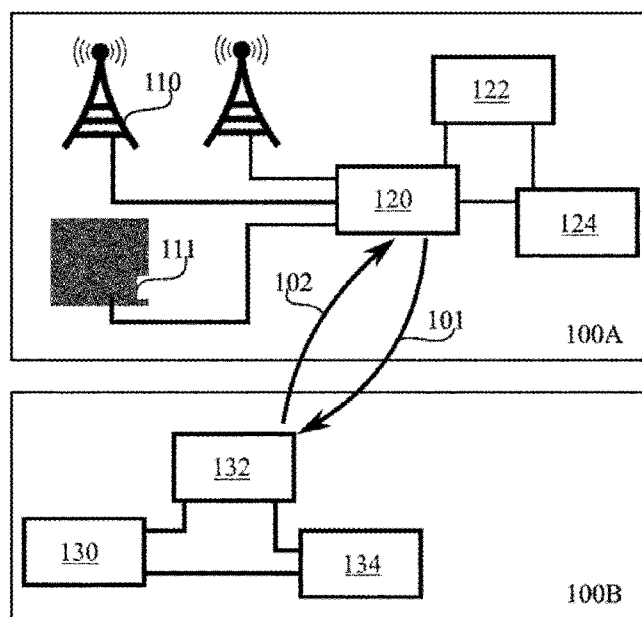


FIGURE 1

(57) Abstract: According to an example aspect of the present invention, there is provided an apparatus comprising at least one processing core, at least one memory including computer program code, the at least one memory and the computer program code being configured to, with the at least one processing core, cause the apparatus at least to process a request, received in the apparatus from a network end element, for a first network-level cryptographic certificate of the network end element, the request comprising a vendor-level cryptographic certificate of the network end element, request verification of the vendor-level cryptographic certificate from a node participating in a vendor-specific block chain, generate the first network-level cryptographic certificate responsive to the verification succeeding, and register the first network-level cryptographic certificate in a network-specific block chain the apparatus participates in.



DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

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

Published:

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

NETWORK SECURITY

FIELD

[0001] The present application generally relates to management of communication
5 networks, such as wireless communication networks.

BACKGROUND

[0002] Cryptographic certificates are used to establish trust between communicating parties. For example, a cryptographic certificate may comprise a public key of a party owning
10 the certificate, validity information and a cryptographic signature of a trusted party, such as a certificate authority. Since the trusted cryptographic signature covers the public key, a communicating party capable of verifying the signature of the trusted party may obtain a certain level of confidence the public key is indeed a key the party presenting the certificate claims it to be. An example certificate format is the X.509 format, which has been defined by
15 the International Telecommunication Union.

[0003] In communication networks, certificates may be used in establishing trust and protocol connections between various nodes comprised in the networks. Often, the cryptographic signatures in cryptographic certificates are those of certificate authorities, or are based via a chain of trust on signatures of certificate authorities.

20

SUMMARY

[0004] According to some example aspects, there is provided the subject-matter of the
25 independent claims. Some embodiments are defined in the dependent claims.

[0005] According to a first example aspect of the present invention, there is provided an apparatus comprising at least one processing core, at least one memory including computer program code, the at least one memory and the computer program code being configured to, with the at least one processing core, cause the apparatus at least to process a request,

received in the apparatus from a network end element, for a first network-level cryptographic certificate of the network end element, the request comprising a vendor-level cryptographic certificate of the network end element, request verification of the vendor-level cryptographic certificate from a node participating in a vendor-specific block chain, generate the first
5 network-level cryptographic certificate responsive to the verification succeeding, and register the first network-level cryptographic certificate in a network-specific block chain the apparatus participates in.

[0006] According to a second example aspect of the present invention, there is provided an apparatus comprising at least one processing core, at least one memory including computer
10 program code, the at least one memory and the computer program code being configured to, with the at least one processing core, cause the apparatus at least to transmit, to a node participating in a network-specific block chain, a request for a first network-level cryptographic certificate of the apparatus, the request comprising a vendor-level cryptographic certificate of the apparatus, and receive a response from the node participating
15 in the network-specific block chain, the response comprising the requested first network-level cryptographic certificate of the apparatus.

[0007] According to a third example aspect of the present invention, there is provided a method comprising processing a request, received in an apparatus from a network end element, for a first network-level cryptographic certificate of the network end element, the
20 request comprising a vendor-level cryptographic certificate of the network end element, requesting verification of the vendor-level cryptographic certificate from a node participating in a vendor-specific block chain, generating the first network-level cryptographic certificate responsive to the verification succeeding, and registering the first network-level cryptographic certificate in a network-specific block chain the apparatus participates in.

[0008] According to a fourth example aspect of the present invention, there is provided a method, comprising transmitting, to a node participating in a network-specific block chain, a
25 request for a first network-level cryptographic certificate of the apparatus, the request comprising a vendor-level cryptographic certificate of the apparatus, and receiving a response from the node participating in the network-specific block chain, the response comprising the
30 requested first network-level cryptographic certificate of the apparatus.

[0009] According to a fifth example aspect of the present invention, there is provided an apparatus comprising at least one processing core, at least one memory including computer
program code, the at least one memory and the computer program code being configured to,

with the at least one processing core, cause the apparatus at least to receive, from a node participating in a network-specific block chain, a request for verification of a vendor-level cryptographic certificate of a network end element, the request comprising a network-level cryptographic certificate of the network, verify the vendor-level cryptographic certificate with
5 reference to a vendor-specific block chain the apparatus participates in, and respond to the node participating in the network-specific block chain to indicate a result of the verification.

[0010] According to a sixth example aspect of the present invention, there is provided a method, comprising receiving, in an apparatus, from a node participating in a network-specific block chain, a request for verification of a vendor-level cryptographic certificate of a
10 network end element, the request comprising a network-level cryptographic certificate of the network. verifying the vendor-level cryptographic certificate with reference to a vendor-specific block chain the apparatus participates in, and responding to the node participating in the network-specific block chain to indicate a result of the verification.

[0011] According to a seventh example aspect of the present invention, there is
15 provided an apparatus comprising means for processing a request, received in an apparatus from a network end element, for a first network-level cryptographic certificate of the network end element, the request comprising a vendor-level cryptographic certificate of the network end element, means for requesting verification of the vendor-level cryptographic certificate from a node participating in a vendor-specific block chain, means for generating the first
20 network-level cryptographic certificate responsive to the verification succeeding, and means for registering the first network-level cryptographic certificate in a network-specific block chain the apparatus participates in.

[0012] According to an eighth example aspect of the present invention, there is
25 provided an apparatus comprising means for transmitting, to a node participating in a network-specific block chain, a request for a first network-level cryptographic certificate of the apparatus, the request comprising a vendor-level cryptographic certificate of the apparatus, and means for receiving a response from the node participating in the network-specific block chain, the response comprising the requested first network-level cryptographic certificate of the apparatus.

[0013] According to a ninth example aspect of the present invention, there is provided
30 an apparatus comprising means for receiving, from a node participating in a network-specific block chain, a request for verification of a vendor-level cryptographic certificate of a network end element, the request comprising a network-level cryptographic certificate of the network,

means for verifying the vendor-level cryptographic certificate with reference to a vendor-specific block chain the apparatus participates in, and means for responding to the node participating in the network-specific block chain to indicate a result of the verification.

[0014] According to a tenth example aspect of the present invention, there is provided a
5 non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least process a request, received in the apparatus from a network end element, for a first network-level cryptographic certificate of the network end element, the request comprising a vendor-level cryptographic certificate of the network end element, request verification of the vendor-
10 level cryptographic certificate from a node participating in a vendor-specific block chain, generate the first network-level cryptographic certificate responsive to the verification succeeding, and register the first network-level cryptographic certificate in a network-specific block chain the apparatus participates in.

[0015] According to an eleventh example aspect of the present invention, there is
15 provided a non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least transmit, to a node participating in a network-specific block chain, a request for a first network-level cryptographic certificate of the apparatus, the request comprising a vendor-level cryptographic certificate of the apparatus, and receive a response from the node
20 participating in the network-specific block chain, the response comprising the requested first network-level cryptographic certificate of the apparatus.

[0016] According to a twelfth example aspect of the present invention, there is provided a non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least
25 receive, from a node participating in a network-specific block chain, a request for verification of a vendor-level cryptographic certificate of a network end element, the request comprising a network-level cryptographic certificate of the network, verify the vendor-level cryptographic certificate with reference to a vendor-specific block chain the apparatus participates in, and respond to the node participating in the network-specific block chain to indicate a result of the
30 verification.

[0017] According to a thirteenth example aspect of the present invention, there is provided a computer program configured to cause a method in accordance with at least one of the third, fourth or sixth aspects to be performed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] FIGURE 1 illustrates an example system in accordance with at least some
5 embodiments of the present invention;

[0019] FIGURE 2 illustrates examples of vendor-specific and network-specific block
chains;

[0020] FIGURE 3 illustrates an example apparatus capable of supporting at least some
embodiments of the present invention;

10 [0021] FIGURE 4 illustrates signalling in accordance with at least some embodiments
of the present invention;

[0022] FIGURE 5 is a flow graph of a method in accordance with at least some
embodiments of the present invention;

[0023] FIGURE 6 is a flow graph of a method in accordance with at least some
15 embodiments of the present invention, and

[0024] FIGURE 7 is a flow graph of a method in accordance with at least some
embodiments of the present invention.

EMBODIMENTS

20

[0025] Reference to certificate authorities may be avoided in a network environment,
where certificates are registered in block chains. A certificate authority may present a point of
vulnerability, wherefore it may be desired to avoid their use and keep authentication in the
control of more involved parties. Vendors and network operators may each maintain separate
25 block chains which are used to register certificates used in the system. A network operator
may verify the correctness of a new network end element from a vendor block chain before
admitting the end element into the operator's network by registering its network-level
cryptographic certificate in a network-specific block chain.

[0026] FIGURE 1 illustrates an example system in accordance with at least some example embodiments of the present invention. The illustrated system includes an operator domain 100A and a vendor domain 100B. The operator domain comprises a communication network, and the operator domain may also be referred to as a network domain, or a network.

5 The example network illustrated in FIGURE 1 comprises a radio access network, which comprises base stations, such as base station 110, and access points, such as access point 111. In general, where a cellular technology is used, an end element may be referred to as a base station, and where a non-cellular technology is used, an end element may be referred to as an access point. An end element of a network is a network end element. The operator domain
10 further comprises network nodes, for example network nodes, 120, 122 and 124. These nodes may comprise core network nodes, such as serving gateways, S-GWs, mobility management entities, MMEs, core network servers and subscriber registers, for example.

[0027] Although illustrated as comprising base stations and access points in FIGURE 1, in other embodiments a network comprises simply either base stations or access points. In yet
15 further embodiments, a network may comprise, for example base stations configured to operate in accordance with more than one cellular communication technology. As such, a network may comprise separately first-technology base stations and second-technology base stations, or base stations supporting both the first and the second technology.

[0028] Examples of cellular communication technologies include long term evolution, LTE, and fifth generation, 5G. Examples of non-cellular communication technologies include
20 wireless local area network, WLAN, and worldwide interoperability for worldwide access, WiMAX.

[0029] The vendor domain 100B comprises vendor servers 130, 132 and 134. These servers, which may also be known as vendor nodes, may comprise, for example, production
25 management entities, registers or cloud service entities. The operator domain 100A and the vendor domain 100B are not, necessarily, integrated into a single network, but are enabled to exchange messages with each other, for example via at least one intermediate network, such as the Internet, for example. Vendor servers 130, 132, 134 are configured to maintain a block chain, which will herein be referred to as a vendor-specific block chain. The vendor-specific
30 block chain comprises blocks, the blocks comprising information on network elements manufactured by the vendor. Network elements may comprise network end elements, for example.

[0030] In general, blocks of a block chain are joined together by hashes, such that each block contains a hash of an immediately preceding block, enabling block-by-block verification of information stored in a block chain. In case an older block is modified, the hash of it in the succeeding block will not be correct, wherefore changing one block would
5 necessitate modifying hashes in each succeeding block to conceal the fact that a change was made.

[0031] In some block chains, a proof-of-work is used to make amending already established blocks more difficult. For example, it may be required that once the data for the block, known as transaction data, is ready, a nonce is sought, such that a hash over the entire
10 block, including the transaction data and the nonce, is in a target area of the hash function output space, the target area being a sub-space of the output space. Searching for the correct nonce thus includes re-deriving the hash value repeatedly with different nonce values, potentially millions of times. The nonce, or proof-of-work, is included in the block as it is established, locking the transaction data in place. Subsequently, modifying the block would
15 require re-obtaining a proof-of-work for all the subsequent blocks, which would require a large computational effort. The smaller is the target area of the hash function output space, the larger is the required computational effort. Nodes which establish blocks into a block chain are referred to as miner nodes.

[0032] In the system of FIGURE 1, vendor servers 130, 132, 134 are miner nodes of the
20 vendor-specific block chain. The transaction data in the vendor-specific block chain comprises vendor-level cryptographic certificates of network end elements produced by the vendor. For example, these vendor-level cryptographic certificates may comprise serial numbers, and at least one encryption key, associated with the manufactured end element. Vendor-level cryptographic certificates may comprise an indication that they are vendor-level
25 certificates. The at least one encryption key may comprise a vendor-associated public key of the end element. The end element may be provisioned with a copy of the vendor-level cryptographic certificate in connection with its manufacturer, wherefore this certificate will then be present in the vendor-specific block chain and in the newly manufactured network node. Vendor-level cryptographic certificates may be signed using a secret key of the vendor.
30 Vendor-level cryptographic certificates may be used in connection with installing new network elements, such as end elements, for example.

[0033] Vendor-level cryptographic certificates may be refused, for example by end elements and/or network nodes 120, 122, 124, if an attempt is made to use them in connection

with establishing a protocol connection, such as a transport layer security, TLS, connection, since network-level certificates are used for that purpose. Using a separate network-level cryptographic certificate provides the benefit that end elements are more specifically identified as members of a specific network, as opposed to merely being manufactured by a certain vendor.

[0034] In the system of FIGURE 1, network nodes, 120, 122 and 124 are miner nodes of an operator-specific block chain, also known as a network-specific block chain. Transaction data in the network-specific block chain comprises network-level cryptographic certificates of network nodes comprised in the network. The network-level cryptographic certificates may be used in establishing protocol connections and network configurations, for example. Network-level cryptographic certificates may comprise an indication that they are network-level certificates. Protocol connections may comprise transport layer security, TLS, connections, or intra-network protocol connections, for example. Once an end element or other network node has been admitted into the network, its network-level cryptographic certificate may be in the network-specific block chain and it may be presented toward other networks as a member of network domain 100A. The network-specific block chain will then agree to verify the network-level cryptographic certificate toward nodes in other networks, thus recognizing the new node also externally as being comprised in network domain 100A. Such recognition may comprise verifying and confirming, upon request, that the network-level cryptographic certificate end element or other network node is comprised in the transaction data of the network-specific block chain.

[0035] Once a network operator has chosen to furnish his network 100A with a new node, such as a new end element, the vendor may deliver the end element to the operator. Once the new end element is connected with nodes of network 100A, the new node may request a network-level cryptographic certificate, for example from server 120 or another server participating in the network-specific block chain.

[0036] The end element may identify itself to an operator node by taking its serial number and a timestamp, and signing this information with a secret key associated with its vendor-level cryptographic certificate. An operator node may further, or alternatively, provide a nonce to the end element for the end element to sign using this secret key, to verify the end element has been manufactured by the vendor it claims to be manufactured by. This identifying may take place in connection with the request for a network-level cryptographic certificate.

[0037] Responsive to the request for a network-level cryptographic certificate, the request comprising the vendor-level cryptographic certificate of the new end element, the node participating in the network-specific block chain may verify the vendor-level cryptographic certificate is authentic. This verification may comprise transmitting a verification request to a node participating in the vendor-specific block chain in vendor domain 100B. The verification request, illustrated as request 101 in FIGURE 1, may comprise the vendor-level cryptographic certificate.

[0038] In response to the verification request 101, the node participating in the vendor-specific block chain in vendor domain 100B may check, if the vendor-level cryptographic certificate is comprised in the vendor-specific block chain. If it is not recorded there, the end element in network 100A may be counterfeit, and the verification will fail. If on the other hand the vendor-level cryptographic certificate is recorded in the transaction data of the vendor-specific block chain, the node handling request 101 may respond by response 102, indicating the vendor-level cryptographic certificate is authentic. This provides the benefit, that trust in the authenticity of the new end element may be enhanced. A counterfeit end element may be corrupted with malicious software, potentially compromising availability of service, or even the confidentiality of information communicated via the end element. In some embodiments, response 102 may be issued also in case the verification does not succeed, that is, in case the vendor-level cryptographic certificate is not present in the transaction data of the vendor-specific block chain. In such cases, response 102 will indicate that the verification failed.

[0039] In some embodiments, the vendor-level cryptographic certificate comprises a hash of a firmware version installed in the end element, together with a cryptographic signature applied over the hash with the secret key of the vendor, to enable verifying the firmware of the end element has not been tampered with.

[0040] Responsive to the indication 102 that the vendor-level cryptographic certificate of the new end element is authentic, the node participating in the network-specific block chain may generate the requested network-level cryptographic certificate, register this certificate in the network-specific block chain and provide it to the new end element, which is thus registered into network domain 100A. A secret key may be generated in connection with generating the network-level cryptographic certificate, and this secret key may likewise be provided to the new end element. The secret key may be deleted from the generating node after it is provided to the new end element. The secret key is a secret key corresponding to a

network-associated public key of the new end element, this public key being comprised in the network-level cryptographic certificate. The end element may use the network-level certificate together with the associated secret key in establishing TLS sessions, for example.

[0041] A node participating in the network-specific block chain may be configured to generate, for the end element, a second network-level cryptographic certificate upon request. For example, the end element itself may request a new certificate to be generated, for example in case the previous one is facing expiry. Alternatively, the node participating in the network-specific block chain may generate the second certificate without a request, upon noticing the earlier certificate will soon expire. For example, smart contracts may be used to automatically generate new certificates. Smart contracts may also be used to automate authentication of network elements. A new key pair may be generated for the new certificate, but this is not mandatory as the earlier key pair may be re-used. The end element may specify in the request for a new certificate, whether it wants a new key pair. In case new keys are not generated, the end element may retain the earlier secret key and the public key in the new certificate will be the same one as was comprised in the earlier certificate. The new certificate is recorded in the transaction data of the network-specific block chain. In connection with generating the new certificate, the earlier one may be revoked. Revocation may comprise recording the certificate as revoked in transaction data of the network-specific block chain. Revocation may further comprise listing the revoked certificate in a revocation list, which may be disseminated in network 100A.

[0042] A node participating in the network-specific block chain may be configured to revoke a network-level cryptographic certificate upon request. Responsive to such a request, which may be received in the node from an operator station, for example, the network-specific block chain may be furnished with an indication in its transaction data that the certificate is revoked. For example, in case it transpires that the secret key associated with the certificate has been stolen, the certificate should be revoked and a new one generated for the end element. In some embodiments, the end element associated with a revoked network-level cryptographic certificate is disconnected from the network 100A responsive to the revocation.

[0043] In general, by participating in a block chain, it is meant the nodes so participating store a copy of the blocks of the block chain, and participate in establishing new blocks by determining the validity of the new blocks in terms of proof of work, where proof-of-work is used, and whether consensus is present more broadly.

[0044] FIGURE 2 illustrates examples of vendor-specific and network-specific block chains. In the upper part of the figure is illustrated an example vendor-specific block chain, wherein each block comprises a block identity, id, a timestamp when the block was established into the chain, a hash of the immediately preceding block, a nonce, such as a proof of work, and the transaction data of the block, including at least one vendor-level cryptographic certificate. As described above, a vendor-level cryptographic certificate may comprise at least one of: a serial number of the end element and a vendor-associated public key of the end element.

[0045] In the lower part of the figure is illustrated an example network-specific block chain, wherein each block comprises a block identity, id, a timestamp when the block was established into the chain, a hash of the immediately preceding block, a nonce, such as a proof of work, and the transaction data of the block, including at least one network-level cryptographic certificate. As described above, a network-level cryptographic certificate may comprise network-associated public key of the end element. Blocks of a network-specific block chain may also comprise a revocation list, indicating which network-level cryptographic certificates of the network have been revoked. A revocation list may comprise, for example, certificate identities of revoked certificates. Certificates in accordance with the X.509 standard, for example, comprise certificate identities in the form of serial numbers.

[0046] FIGURE 3 illustrates an example apparatus capable of supporting at least some embodiments of the present invention. Illustrated is device 300, which may comprise, for example, a node such as end element 110 operator node 120 or vendor node 132 of FIGURE 1, for example. Comprised in device 300 is processor 310, which may comprise, for example, a single- or multi-core processor wherein a single-core processor comprises one processing core and a multi-core processor comprises more than one processing core. Processor 310 may comprise, in general, a control device. Processor 310 may comprise more than one processor. Processor 310 may be a control device. A processing core may comprise, for example, a Cortex-A8 processing core manufactured by ARM Holdings or a Steamroller processing core designed by Advanced Micro Devices Corporation. Processor 310 may comprise at least one Qualcomm Snapdragon and/or Intel Xeon processor. Processor 310 may comprise at least one application-specific integrated circuit, ASIC. Processor 310 may comprise at least one field-programmable gate array, FPGA. Processor 310 may be means for performing method steps in device 300. Processor 310 may be configured, at least in part by computer instructions, to perform actions.

[0047] A processor may comprise circuitry, or be constituted as circuitry or circuitries, the circuitry or circuitries being configured to perform phases of methods in accordance with embodiments described herein. As used in this application, the term “circuitry” may refer to one or more or all of the following: (a) hardware-only circuit implementations, such as
5 implementations in only analog and/or digital circuitry, and (b) combinations of hardware circuits and software, such as, as applicable: (i) a combination of analog and/or digital hardware circuit(s) with software/firmware and (ii) any portions of hardware processor(s) with software (including digital signal processor(s)), software, and memory(ies) that work together to cause an apparatus, such as a server or end element, to perform various functions)
10 and (c) hardware circuit(s) and or processor(s), such as a microprocessor(s) or a portion of a microprocessor(s), that requires software (e.g., firmware) for operation, but the software may not be present when it is not needed for operation.

[0048] This definition of circuitry applies to all uses of this term in this application, including in any claims. As a further example, as used in this application, the term circuitry
15 also covers an implementation of merely a hardware circuit or processor (or multiple processors) or portion of a hardware circuit or processor and its (or their) accompanying software and/or firmware. The term circuitry also covers, for example and if applicable to the particular claim element, a baseband integrated circuit or processor integrated circuit for a mobile device or a similar integrated circuit in server, a cellular network device, or other
20 computing or network device.

[0049] Device 300 may comprise memory 320. Memory 320 may comprise random-access memory and/or permanent memory. Memory 320 may comprise at least one RAM chip. Memory 320 may comprise solid-state, magnetic, optical and/or holographic memory, for example. Memory 320 may be at least in part accessible to processor 310. Memory 320
25 may be at least in part comprised in processor 310. Memory 320 may be means for storing information. Memory 320 may comprise computer instructions that processor 310 is configured to execute. When computer instructions configured to cause processor 310 to perform certain actions are stored in memory 320, and device 300 overall is configured to run under the direction of processor 310 using computer instructions from memory 320, processor
30 310 and/or its at least one processing core may be considered to be configured to perform said certain actions. Memory 320 may be at least in part comprised in processor 310. Memory 320 may be at least in part external to device 300 but accessible to device 300.

[0050] Device 300 may comprise a transmitter 330. Device 300 may comprise a receiver 340. Transmitter 330 and receiver 340 may be configured to transmit and receive, respectively, information in accordance with at least one cellular or non-cellular standard. Transmitter 330 may comprise more than one transmitter. Receiver 340 may comprise more than one receiver. Transmitter 330 and/or receiver 340 may be configured to operate in accordance with global system for mobile communication, GSM, wideband code division multiple access, WCDMA, 5G, long term evolution, LTE, IS-95, wireless local area network, WLAN, Ethernet and/or worldwide interoperability for microwave access, WiMAX, standards, for example.

[0051] Device 300 may comprise a near-field communication, NFC, transceiver 350. NFC transceiver 350 may support at least one NFC technology, such as NFC, Bluetooth, Wibree or similar technologies.

[0052] Device 300 may comprise user interface, UI, 360. UI 360 may comprise at least one of a display, a keyboard, a touchscreen, a vibrator arranged to signal to a user by causing device 300 to vibrate, a speaker and a microphone. A user may be able to operate device 300 via UI 360, for example to configure device 300 to perform as part of a communication network.

[0053] Device 300 may comprise or be arranged to accept an identity module 370. Identity module 370 may comprise, for example, a smart card installable in device 300. An identity module 370 may comprise information comprising certificates of device 300. An identity module 370 may comprise cryptographic information usable to verify the identity of device 300 and/or to facilitate encryption of communicated information device 300 for communication effected via device 300.

[0054] Processor 310 may be furnished with a transmitter arranged to output information from processor 310, via electrical leads internal to device 300, to other devices comprised in device 300. Such a transmitter may comprise a serial bus transmitter arranged to, for example, output information via at least one electrical lead to memory 320 for storage therein. Alternatively to a serial bus, the transmitter may comprise a parallel bus transmitter. Likewise processor 310 may comprise a receiver arranged to receive information in processor 310, via electrical leads internal to device 300, from other devices comprised in device 300. Such a receiver may comprise a serial bus receiver arranged to, for example, receive information via at least one electrical lead from receiver 340 for processing in processor 310. Alternatively to a serial bus, the receiver may comprise a parallel bus receiver.

[0055] Device 300 may comprise further devices not illustrated in FIGURE 3. For example, where device 300 comprises a base station, it may comprise at least one back-up energy source. For example, some devices 300 may lack a NFC transceiver 350 and/or identity module 370.

5 [0056] Processor 310, memory 320, transmitter 330, receiver 340, NFC transceiver 350, UI 360 and/or identity module 370 may be interconnected by electrical leads internal to device 300 in a multitude of different ways. For example, each of the aforementioned devices may be separately connected to a master bus internal to device 300, to allow for the devices to exchange information. However, as the skilled person will appreciate, this is only one
10 example and depending on the embodiment various ways of interconnecting at least two of the aforementioned devices may be selected without departing from the scope of the present invention.

[0057] FIGURE 4 illustrates signalling in accordance with at least some embodiments of the present invention. On the vertical axes are disposed, on the left, end element 110 of
15 FIGURE 1, in the centre, operator node 120 of FIGURE 1 and on the right, vendor node 132 of FIGURE 1. Time advances from the top toward the bottom. Operator node 120 participates in the network-specific block chain and vendor node 132 participates in the vendor-specific block chain. FIGURE 4 comprises three distinct process flows, which will be described below.

20 [0058] Phases 410 – 418 form an initial registration flow. In phase 410, a new end element 110 requests a network-level cryptographic certificate from operator node 120, thus end element 110 also requests admission to the network of operator node 120. The request of phase 410 may comprise a vendor-level cryptographic certificate of end element 110.

[0059] Responsive to the request of phase 410, operator node 120 requests verification
25 of the vendor-level cryptographic certificate in the request of phase 410, by transmitting, phase 412, a verification request to the vendor, in particular to vendor node 132 which participates in the vendor-specific block chain. In phase 414, vendor node 132 indicates to operator node 120 whether the verification succeeded, that is, if the vendor-level cryptographic certificate is comprised in the transaction data of the vendor-specific block
30 chain in which vendor node 132 participates.

[0060] In case the verification of the vendor-level cryptographic certificate is successful, operator node 120 generates the requested network-level cryptographic certificate

in phase 416. This may comprise generation of a key pair of a public key cryptosystem, such as RSA or ElGamal, for example. The network-level cryptographic certificate is recorded in transaction data of the network-specific block chain in which operator node 120 participates.

[0061] In phase 418, the network-level cryptographic certificate is provided to end element 110. The associated secret key may likewise be provided to end element 110. End element 110 may then participate in protocol connections as a member of the network of operator node 120.

[0062] Phases 420 – 424 form a certificate renewal flow. In phase 420, end element 110 requests from operator node 120 a new network-level cryptographic certificate. For example, an earlier network-level cryptographic certificate of end element may be close to expiry. The request of phase 420 may comprise a copy of an earlier network-level cryptographic certificate, or, alternatively, it may comprise a timestamp or other information signed with a secret key associated with such an earlier certificate, to prove end element 110 is in possession of the secret key.

[0063] Responsive to the request, operator node 120 may verify the earlier certificate is in the network-specific block chain, and if so, generate, phase 422, the requested new certificate, as is described above. Where the request of phase 420 comprises the signed information, operator node 120 may use the copy of the earlier certificate in the network-specific block chain to verify the signature. In phase 424, the newly generated network-level cryptographic certificate is provided to end element 110.

[0064] Phases 430 – 436 form a certificate revocation flow. In phase 430, an operator station OP directs operator node 120 to revoke a network-level cryptographic certificate. The request of phase 430 may comprise an identifier, such as serial number, of the network-level cryptographic certificate to be revoked. The request of phase 430 may comprise a proof the operator station, or an operator of the operator station, is authorized to revoke certificates. For example, such proof may comprise information signed with a secret key of the operator station, or of the operator thereof.

[0065] In phase 432, operator node 120 inserts into the transaction data of the network-specific block chain an indication the certificate is revoked. This indication may be included in the next new block to be established into the block chain, since editing already established blocks is not possible.

[0066] Operator node 120 may, optionally, inform end element 110 that its network-level cryptographic certificate has been revoked, phase 434. Also other nodes in the network may be informed of the revocation, phase 436, for example by updating a disseminated revocation list of the network. Revocation may be beneficial in terms of, for example, ejecting a spoofed base station from a communication network.

[0067] In general, an end element 110 may receive its initial network-level cryptographic certificate from operator node 120, and request renewal of the network-level cryptographic certificate from any operator node participating in the network-specific block chain, it need not be the same one. Likewise, operator station OP may request revocation of a network-level cryptographic certificate of end element 110 from any node participating in the network-specific block chain, it need not be the same one as generated the certificate.

[0068] FIGURE 5 is a flow graph of a method in accordance with at least some embodiments of the present invention. The phases of the illustrated method may be performed in operator node 120, an auxiliary device or a personal computer, for example, or in a control device configured to control the functioning thereof, when installed therein.

[0069] Phase 510 comprises processing a request, received in an apparatus from a network end element, for a first network-level cryptographic certificate of the network end element, the request comprising a vendor-level cryptographic certificate of the network end element. Phase 520 comprises requesting verification of the vendor-level cryptographic certificate from a node participating in a vendor-specific block chain. Phase 530 comprises generating the first network-level cryptographic certificate responsive to the verification succeeding. Finally, phase 540 comprises registering the first network-level cryptographic certificate in a network-specific block chain the apparatus participates in.

[0070] FIGURE 6 is a flow graph of a method in accordance with at least some embodiments of the present invention. The phases of the illustrated method may be performed in end element 110, an auxiliary device or a personal computer, for example, or in a control device configured to control the functioning thereof, when installed therein.

[0071] Phase 610 comprises transmitting, to a node participating in a network-specific block chain, a request for a first network-level cryptographic certificate of the apparatus, the request comprising a vendor-level cryptographic certificate of the apparatus. Phase 620 comprises receiving a response from the node participating in the network-specific block

chain, the response comprising the requested first network-level cryptographic certificate of the apparatus.

[0072] FIGURE 7 is a flow graph of a method in accordance with at least some embodiments of the present invention. The phases of the illustrated method may be performed
5 in a vendor node, an auxiliary device or a personal computer, for example, or in a control device configured to control the functioning thereof, when installed therein

[0073] Phase 710 comprises receiving, in an apparatus, from a node participating in a network-specific block chain, a request for verification of a vendor-level cryptographic certificate of a network end element, the request comprising a network-level cryptographic
10 certificate of the network. Phase 720 comprises verifying the vendor-level cryptographic certificate with reference to a vendor-specific block chain the apparatus participates in. Finally, phase 730 comprises responding to the node participating in the network-specific block chain to indicate a result of the verification.

[0074] It is to be understood that the embodiments of the invention disclosed are not
15 limited to the particular structures, process steps, or materials disclosed herein, but are extended to equivalents thereof as would be recognized by those ordinarily skilled in the relevant arts. It should also be understood that terminology employed herein is used for the purpose of describing particular embodiments only and is not intended to be limiting.

[0075] Reference throughout this specification to one embodiment or an embodiment
20 means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, appearances of the phrases “in one embodiment” or “in an embodiment” in various places throughout this specification are not necessarily all referring to the same embodiment. Where reference is made to a numerical value using a term such as, for example, about or
25 substantially, the exact numerical value is also disclosed.

[0076] As used herein, a plurality of items, structural elements, compositional elements, and/or materials may be presented in a common list for convenience. However, these lists should be construed as though each member of the list is individually identified as a separate and unique member. Thus, no individual member of such list should be construed as a de
30 facto equivalent of any other member of the same list solely based on their presentation in a common group without indications to the contrary. In addition, various embodiments and examples of the present invention may be referred to herein along with alternatives for the various components thereof. It is understood that such embodiments, examples, and

alternatives are not to be construed as de facto equivalents of one another, but are to be considered as separate and autonomous representations of the present invention.

[0077] Furthermore, the described features, structures, or characteristics may be combined in any suitable manner in one or more embodiments. In the preceding description, numerous specific details are provided, such as examples of lengths, widths, shapes, etc., to provide a thorough understanding of embodiments of the invention. One skilled in the relevant art will recognize, however, that the invention can be practiced without one or more of the specific details, or with other methods, components, materials, etc. In other instances, well-known structures, materials, or operations are not shown or described in detail to avoid obscuring aspects of the invention.

[0078] While the forgoing examples are illustrative of the principles of the present invention in one or more particular applications, it will be apparent to those of ordinary skill in the art that numerous modifications in form, usage and details of implementation can be made without the exercise of inventive faculty, and without departing from the principles and concepts of the invention. Accordingly, it is not intended that the invention be limited, except as by the claims set forth below.

[0079] The verbs “to comprise” and “to include” are used in this document as open limitations that neither exclude nor require the existence of also un-recited features. The features recited in depending claims are mutually freely combinable unless otherwise explicitly stated. Furthermore, it is to be understood that the use of “a” or “an”, that is, a singular form, throughout this document does not exclude a plurality.

INDUSTRIAL APPLICABILITY

[0080] At least some embodiments of the present invention find industrial application in managing communication networks.

CLAIMS:

1. An apparatus comprising at least one processing core, at least one memory including
5 computer program code, the at least one memory and the computer program code being
configured to, with the at least one processing core, cause the apparatus at least to:
- process a request, received in the apparatus from a network end element, for a first
network-level cryptographic certificate of the network end element, the request
comprising a vendor-level cryptographic certificate of the network end element;
 - 10 – request verification of the vendor-level cryptographic certificate from a node
participating in a vendor-specific block chain;
 - generate the first network-level cryptographic certificate responsive to the
verification succeeding, and
 - register the first network-level cryptographic certificate in a network-specific block
15 chain the apparatus participates in.
2. The apparatus according to claim 1, wherein the network end element comprises a
cellular base station, a non-cellular access point or a base station controller node.
- 20 3. The apparatus according to claim 1 or 2, wherein the first network-level cryptographic
certificate comprises a network-associated public key of the network end element.
4. The apparatus according to any of claims 1 - 3, wherein the vendor-level cryptographic
25 certificate comprises a vendor-associated public key of the network end element.
5. The apparatus according to any of claims 1 – 4, wherein the apparatus is configured to
process, with reference to the network-specific block chain, a request to verify the first
network-level cryptographic certificate of the network end element.
- 30 6. The apparatus according to any of claims 1 – 5, wherein the apparatus is configured to
generate a second network-level cryptographic certificate for the network end element

responsive to a request, from the network end element, the request comprising the first network-level cryptographic certificate.

7. The apparatus according to any of claims 1 – 6, wherein the apparatus is further
5 configured to receive a request to revoke the first network-level cryptographic certificate of the network end element, and responsive to the request to revoke, to update the network-specific block chain to indicate that the first network-level cryptographic certificate of the network end element is revoked.
- 10 8. The apparatus according to claim 7, wherein the apparatus is further configured to update a revocation list with information indicating the first network-level cryptographic certificate of the network end element is revoked.
9. The apparatus according to claim 8, wherein the apparatus is further configured to
15 transmit the revocation list to plural network nodes of a network in which the apparatus is comprised.
10. The apparatus according to any of claims 7 – 9, wherein the apparatus is further configured to, responsive to revocation of the first network-level cryptographic certificate
20 of the network end element, cause disconnection of the network end element.
11. An apparatus comprising at least one processing core, at least one memory including computer program code, the at least one memory and the computer program code being configured to, with the at least one processing core, cause the apparatus at least to:
- 25 – transmit, to a node participating in a network-specific block chain, a request for a first network-level cryptographic certificate of the apparatus, the request comprising a vendor-level cryptographic certificate of the apparatus, and
- receive a response from the node participating in the network-specific block chain, the response comprising the requested first network-level cryptographic certificate
30 of the apparatus.
12. A method comprising:

- processing a request, received in an apparatus from a network end element, for a first network-level cryptographic certificate of the network end element, the request comprising a vendor-level cryptographic certificate of the network end element;
- requesting verification of the vendor-level cryptographic certificate from a node participating in a vendor-specific block chain;
- generating the first network-level cryptographic certificate responsive to the verification succeeding, and
- registering the first network-level cryptographic certificate in a network-specific block chain the apparatus participates in.

10

13. The method according to claim 12, wherein the network end element comprises a cellular base station, a non-cellular access point or a base station controller node.

14. The method according to claim 12 or 13, wherein the first network-level cryptographic certificate comprises a network-associated public key of the network end element.

15. The method according to any of claims 12 - 14, wherein the vendor-level cryptographic certificate comprises a vendor-associated public key of the network end element.

16. The method according to any of claims 12 – 15, further comprising processing, with reference to the network-specific block chain, a request to verify the first network-level cryptographic certificate of the network end element.

17. The method according to any of claims 12 – 16, further comprising generating a second network-level cryptographic certificate for the network end element responsive to a request, from the network end element, the request comprising the first network-level cryptographic certificate.

18. The method according to any of claims 12 – 17, further comprising receiving a request to revoke the first network-level cryptographic certificate of the network end element, and responsive to the request to revoke, updating the network-specific block chain to indicate that the first network-level cryptographic certificate of the network end element is revoked.

19. The method according to claim 18, further comprising updating a revocation list with information indicating the first network-level cryptographic certificate of the network end element is revoked.
- 5 20. The method according to claim 19, further comprising transmitting the revocation list to plural network nodes of a network in which the apparatus is comprised.
21. The method according to any of claims 18 – 20, further comprising, responsive to revocation of the first network-level cryptographic certificate of the network end element,
10 causing disconnection of the network end element
22. A method, comprising:
- transmitting, to a node participating in a network-specific block chain, a request for a first network-level cryptographic certificate of the apparatus, the request
15 comprising a vendor-level cryptographic certificate of the apparatus, and
 - receiving a response from the node participating in the network-specific block chain, the response comprising the requested first network-level cryptographic certificate of the apparatus.
- 20 23. An apparatus comprising at least one processing core, at least one memory including computer program code, the at least one memory and the computer program code being configured to, with the at least one processing core, cause the apparatus at least to:
- receive, from a node participating in a network-specific block chain, a request for verification of a vendor-level cryptographic certificate of a network end element,
25 the request comprising a network-level cryptographic certificate of the network;
 - verify the vendor-level cryptographic certificate with reference to a vendor-specific block chain the apparatus participates in, and
 - respond to the node participating in the network-specific block chain to indicate a result of the verification.
- 30
24. A method, comprising:
- receiving, in an apparatus, from a node participating in a network-specific block chain, a request for verification of a vendor-level cryptographic certificate of a

network end element, the request comprising a network-level cryptographic certificate of the network;

- verifying the vendor-level cryptographic certificate with reference to a vendor-specific block chain the apparatus participates in, and
- 5 – responding to the node participating in the network-specific block chain to indicate a result of the verification.

25. An apparatus comprising:

- 10 – means for processing a request, received in an apparatus from a network end element, for a first network-level cryptographic certificate of the network end element, the request comprising a vendor-level cryptographic certificate of the network end element;
- means for requesting verification of the vendor-level cryptographic certificate from a node participating in a vendor-specific block chain;
- 15 – means for generating the first network-level cryptographic certificate responsive to the verification succeeding, and
- means for registering the first network-level cryptographic certificate in a network-specific block chain the apparatus participates in.

20 26. An apparatus comprising:

- means for transmitting, to a node participating in a network-specific block chain, a request for a first network-level cryptographic certificate of the apparatus, the request comprising a vendor-level cryptographic certificate of the apparatus, and
- means for receiving a response from the node participating in the network-specific
- 25 block chain, the response comprising the requested first network-level cryptographic certificate of the apparatus.

27. An apparatus comprising:

- 30 – means for receiving, from a node participating in a network-specific block chain, a request for verification of a vendor-level cryptographic certificate of a network end element, the request comprising a network-level cryptographic certificate of the network;

- means for verifying the vendor-level cryptographic certificate with reference to a vendor-specific block chain the apparatus participates in, and
- means for responding to the node participating in the network-specific block chain to indicate a result of the verification.

5

28. A non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least:

- process a request, received in the apparatus from a network end element, for a first network-level cryptographic certificate of the network end element, the request comprising a vendor-level cryptographic certificate of the network end element;
- request verification of the vendor-level cryptographic certificate from a node participating in a vendor-specific block chain;
- generate the first network-level cryptographic certificate responsive to the verification succeeding, and
- register the first network-level cryptographic certificate in a network-specific block chain the apparatus participates in.

10

15

29. A non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least:

- transmit, to a node participating in a network-specific block chain, a request for a first network-level cryptographic certificate of the apparatus, the request comprising a vendor-level cryptographic certificate of the apparatus, and
- receive a response from the node participating in the network-specific block chain, the response comprising the requested first network-level cryptographic certificate of the apparatus.

25

30. A non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least:

30

- receive, from a node participating in a network-specific block chain, a request for verification of a vendor-level cryptographic certificate of a network end element, the request comprising a network-level cryptographic certificate of the network;
- verify the vendor-level cryptographic certificate with reference to a vendor-specific
5 block chain the apparatus participates in, and
- respond to the node participating in the network-specific block chain to indicate a result of the verification.

31. A computer program configured to cause a method in accordance with at least one of
10 claims 12 – 21, 22 or 24 to be performed.

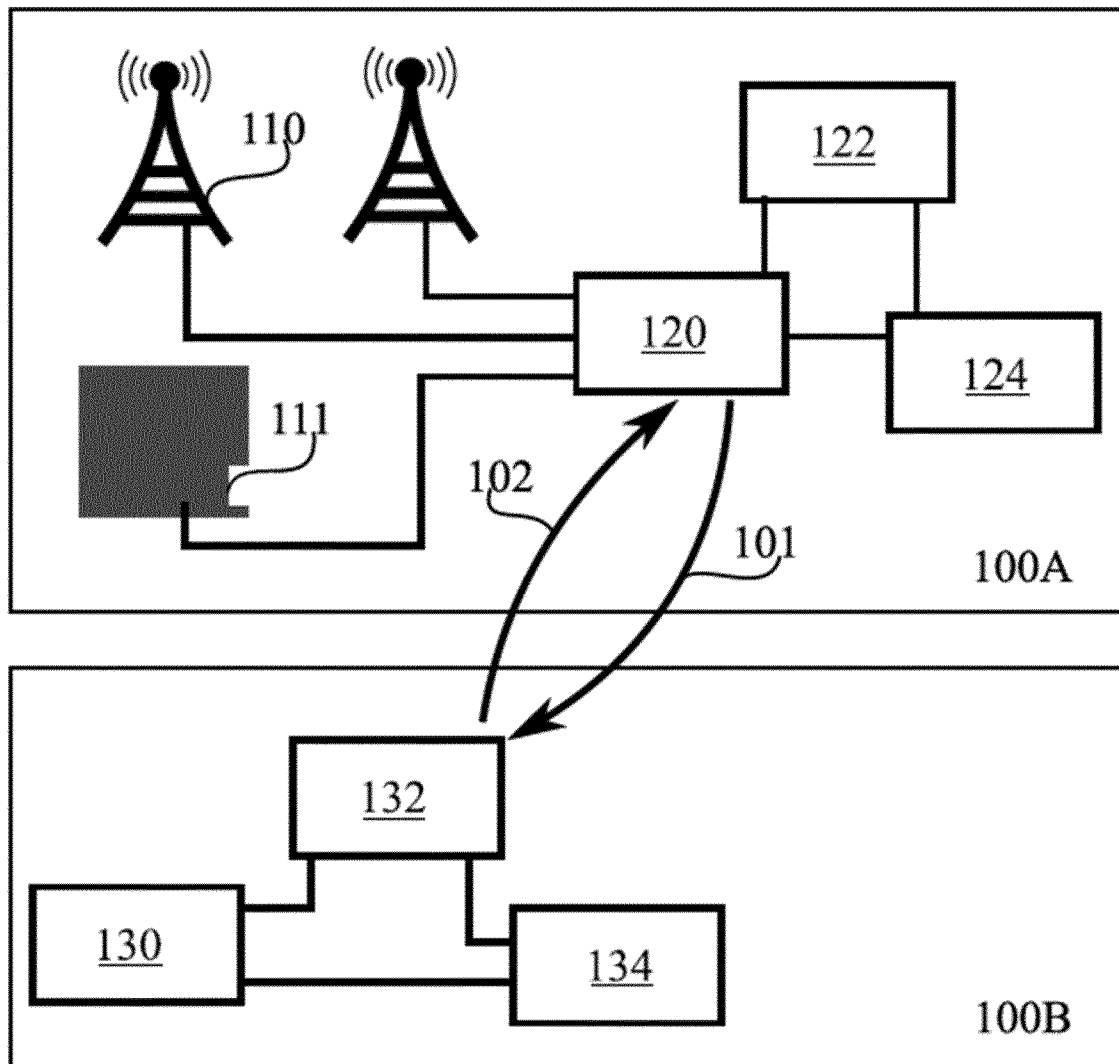
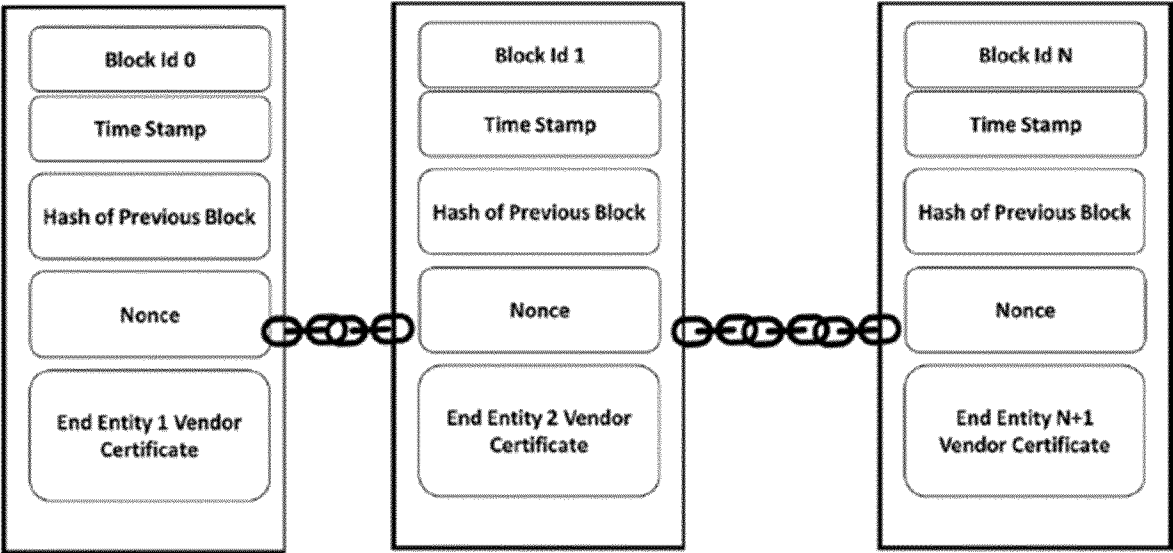


FIGURE 1

Sample Block Chain at Vendor Miner



Sample Block Chain at Operator Miner

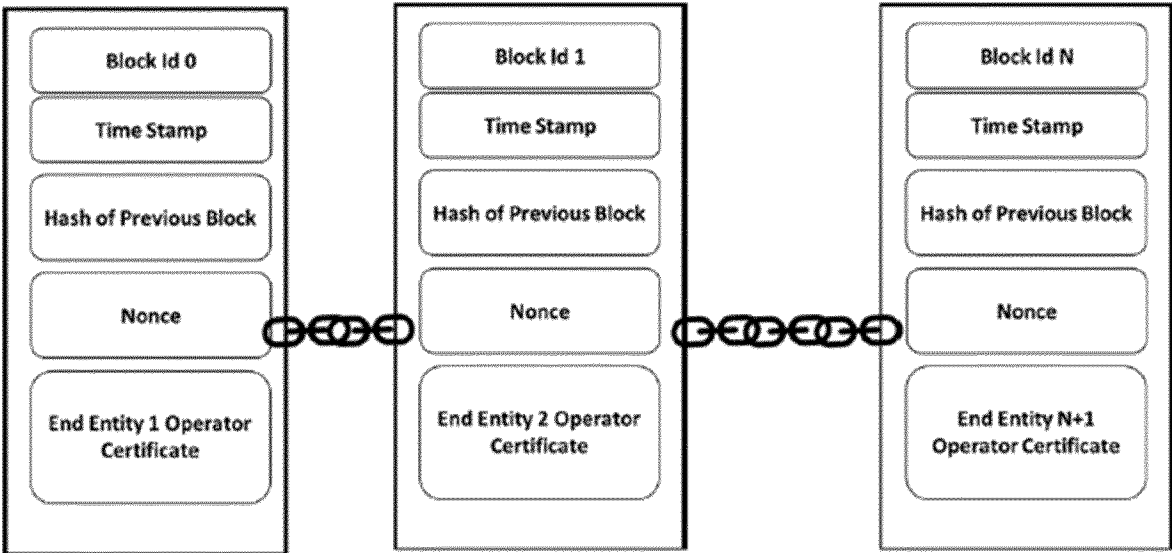


FIGURE 2

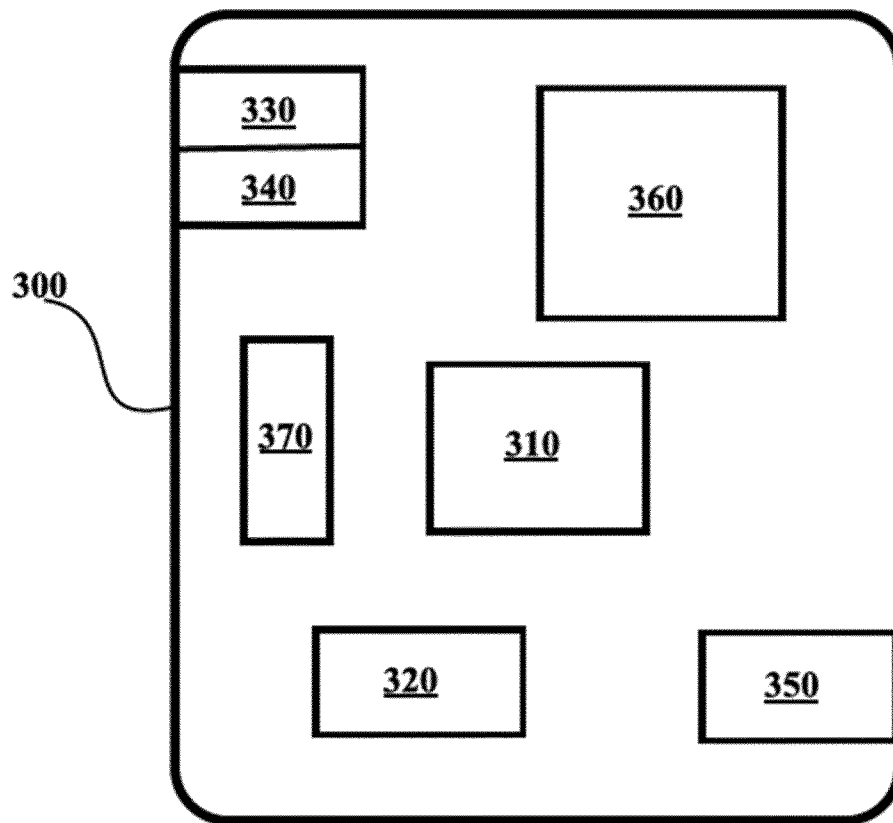


FIGURE 3

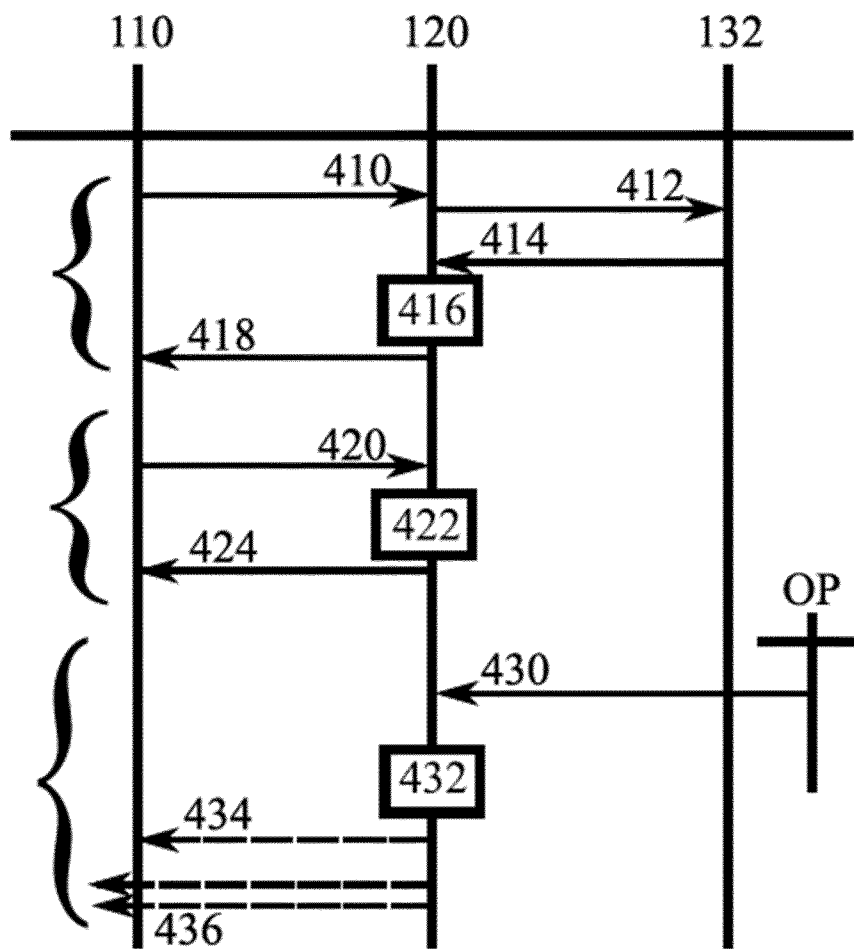


FIGURE 4

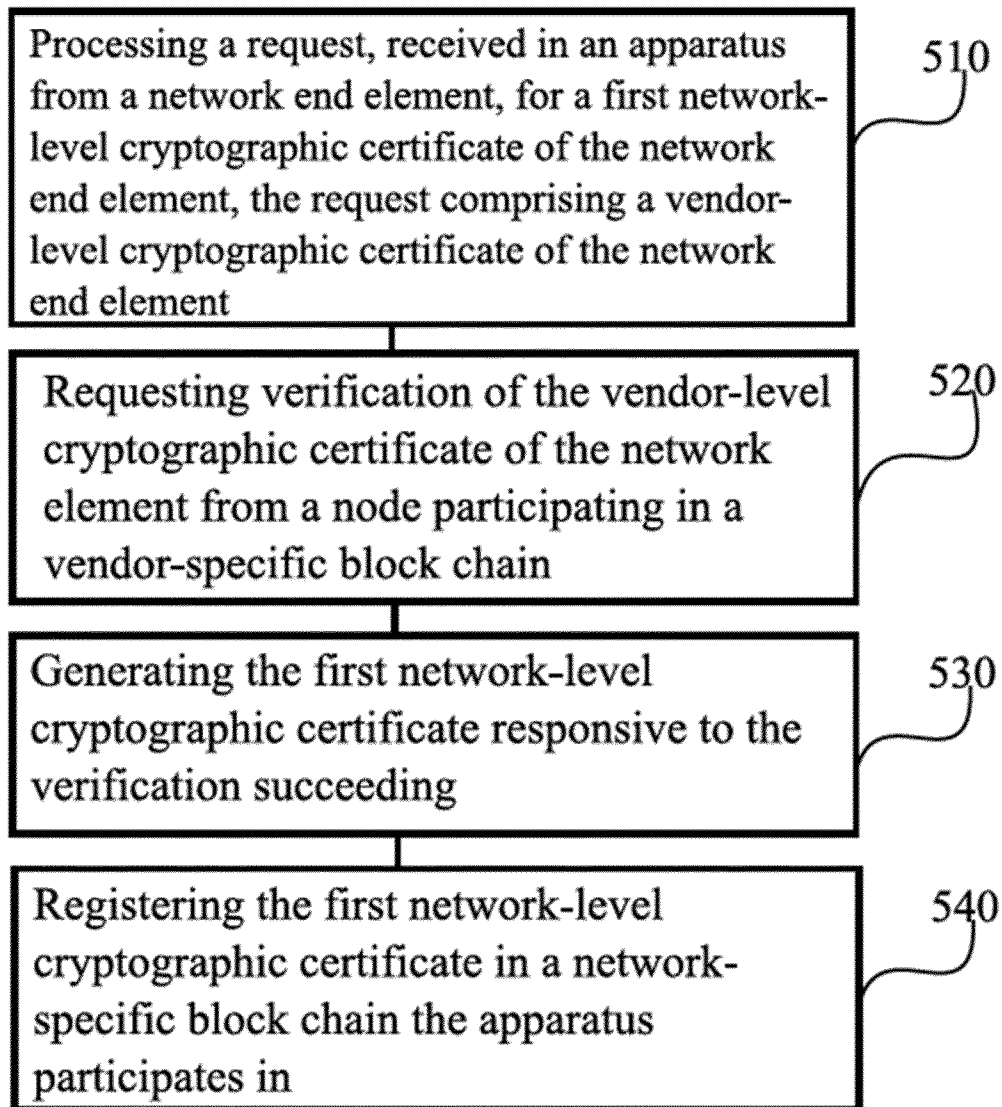


FIGURE 5

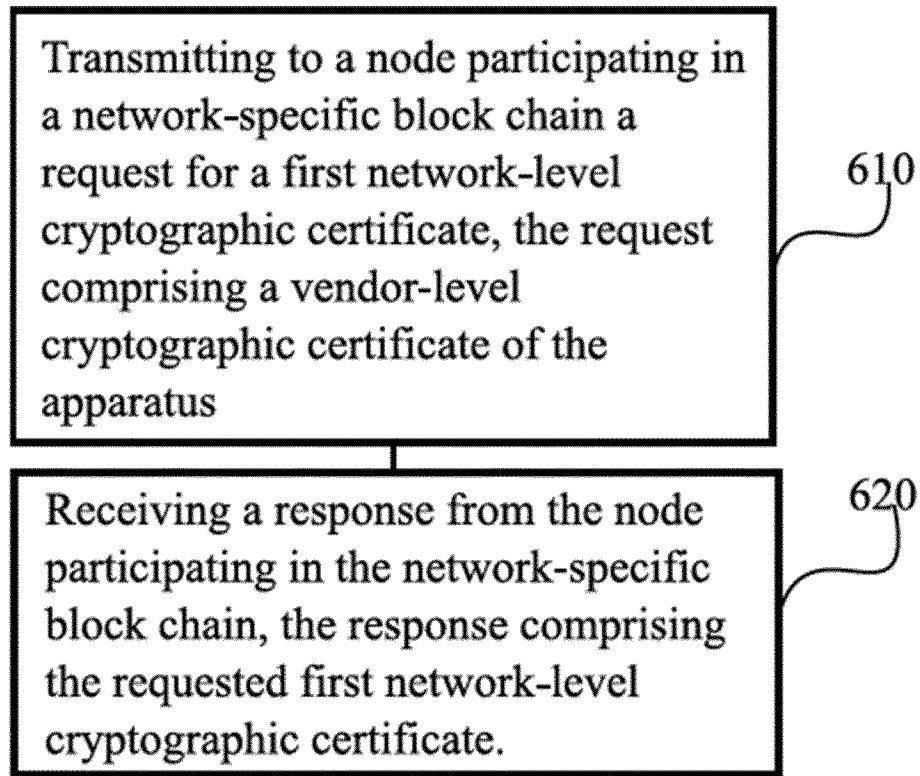


FIGURE 6

7/7

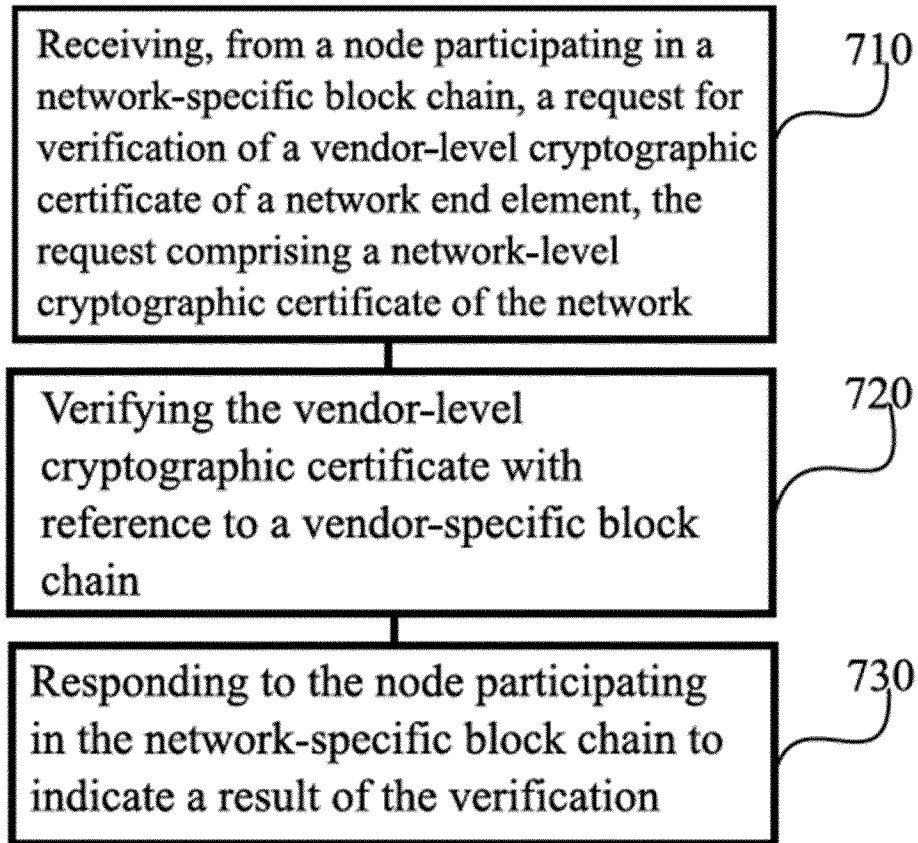


FIGURE 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2020/050669

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/33 H04L9/32 H04L29/06
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KONSTANTIN SHEMYAK ET AL: "Secure Delivery of Equipment Identity from Vendor to Operator", NEW TECHNOLOGIES, MOBILITY AND SECURITY (NTMS), 2011 4TH IFIP INTERNATIONAL CONFERENCE ON, IEEE, 7 February 2011 (2011-02-07), pages 1-5, XP031982199, DOI: 10.1109/NTMS.2011.5720591 ISBN: 978-1-4244-8705-9 page 3 - page 4 ----- -/--	1-31



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

26 March 2020

Date of mailing of the international search report

06/04/2020

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Mäenpää, Jari

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2020/050669

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	YAKUBOV ALEXANDER ET AL: "A blockchain-based PKI management framework", NOMS 2018 - 2018 IEEE/IFIP NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM, IEEE, 23 April 2018 (2018-04-23), pages 1-6, XP033374063, DOI: 10.1109/NOMS.2018.8406325 [retrieved on 2018-07-06] page 3 - page 4 -----	1-31
A	WO 2017/194815 A1 (NOKIA TECHNOLOGIES OY [FI]) 16 November 2017 (2017-11-16) paragraph [0026] - paragraph [0068] -----	1-31
A	US 2015/264040 A1 (SCHNEIDER PETER [DE]) 17 September 2015 (2015-09-17) the whole document -----	1-31

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2020/050669

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2017194815 A1	16-11-2017	CN 109314635 A EP 3455996 A1 US 2019139047 A1 WO 2017194815 A1	05-02-2019 20-03-2019 09-05-2019 16-11-2017
US 2015264040 A1	17-09-2015	CN 104704789 A EP 2907287 A1 US 2015264040 A1 WO 2014060013 A1	10-06-2015 19-08-2015 17-09-2015 24-04-2014