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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 June 2017 (08.06.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/093597 A1

(51) International Patent Classification:
G07C 9/00 (2006.01) *G06F 21/45* (2013.01)
H04L 9/32 (2006.01) *H04W 12/08* (2009.01)

(21) International Application Number:
PCT/FI2015/050852

(22) International Filing Date:
3 December 2015 (03.12.2015)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **NOKIA TECHNOLOGIES OY** [FI/FI]; Karaportti 3, 02610 Espoo (FI).

(72) Inventors: **KOSKIMIES, Olli Oskari**; Varjakanvalkama 16 E, 00950 Helsinki (FI). **MIKOLA, Timo Tapani**; Hirvikatu 18, 33240 Tampere (FI). **BLANTS, Lioudmila Lucy**; Säynävätie 14 B 10, 02170 Espoo (FI).

(74) Agent: **SEPPO LAINE OY**; Itämerenkatu 3 B, 00180 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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, 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).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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

(54) Title: ACCESS MANAGEMENT

(57) Abstract: According to an example aspect of the present invention, there is provided an apparatus comprising a memory configured to store an encryption key and a list of access tokens and at least one processing core configured to select a first access token from the list of access tokens based, at least partly, on at least one of a current time and a sequence number, decide, based at least partly on the first access token, whether to grant a user device access to the apparatus, and cause the apparatus to receive a second list of access tokens from at least one of the user device and a second user device.

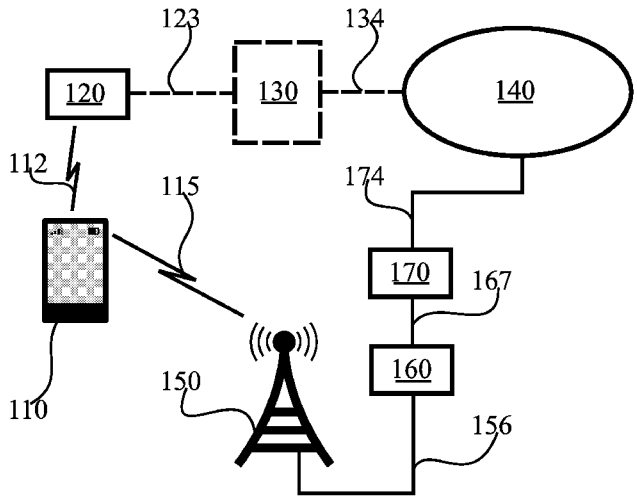

FIGURE 1

WO 2017/093597 A1

ACCESS MANAGEMENT

FIELD

[0001] The present invention relates to the field of managing access to devices using access tokens.

BACKGROUND

[0002] When a user device attempts to access an apparatus that is access controlled, the user device may be requested to provide a credential to prove it, or the user, is authorized to access the apparatus. For example, where the apparatus being accessed is an electronic lock controller, the user device needs to be in possession of a key, which may comprise a cryptographic token, for example, to present to the apparatus to cause access to be granted.

[0003] A credential may be static, in that it remains constant over time, or the access controlled apparatus may be arranged to receive new credentials, for example periodically, over a fixed network connection. An advantage of changing credentials is that on case a single credential is compromised, an unauthorized party cannot gain permanent access to the access controlled device.

[0004] In an Internet of Things, IoT, setting, an access controlled apparatus may be arranged to periodically, or on request once credentials are used up, request for new credentials via a suitable fixed gateway, for example. Credentials may comprise access tokens, wherein a user device may be provided with an access token that matches an access token in the access controlled apparatus. For example, the access token may comprise a shared secret that is usable in establishing a cryptographic protocol connection between the user device and the access controlled apparatus. The access token may be usable in authenticating the user device and/or access controlled apparatus, for example.

[0005] Connections between user devices and access controlled apparatuses may be implemented as wire-line or wireless connections, such as, for example, universal serial

bus, USB, connections, wireless local area network, WLAN, or Bluetooth connections, as is convenient and depending on the implementation in question.

[0006] Examples of access controlled devices may comprise, in addition to electronic lock controllers, laboratory equipment, medical equipment, cars, bicycles, motorcycles, personal appliances such as washing machines, industrial machinery, industrial process controllers, and commercial or residential machinery.

SUMMARY OF THE INVENTION

[0007] The invention is defined by the features of the independent claims. Some specific embodiments are defined in the dependent claims.

[0008] According to a first aspect of the present invention, there is provided an apparatus comprising a memory configured to store an encryption key and a list of access tokens and at least one processing core configured to select a first access token from the list of access tokens based, at least partly, on at least one of a current time and a sequence number, decide, based at least partly on the first access token, whether to grant a user device access to the apparatus, and cause the apparatus to receive a second list of access tokens from at least one of the user device and a second user device.

[0009] Various embodiments of the first aspect may comprise at least one feature from the following bulleted list:

- the at least one processing core is configured to cause the apparatus to receive the second list of access tokens over a short-range wireless interface
- the short-range wireless interface comprises a Bluetooth interface
- the memory is configured to store a plurality of lists of access tokens, each list of access tokens comprising access tokens that are usable in obtaining a different level of access to the apparatus
- each list corresponds to a distinct role a user may assume with respect to the apparatus

- the at least one processing core is configured to select the first access token based at least partly on the current time, each access token being associated with a validity time interval
- the at least one processing core is configured to select the first access token based at least partly on the sequence number by allowing each access token to be used a set number of times
- the at least one processing core is configured to select the first access token based at least partly on the sequence number, wherein each access token is enabled for a preconfigured time duration, after which the sequence number used is incremented
- the at least one processing core is configured to cause the apparatus to advertise at least one of the current time and the sequence number
- the at least one processing core is configured to cause the apparatus to decrypt the second list of access tokens, using the encryption key, and to authenticate the second list of access tokens based at least partly based on a result of the decrypting.

[0010] According to a second 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 obtain a list of access tokens, process information, the information comprising at least one of a sequence number and a current time indication, and select, based at least partly on the at least one of the sequence number and the current time indication, a first access token from the list of access tokens and establish a connection with a first device based at least partly on the first access token.

[0011] Various embodiments of the second aspect may comprise at least one feature from the following bulleted list:

- the at least one memory and the computer program code are configured to, with the at least one processing core, cause the apparatus to select the first access token based at least partly on the current time, each access token being associated with a validity time interval
- the at least one memory and the computer program code are configured to, with the at least one processing core, cause the apparatus to select the first access token

based at least partly on the sequence number, each access token being allowed to be used a set number of times

- the at least one memory and the computer program code are configured to, with the at least one processing core, cause the apparatus to select the first access token based at least partly on the sequence number, wherein each access token is enabled for a preconfigured time duration, after which the sequence number used is incremented
- the at least one memory and the computer program code are configured to, with the at least one processing core, cause the apparatus to obtain a second list of access tokens, and to provide the second list of access tokens to the first device.

[0012] According to a third aspect of the present invention, there is provided a method comprising storing an encryption key and a list of access tokens, selecting a first access token from the list of access tokens based, at least partly, on at least one of a current time and a sequence number, deciding, based at least partly on the first access token, whether to grant a user device access to an apparatus, and causing the apparatus to receive a second list of access tokens from at least one of the user device and a second user device.

[0013] Various embodiments of the third aspect may comprise at least one feature corresponding to a feature from the preceding bulleted list laid out in connection with the first aspect.

[0014] According to a fourth aspect of the present invention, there is provided a method comprising obtaining a list of access tokens, processing information, the information comprising at least one of a sequence number and a current time indication, and selecting, based at least partly on the at least one of the sequence number and the current time indication, a first access token from the list of access tokens and establishing a connection with a first device based at least partly on the first access token.

[0015] Various embodiments of the fourth aspect may comprise at least one feature corresponding to a feature from the preceding bulleted list laid out in connection with the second aspect.

[0016] According to a fifth aspect of the present invention, there is provided an apparatus comprising means for storing an encryption key and a list of access tokens, means for selecting a first access token from the list of access tokens based, at least partly, on at least one of a current time and a sequence number, means for deciding, based at least

partly on the first access token, whether to grant a user device access to an apparatus, and means for causing the apparatus to receive a second list of access tokens from at least one of the user device and a second user device.

[0017] According to a sixth aspect of the present invention, there is provided an apparatus comprising means for obtaining a list of access tokens, means for processing an advertisement originating in a first device, the advertisement comprising at least one of a sequence number and a current time indication, and means for selecting, based at least partly on the at least one of the sequence number and the current time indication, a first access token from the list of access tokens, and for establishing a connection with the first device based at least partly on the first access token.

[0018] According to a seventh 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 store an encryption key and a list of access tokens, select a first access token from the list of access tokens based, at least partly, on at least one of a current time and a sequence number, decide, based at least partly on the first access token, whether to grant a user device access to an apparatus, and cause the apparatus to receive a second list of access tokens from at least one of the user device and a second user device.

[0019] According to an eighth 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 obtain a list of access tokens, process an advertisement originating in a first device, the advertisement comprising at least one of a sequence number and a current time indication, and select, based at least partly on the at least one of the sequence number and the current time indication, a first access token from the list of access tokens and establish a connection with the first device based at least partly on the first access token.

[0020] According to a ninth aspect of the present invention, there is provided a computer program configured to cause a method in accordance with at least one of the second and third aspects to be performed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] FIGURE 1 illustrates a system in accordance with at least some embodiments of the present invention;

[0022] FIGURE 2 illustrates a system in accordance with at least some embodiments of the present invention;

[0023] FIGURE 3 illustrates an example apparatus capable of supporting at least some embodiments of the present invention, and

[0024] FIGURE 4 illustrates signalling in accordance with at least some embodiments of the present invention;

[0025] FIGURE 5 is a first flow graph of a first method in accordance with at least some embodiments of the present invention, and

[0026] FIGURE 6 is a second flow graph of a second method in accordance with at least some embodiments of the present invention.

EMBODIMENTS

[0027] By receiving access tokens from an access service via a user device, as opposed to via a gateway, an advantage may be obtained in that an access controlled device may be made simpler in that there may no longer be a need to equip the access controlled device with a distinct communications capability toward the gateway. Examples of access controlled devices and user devices are provided here in below.

[0028] FIGURE 1 illustrates a system in accordance with at least some embodiments of the present invention. The system comprises an access controlled device 120, which may comprise, for example, an IoT device or another kind of access controlled device, such as, for example, a medical patient information repository or controller thereof. Access controlled device 120 may comprise a processing core and memory, and may be powered by a stable power source or, for example, by a rechargeable battery. For example, access controlled device 120 may comprise a personal, wearable and/or embedded device. Access controlled device 120 may be configured to collect sensor data and/or actuate further devices, such as, for example, a door. Access controlled device 120 may be accessible in

different roles, such that where access controlled device 120 comprises a patient information repository, for example, a doctor may have broader access to information contained therein than a nurse, with the nurse having narrower access. Broader access may comprise, for example, authority to modify treatment plans, while narrower access may comprise authority to view treatment plans. Access controlled device 120 may lack a fixed connection.

[0029] User device 110 may comprise, for example, a mobile phone, smartphone, tablet device, laptop computer or other suitable device. User device 110 may be used to access access controlled device 120, for example via connection 112. Connection 112 may comprise a wire-line connection, or, as illustrated, a wireless connection. Connection 112 may comprise a USB, WLAN or Bluetooth connection, for example.

[0030] User device 110 may be configured to access access controlled device 120 via connection 112. Access controlled device 120 may be configured to verify user device 110 is authorized to access it, wherein such verifying may comprise employing cryptographic information. In general, such cryptographic information may be referred to as an access token. For successful verification, user device 110 and access controlled device 120 may, in some embodiments, be required to have matching access tokens. Matching access tokens may comprise the same cryptographic information, or cryptographic information that is not the same, but compatible. Where the cryptographic information is the same, it may comprise a shared secret. Where the cryptographic information is not the same, it may comprise, for example, a public key on the one hand and a private key on the other hand, of a public key-private key pair in a public key cryptographic system.

[0031] User device 110 may select an access token to use in dependence of information received in user device 110 from access controlled device 120. The information may be received from a broadcast sent by access controlled device 120, or by querying and responsively receiving the information, for example. A broadcast may comprise a transmission that is not addressed to any node in particular. A broadcast may be wireless, for example over a Bluetooth interface. A Bluetooth broadcast may comprise a Bluetooth advertising packet. Access controlled device 120 may select a corresponding access token, in accordance with the information. Alternatively to selecting access tokens based on information originating in access controlled device 120, both access controlled

device 120 and user device 110 may select their access tokens based on information that is available to both devices. An example of such information available to both devices is a clock signal.

[0032] User device 110 may select an address for itself for communicating with access controlled device 120. For example, user device 110 may select a resolvable private device address so that a user device 110 identity perceived by the access controlled device is consistent with an encryption key used when communicating over connection 112. An example of such a key is an identity resolving key, which may be comprised in the access token used. A role user device 110 assumes toward access controlled device 120 may determine which access token, encryption key and thus address user device 110 takes into use toward access controlled device 120.

[0033] Access controlled device 120 may store lists of access tokens, each list comprising access tokens usable in accessing access controlled device 120 in a corresponding role. In other words, access controlled device 120 may have a first list of access tokens configured to grant a first kind of access, corresponding to a first role, and access controlled device 120 may have a second list of access tokens configured to grant a second kind of access, corresponding to a second role. In other words, when access controlled device 120 is accessed using an access token from the first list, access controlled device 120 may grant the first kind of access, corresponding to the first role. For example, a nurse may request access to a medical information store using an access token associated with a nurse role, and he would responsively be granted nurse-role access.

[0034] Access tokens may be configured to be usable for a finite number of times, and/or for a finite length of time. In case an access token was static, that is, permanent, then a stolen access token could be used to provide permanent unauthorised access to the access controlled device. Therefore changing the access tokens from time to time increases the security level of the access controlled device.

[0035] An access service 140, which may be disposed in a server or cloud service, for example, may be arranged to provide access tokens to user device 110. For example, access service 140 may provide access tokens to user device 110, the access tokens being arranged to provide an appropriate level of access to access controlled device 120. The appropriate level of access may correspond to a role that a user of user device 110 has, for example. Where user device 110 may have several users, these users may have different

roles with respect to access controlled devices, and such a user device may be provided with appropriate access tokens to enable such use by plural users in plural roles. User device 110 may communicate with access service 140 via wireless link 115, base station 150, connection 156, controller 160, connection 167, gateway 170 and connection 174, for example. Wireless link 115 and base station 150 may be arranged to operate in accordance with a suitable cellular or non-cellular technology. Examples of cellular technology include long term evolution, LTE, and wireless code division multiple access, WCDMA. Examples of non-cellular technologies include WLAN and worldwide interoperability for microwave access, WiMAX. Alternatively, user device 110 may be configured to communicate with access service 140 more directly, for example, via a touch interaction with a server. Near-field communication, NFC, may provide touch interaction-based communication. User device 110 may be authenticated before providing it with access tokens from access service 140. Such authentication may be based on a cryptographic certificate, or simply a password, for example. Where a more direct communication with access service is employed, base station 150, connection 156, controller 160, connection 167, gateway 170 and connection 174 are optional features.

[0036] Access controlled device 120 may also obtain access tokens from access service 140. In principle, access controlled device 120 may obtain the access tokens via connection 123, gateway 130 and connection 134, where a permanent data pathway is arranged or available to link access controlled device 120 with access service 140. However, in the absence of connection 123, gateway 130 and connection 134, in accordance with various embodiments of the present invention, access controlled device 120 may obtain access tokens from access service 140 using user devices, such as, for example, user device 110. Access controlled device 120 may lack a fixed connection to access service 140. Access controlled device 120 may lack a connection to access service 140 that would be independent of user devices.

[0037] To furnish access controlled device 120 with access tokens, for example lists of access tokens, via a user device, access service 140 may encrypt such access tokens using an encryption key configured in access controlled device 120 and access service 140. Such an encryption key may be referred to as a master encryption key, for example. Access service 140 may provide the encrypted access tokens to a user device, for example in connection with providing separate access tokens for the user device for use by the user device. Thereafter, when the user device accesses access controlled device 120, the user

device may, in addition to accessing access controlled device 120 normally, provide the encrypted access tokens to access controlled device 120. Access controlled device 120 may then decrypt the access tokens, using the encryption key, and take them into use for subsequent accesses by user devices. The encryption used may be based on the advanced encryption standard, AES, for example.

[0038] Access service 140 may generate access tokens using a random or pseudorandom process. Access tokens may be generated using such a process, in principle, in unlimited amounts, in other words, access service 140 need never find itself in a situation where it has no access tokens to provide.

[0039] Access controlled device 120 and user device 110 may each select an access token to use in dependence of information, as described above. The information may originate in access controlled device 120, or be obtained from another source, such as, for example a satellite positioning signal clock signal. Selecting the access token to use may be achieved in separate ways.

[0040] Firstly, each access token in a list of access tokens may be associated with a validity time. For example, a first access token on the list may be valid on January 1st, while the second one will be valid on January 2nd, wherein when the second one is valid the first one will be expired, such that at any given time, the number of valid access tokens is low, for example exactly one. The validity time may be expressed as a date, as separate beginning and end times, or as a beginning or end time and an associated duration, for example. The information used in selecting an access token in this first scheme comprises an indication of a current time, which enables selecting the correct access token from the list in both access controlled device 120 and user device 110 when both access controlled device 120 and user device 110 use the same indication of current time.

[0041] Secondly, access controlled device 120 may be configured to use each access token a set number of times, for example once or ten times, after which the next access token in the list will be taken into use. In these embodiments, access controlled device 120 may provide in the information an indication as to which access token is currently in use, to enable user device 110 to select the corresponding access token. Such an indication may comprise, for example, a serial number of the access token in use. Where plural lists of access tokens are in use in access controlled device 120, access controlled device 120 may provide an indication as to which access token is in use in each of the lists. For example,

the information provided by access controlled device 120 may comprise indications of the form {{list_A, access_token_i}, {list_B, access_token_j}}, or similar, to inform user devices concerning which access token on each list are in use. When the access token has been used the set number of times, access controlled device 120 may increment the access token number in the provided information, and cease accepting accesses using the previous access token. An advantage of this second scheme is that a clock is not needed to produce the indication of a current time of the first scheme, since the indication of a current time itself is not needed. On the other hand, it may be difficult to predict a rate at which access tokens are used up in this second scheme. A longer list of access tokens may be provided to guard against their depletion, for example. A variation of the indications of the type {list_A, access_token_i} is one where a single counter is maintained, instead of one counter per list. In this variation, the single counter is incremented each time an access token is used, regardless of which list the used access token is comprised in. An advantage of this variation is that access controlled device 120 may be constructed to a simpler specification since plural counters are not necessary. A further advantage of this variation is that the time to deplete an access token list is less sensitive to the distribution of accesses to the lists, increasing predictability.

[0042] Thirdly, access controlled device 120 may allow each access token in each list to be used for a set period of time. In this third scheme, access controlled device 120 may provide in the information an indication as to which access token is usable, for example for each list as in the second scheme. An advantage of the third scheme is that an absolute time is not needed, only a time period measured by access controlled device 120.

[0043] The first, second and third schemes may be used even at the same time, as user device 110 may be configured to select an access token in dependence of the information. Some access controlled devices may use the first scheme, while others may use the second or third scheme. User device 110 may be configured to react correctly to each type of information provided, to select a suitable access token. In case user device 110 has an access token list that is numbered, but access controlled device 120 provides an indication of a current time in the information, an error may be presented to a user, for example, for administrative corrective measures.

[0044] An access token may comprise, for example, a long term key, a connection signature resolving key and/or an identity resolving key, in accordance with Bluetooth

specifications. In other implementations, cryptographic information of another kind may be comprised in access tokens.

[0045] In case an access controlled device 120 is rendered in a condition where it has no valid access tokens, a master access token may be used to enable an administrator to access the access controlled device 120 to provide it with access tokens. Access tokens may run out, for example, where the access tokens have validity times defined in absolute time, as in the first scheme, and the validity period of the last access token in the list ends without new access tokens being provided. Alternatively, an internal clock of an access controlled device may be reset or changed to a value outside the validity times of the available access tokens. In such a case, an administrator may access the access controlled device using the master access token and his own user device, to provide new access tokens and/or set the internal clock of access controlled device 120. Such new access tokens, again, may originate in access service 140. In some embodiments, the master access token is changed each time it is used.

[0046] Overall, an advantage may be obtained, separately and/or in combination, from each of the the first, second and third schemes in that access controlled devices need not have a connection of their own to access service 140 to obtain access tokens.

[0047] FIGURE 2 illustrates a system in accordance with at least some embodiments of the present invention. In FIGURE 2, like numbering denotes like structure as in FIGURE 1. In FIGURE 2, the connection between user device 110 and access service 140 is denoted schematically with connection 114.

[0048] The system of FIGURE 2 comprises an application management function 210, which may be usable in managing applications running on user devices. Such applications may be usable, for example, in generating access requests to access controlled devices 120 and generating a user interface to enable a user to interact with information in access controlled device 120. Managing applications may comprise, for example, providing software updates that affect the applications.

[0049] The system of FIGURE 2 further comprises a user device database 220. Database 220 may comprise information associating specific user devices with access levels to various access controlled devices. Database 220 may be consulted by access

service 140 when providing access tokens to user devices, to enable providing access tokens of a correct type, for example.

[0050] The system of FIGURE 2 further comprises a database 230 storing domain specific algorithms for analysing data. Such algorithms may enable visualizations, predict conditions and/or provide recommendations and personalized notifications.

[0051] 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 user device 110 or access controlled device 120 of FIGURE 1 or FIGURE 2. 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 more than one processor. A processing core may comprise, for example, a Cortex-A8 processing core manufactured by ARM Holdings or a Steamroller processing core produced by Advanced Micro Devices Corporation. Processor 310 may comprise at least one Qualcomm Snapdragon and/or Intel Atom 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.

[0052] 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 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 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.

[0053] 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, long term evolution, LTE, IS-95, wireless local area network, WLAN, Ethernet and/or worldwide interoperability for microwave access, WiMAX, standards, for example.

[0054] 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.

[0055] 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 seek access to an access controlled device.

[0056] Device 300 may comprise or be arranged to accept a user identity module 370. User identity module 370 may comprise, for example, a subscriber identity module, SIM, card installable in device 300. A user identity module 370 may comprise information identifying a subscription of a user of device 300. A user identity module 370 may comprise cryptographic information usable to verify the identity of a user of device 300 and/or to facilitate encryption of communicated information and billing of the user of device 300 for communication effected via device 300.

[0057] 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.

[0058] Device 300 may comprise further components not illustrated in FIGURE 3. For example, where device 300 comprises a smartphone, it may comprise at least one digital camera. Some devices 300 may comprise a back-facing camera and a front-facing camera, wherein the back-facing camera may be intended for digital photography and the front-facing camera for video telephony. Device 300 may comprise a fingerprint sensor arranged to authenticate, at least in part, a user of device 300. In some embodiments, device 300 lacks at least one device described above. For example, some devices 300 may lack a NFC transceiver 350 and/or user identity module 370.

[0059] Processor 310, memory 320, transmitter 330, receiver 340, NFC transceiver 350, UI 360 and/or user 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 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.

[0060] FIGURE 4 illustrates signalling in accordance with at least some embodiments of the present invention. On the vertical axes are disposed, from left to right, access controlled device 120, user device 110 and, finally, access service 140. Time advances from the top toward the bottom.

[0061] In phase 410, access controlled device 120 provides information to user device 110, for example by broadcasting or responsive to a request. In phase 420, user device 120 selects, based at least partly on the information received in phase 410, an access token, for example from a list. The selecting may be further based on an identity of access controlled device 120 and/or a role a user of user device 110 wants to assume with respect to access controlled device 120.

[0062] In phase 430, user device 110 requests for access to access controlled device 120. This phase may comprise setting the user devices' address to be a resolvable private address generated using an identity resolving key obtained from the selected access token.

A resolvable private address may comprise a random component, which makes an outsider's attempt to determine a role of user device 110 more difficult.

[0063] In phase 440, access controlled device 120 verifies the access credential presented by user device 110 is correct. If the credential presented by user device 110 is incorrect, access controlled device 120 may refuse access. Access controlled device 120 also selects an access token, which may correspond to a role user device 110 seeks with respect to access controlled device 120. The selection of access token in access controlled device 120 may also depend on the information communicated in phase 410. In phase 450, a connection is present between access controlled device 120 and user device 110. Such connection may be protected with cryptographic methods and be based, at least partly, on contents of the selected access tokens.

[0064] In phase 460, user device 110 communicates with access service 140. During this communication, user device 110 may be authenticated and presented with new access tokens, for example, new access token lists, each provided list corresponding to a role user device 110 can assume with respect to an access controlled device. Separate access token lists may be provided for distinct access controlled devices. Furthermore, in phase 460 user device 110 may be provided encrypted access token lists to be conveyed to at least one access controlled device. Such encrypted access token lists may comprise access token lists for each role that user devices can assume with respect to the access controlled device concerned.

[0065] In phase 470, as in phase 410, access controlled device 120 provides information to user device 110, for example by broadcasting. Subsequently in phases 480, 490 and 4100, as in corresponding phases 420, 430 and 440 user device 110 is authenticated toward access controlled device 120.

[0066] In phase 4110, a connection is present between access controlled device 120 and user device 110. User device 110 may access access controlled device 120, and access controlled device 120 may obtain the encrypted access token list or lists from user device 110. Access controlled device 120 may then decrypt the access token list or lists, to maintain a fresh store of access tokens.

[0067] FIGURE 5 is a first flow graph of a first method in accordance with at least some embodiments of the present invention. The illustrated method may be performed in

an access controlled device, for example, or in a control device configured to control the functioning of an access controlled device, when implanted therein.

[0068] Phase 510 comprises storing an encryption key and a list of access tokens. Phase 520 comprises selecting a first access token from the list of access tokens based, at least partly, on at least one of a current time and a sequence number. Phase 530 comprises deciding, based at least partly on the first access token, whether to grant a user device access to an apparatus, and causing the apparatus to receive a second list of access tokens from at least one of the user device and a second user device.

[0069] FIGURE 6 is a second flow graph of a second method in accordance with at least some embodiments of the present invention. The illustrated method may be performed in a user device, for example, or in a control device configured to control the functioning of a user device, when implanted therein.

[0070] Phase 610 comprises obtaining a list of access tokens. Phase 620 comprises processing information, the information comprising at least one of a sequence number and a current time indication. Phase 630 comprises selecting, based at least partly on the at least one of the sequence number and the current time indication, a first access token from the list of access tokens and establishing a connection with a first device based at least partly on the first access token. The information may originate in the first device. The information may comprise a broadcasted message. The broadcasted message may comprise an advertisement. The method may further comprise obtaining a second list of access tokens, and providing the second list of access tokens to the first device. The second list of access tokens may comprise a plurality of lists of access tokens. The second list of access tokens may be encrypted with an encryption key the apparatus performing the method of FIGURE 6 does not possess. The second list of access tokens may be obtained from an access service.

[0071] It is to be understood that the embodiments of the invention disclosed are not 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.

[0072] Reference throughout this specification to one embodiment or an

embodiment 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 substantially, the exact numerical value is also disclosed.

[0073] 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 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 example 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.

[0074] Furthermore, the described features, structures, or characteristics may be combined in any suitable manner in one or more embodiments. In the following 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.

[0075] 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.

[0076] 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

[0077] At least some embodiments of the present invention find industrial application in managing access controlled devices, to increase security.

ACRONYMS LIST

AES	advanced encryption standard
IoT	Internet of Things
LTE	long term evolution
NFC	near-field communication
USB	universal serial bus
WCDMA	wideband code division multiple access
WiMAX	worldwide interoperability for microwave access
WLAN	wireless local area network

REFERENCE SIGNS LIST

110	User device
120	Access controlled device
130	Gateway
140	Access Service
150	Base station
160	Controller
170	Gateway
210	Application management function

220	User device database
230	Database storing domain specific algorithms
300 – 370	Structure of the device of FIGURE 3
410 – 4110	Phases of the method of FIGURE 4
510 – 530	Phases of the method of FIGURE 5
610 - 640	Phases of the method of FIGURE 6

CLAIMS:

1. An apparatus comprising:
   - a memory configured to store an encryption key and a list of access tokens;
   - at least one processing core configured to
     - select a first access token from the list of access tokens based, at least partly, on at least one of a current time and a sequence number;
     - decide, based at least partly on the first access token, whether to grant a user device access to the apparatus, and
     - cause the apparatus to receive a second list of access tokens from at least one of the user device and a second user device.

2. The apparatus according to claim 1, wherein the at least one processing core is configured to cause the apparatus to receive the second list of access tokens over a short-range wireless interface.

3. The apparatus according to claim 2, wherein the short-range wireless interface comprises a Bluetooth interface.

4. The apparatus according to any of claims 1 – 3, wherein the memory is configured to store a plurality of lists of access tokens, each list of access tokens comprising access tokens that are usable in obtaining a different level of access to the apparatus.

5. The apparatus according to claim 4, wherein each list corresponds to a distinct role a user may assume with respect to the apparatus.

6. The apparatus according to any of claims 1 – 5, wherein the at least one processing core is configured to select the first access token based at least partly on the current time, each access token being associated with a validity time interval.

7. The apparatus according to any of claims 1 – 5, wherein the at least one processing core is configured to select the first access token based at least partly on the sequence number by allowing each access token to be used a set number of times.

8. The apparatus according to any of claims 1 – 5, wherein the at least one processing core is configured to select the first access token based at least partly on the sequence number, wherein each access token is enabled for a preconfigured time duration, after which the sequence number used is incremented.

9. The apparatus according to any of claims 1 – 8, wherein the at least one processing core is configured to cause the apparatus to advertise at least one of the current time and the sequence number.

10. The apparatus according to any of claims 1 – 9, wherein the at least one processing core is configured to cause the apparatus to decrypt the second list of access tokens, using the encryption key, and to authenticate the second list of access tokens based at least partly based on a result of the decrypting.

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:

- obtain a list of access tokens;
- process information, the information comprising at least one of a sequence number and a current time indication, and
- select, based at least partly on the at least one of the sequence number and the current time indication, a first access token from the list of access tokens and establish a connection with a first device based at least partly on the first access token.

12. The apparatus according to claim 11, wherein the at least one memory and the computer program code are configured to, with the at least one processing core, cause the apparatus to select the first access token based at least partly on the current time, each access token being associated with a validity time interval.

13. The apparatus according to claim 11, wherein the at least one memory and the computer program code are configured to, with the at least one processing core, cause the

apparatus to select the first access token based at least partly on the sequence number, each access token being allowed to be used a set number of times.

14. The apparatus according to claim 11, wherein the at least one memory and the computer program code are configured to, with the at least one processing core, cause the apparatus to select the first access token based at least partly on the sequence number, wherein each access token is enabled for a preconfigured time duration, after which the sequence number used is incremented.

15. The apparatus according to any of claims 11 – 14, wherein the at least one memory and the computer program code are configured to, with the at least one processing core, cause the apparatus to obtain a second list of access tokens, and to provide the second list of access tokens to the first device.

16. A method comprising:

- storing an encryption key and a list of access tokens;
- selecting a first access token from the list of access tokens based, at least partly, on at least one of a current time and a sequence number;
- deciding, based at least partly on the first access token, whether to grant a user device access to an apparatus, and
- causing the apparatus to receive a second list of access tokens from at least one of the user device and a second user device.

17. The method according to claim 16, comprising receiving the second list of access tokens over a short-range wireless interface.

18. The method according to claim 17, wherein the short-range wireless interface comprises a Bluetooth interface.

19. The method according to any of claims 1 – 3, further comprising storing a plurality of lists of access tokens, each list of access tokens comprising access tokens that are usable in obtaining a different level of access to the apparatus.

20. The method according to claim 19, wherein each list corresponds to a distinct role a user may assume with respect to the apparatus.

21. The method according to any of claims 16 – 20, comprising selecting the first access token based at least partly on the current time, each access token being associated with a validity time interval.

22. The method according to any of claims 16 – 20, comprising selecting the first access token based at least partly on the sequence number by allowing each access token to be used a set number of times.

23. The method according to any of claims 16 – 20, comprising selecting the first access token based at least partly on the sequence number, wherein each access token is enabled for a preconfigured time duration, after which the sequence number used is incremented.

24. The method according to any of claims 16 – 23, comprising advertising at least one of the current time and the sequence number.

25. The method according to any of claims 1 – 9, further comprising causing the apparatus to decrypt the second list of access tokens, using the encryption key, and authenticating the second list of access tokens based at least partly based on a result of the decrypting.

26. A method comprising:

- obtaining a list of access tokens;
- processing information, the information comprising at least one of a sequence number and a current time indication, and
- selecting, based at least partly on the at least one of the sequence number and the current time indication, a first access token from the list of access tokens and establishing a connection with a first device based at least partly on the first access token.

27. The method according to claim 26, wherein the first access token is selected based at least partly on the current time, each access token being associated with a validity time interval.

28. The method according to claim 26, wherein the first access token is selected based at least partly on the sequence number, each access token being allowed to be used a set number of times.

29. The method according to claim 26, wherein the first access token is selected based at least partly on the sequence number, wherein each access token is enabled for a preconfigured time duration, after which the sequence number used is incremented.

30. The method according to any of claims 26 – 29, further comprising obtaining a second list of access tokens, and providing the second list of access tokens to the first device.

31. An apparatus comprising:

- means for storing an encryption key and a list of access tokens;
- means for selecting a first access token from the list of access tokens based, at least partly, on at least one of a current time and a sequence number;
- means for deciding, based at least partly on the first access token, whether to grant a user device access to an apparatus, and
- means for causing the apparatus to receive a second list of access tokens from at least one of the user device and a second user device.

32. An apparatus comprising:

- means for obtaining a list of access tokens;
- means for processing an advertisement originating in a first device, the advertisement comprising at least one of a sequence number and a current time indication, and
- means for selecting, based at least partly on the at least one of the sequence number and the current time indication, a first access token from the list of access tokens, and for establishing a connection with the first device based at least partly on the first access token.

33. 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:

- store an encryption key and a list of access tokens;
- select a first access token from the list of access tokens based, at least partly, on at least one of a current time and a sequence number;
- decide, based at least partly on the first access token, whether to grant a user device access to an apparatus, and
- cause the apparatus to receive a second list of access tokens from at least one of the user device and a second user device.

34. 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:

- obtain a list of access tokens;
- process an advertisement originating in a first device, the advertisement comprising at least one of a sequence number and a current time indication, and
- select, based at least partly on the at least one of the sequence number and the current time indication, a first access token from the list of access tokens and establish a connection with the first device based at least partly on the first access token.

35. A computer program configured to cause a method in accordance with at least one of claims 16 – 30 to be performed.

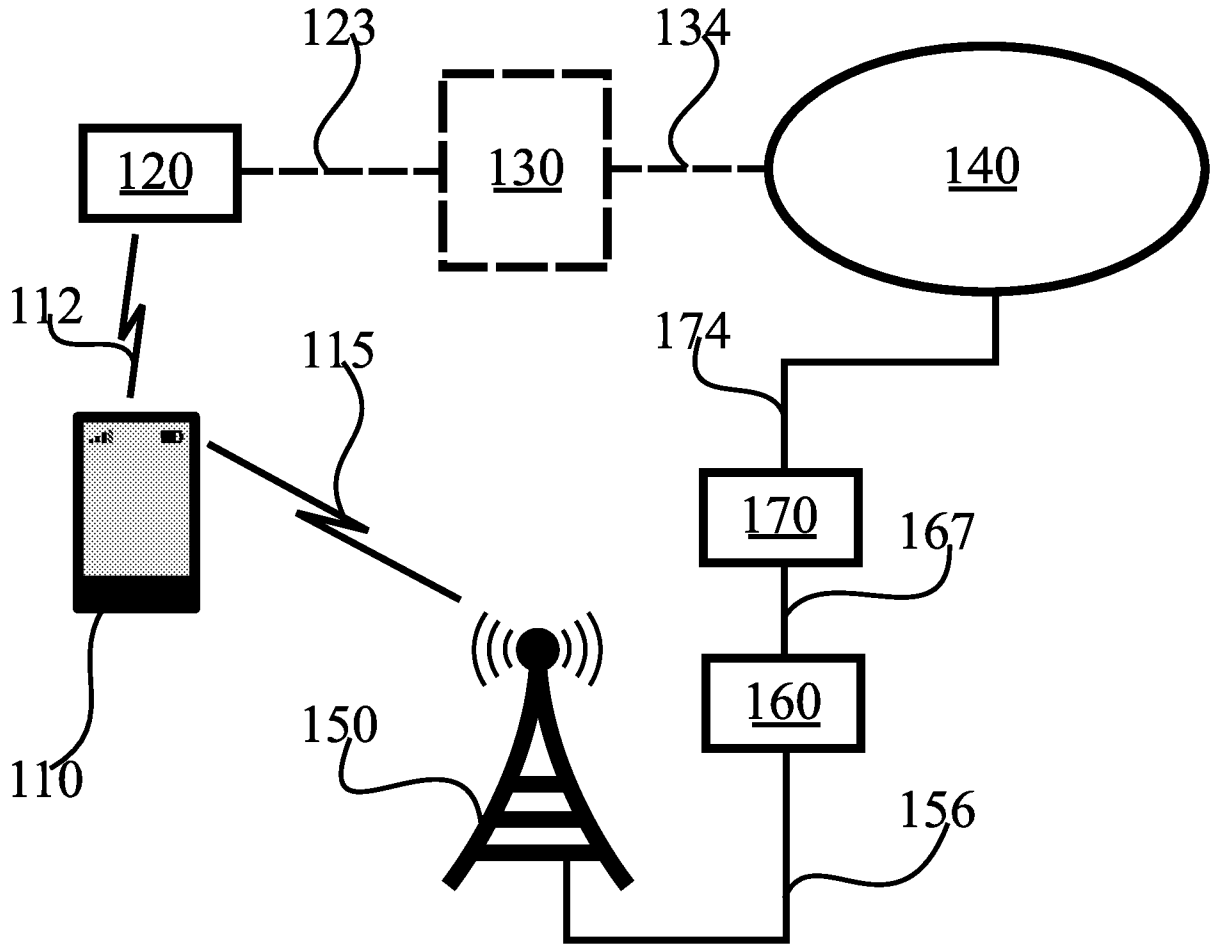

FIGURE 1

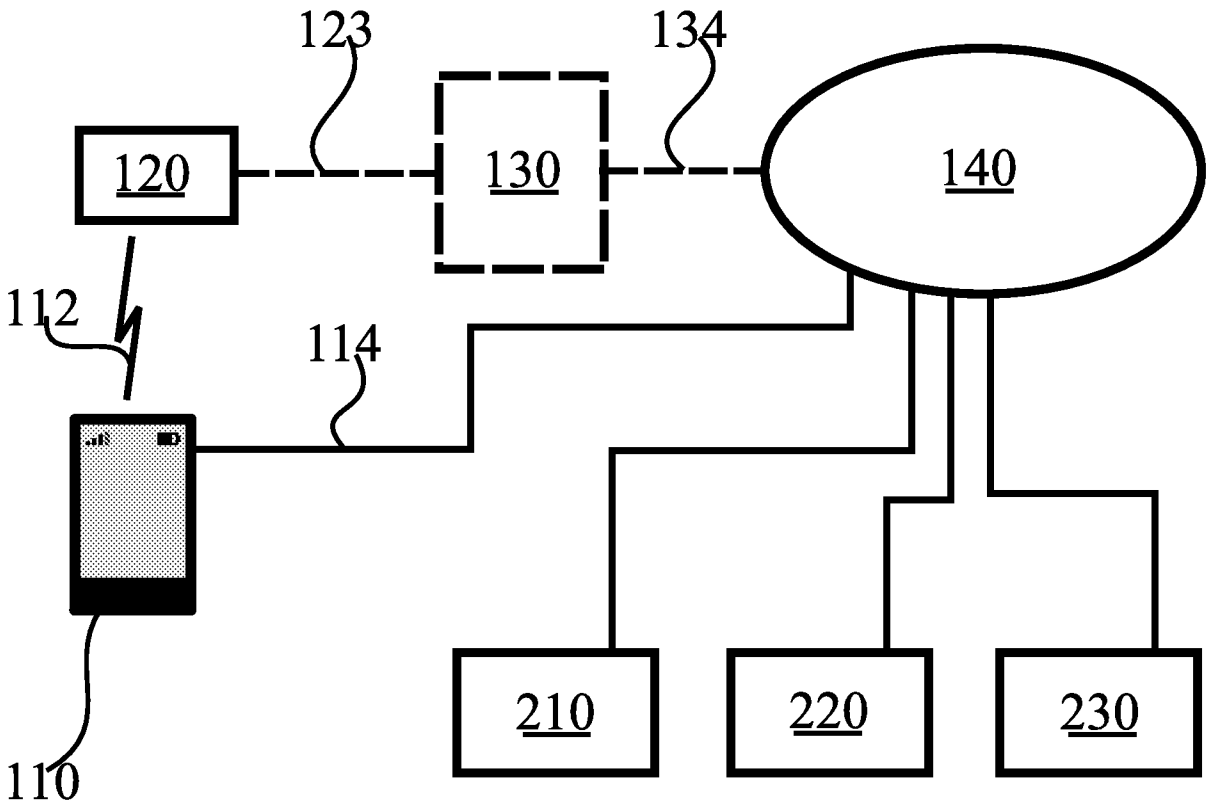

FIGURE 2

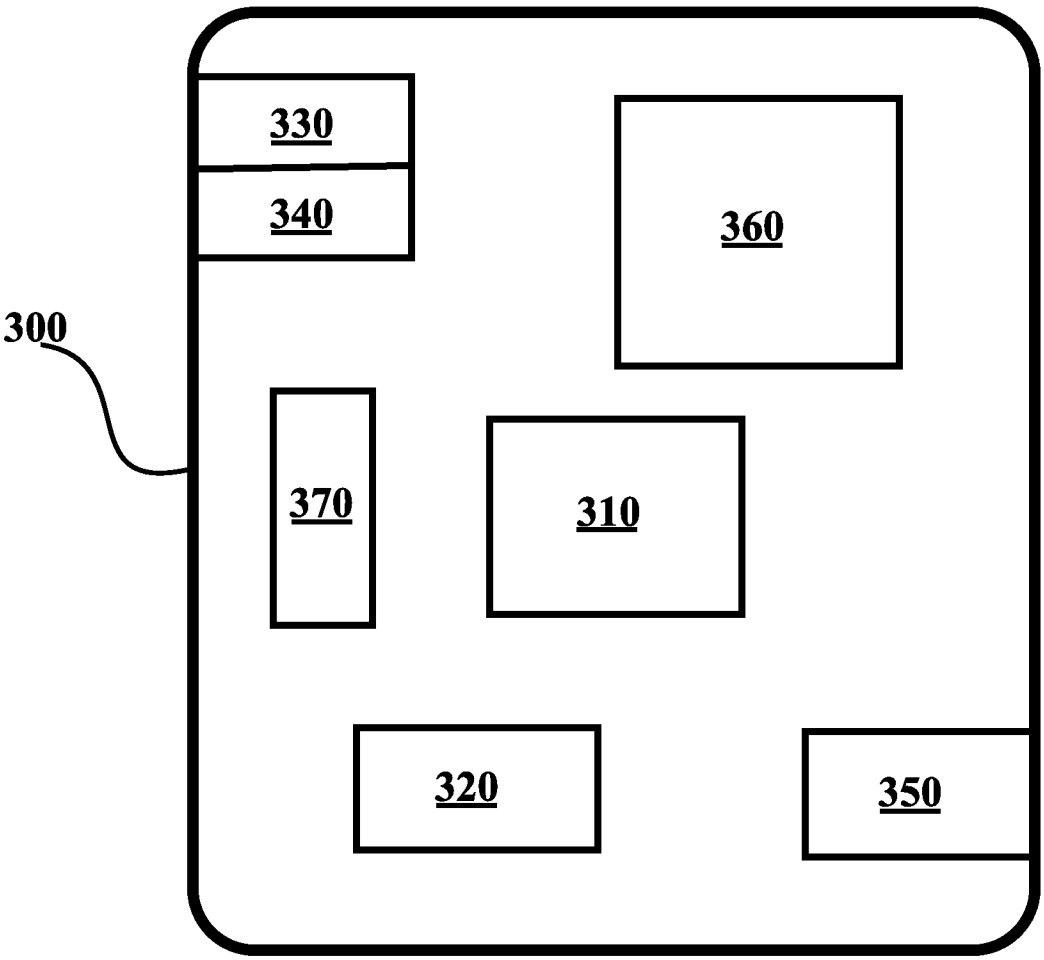

FIGURE 3

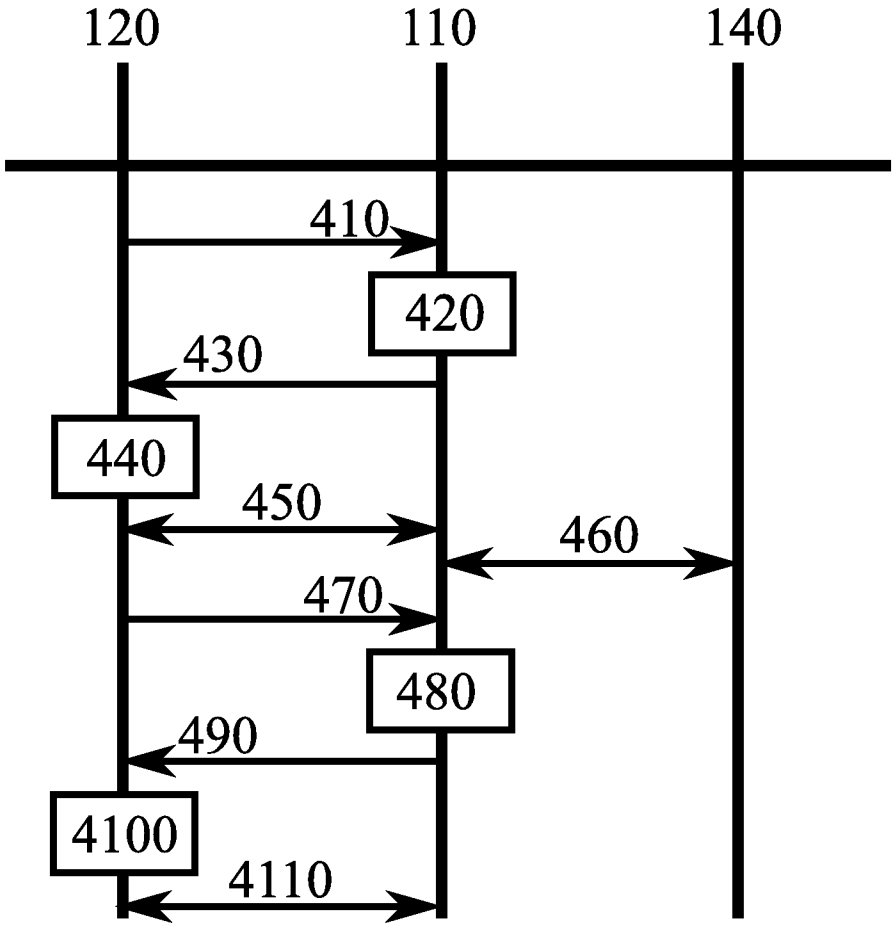

FIGURE 4

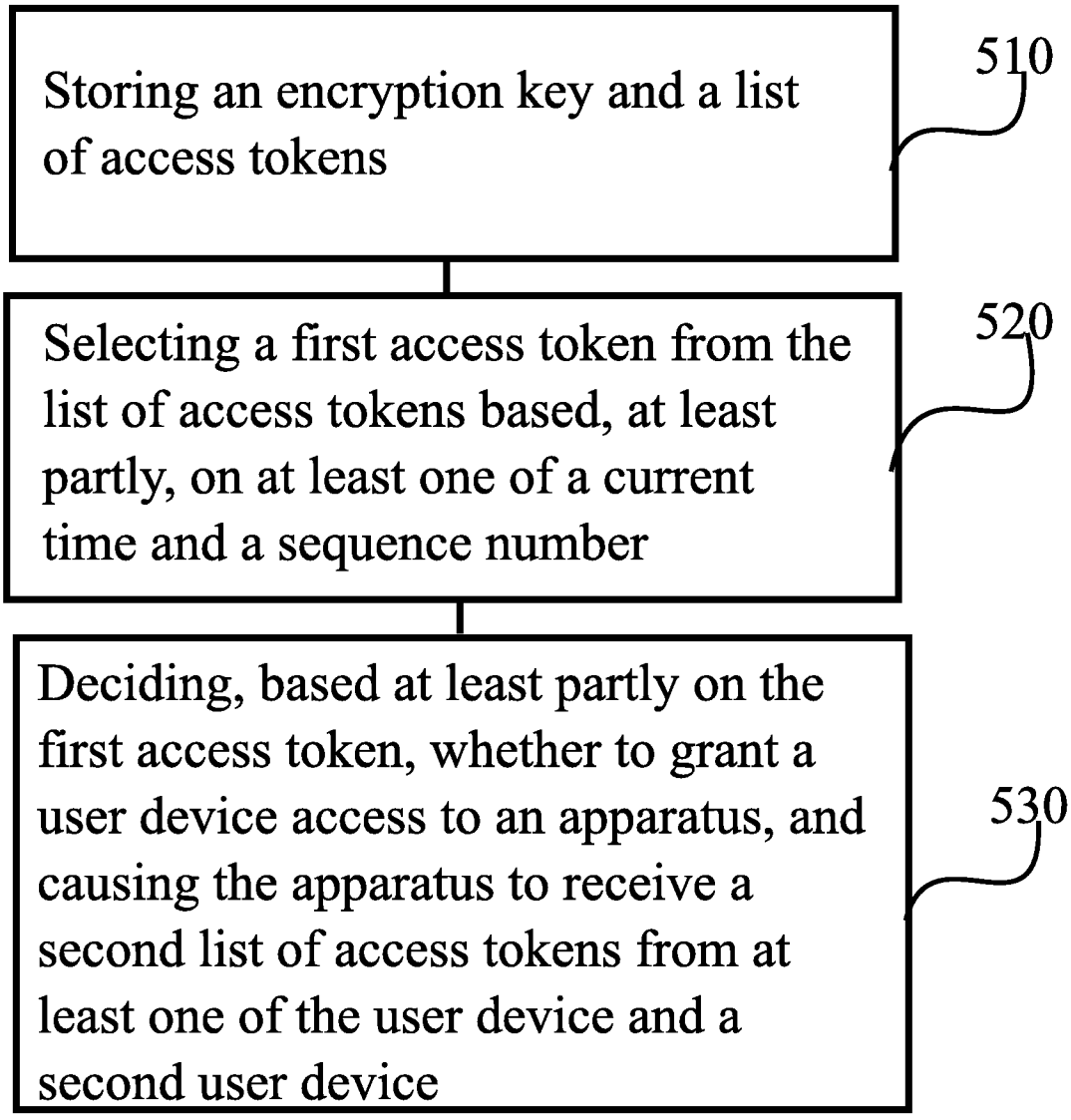
Storing an encryption key and a list of access tokens
510
Selecting a first access token from the list of access tokens based, at least partly, on at least one of a current time and a sequence number
520
Deciding, based at least partly on the first access token, whether to grant a user device access to an apparatus, and causing the apparatus to receive a second list of access tokens from at least one of the user device and a second user device
530

FIGURE 5

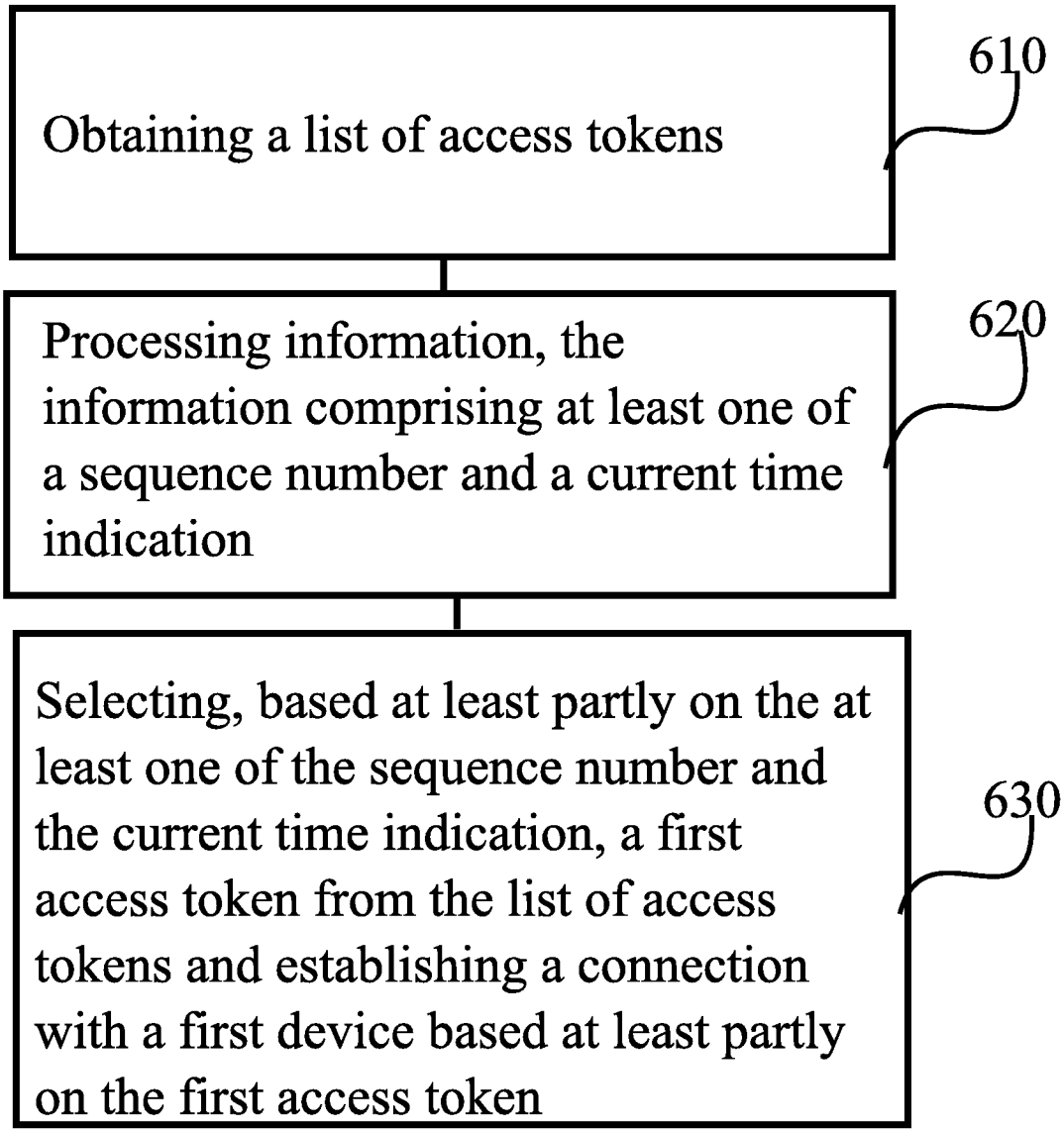
Obtaining a list of access tokens
610
Processing information, the information comprising at least one of a sequence number and a current time indication
620
Selecting, based at least partly on the at least one of the sequence number and the current time indication, a first access token from the list of access tokens and establishing a connection with a first device based at least partly on the first access token
630

FIGURE 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2015/050852

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, H04W, G06F, G07C

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 2434463 A2 (PHONIRO AB [SE]) 28 March 2012 (28.03.2012) abstract, paras [0017],[0019]-[0024],[0028],[0064],[0074]	1-35
Y	US 8793784 B2 (METIVIER PASCAL [FR] et al.) 29 July 2014 (29.07.2014) abstract, col. 2 line 59 – col. 3 line 8, col. 4 lines 24-46	1-35
A	EP 1450312 A2 (COMPUTERIZED SECURITY SYSTEMS [US]) 25 August 2004 (25.08.2004)	1-35
A	US 7114178 B2 (DENT PAUL W [US] et al.) 26 September 2006 (26.09.2006)	1-35
A	US 8042163 B1 (KARR RONALD S [US] et al.) 18 October 2011 (18.10.2011)	1-35

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

*	Special categories of cited documents:	"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
"A"	document defining the general state of the art which is not considered to be of particular relevance	"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
"E"	earlier application or patent but published on or after the international filing date	"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
"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)	"&"	document member of the same patent family
"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		

Date of the actual completion of the international search	Date of mailing of the international search report
17 March 2016 (17.03.2016)	18 March 2016 (18.03.2016)

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

Authorized officer
Jorma Ristola
Telephone No. +358 9 6939 500

INTERNATIONAL SEARCH REPORT
Information on Patent Family Members

International application No.
PCT/FI2015/050852

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
EP 2434463 A2	28/03/2012	DK 2083396 T3	17/12/2012
		DK 201300075 U1	24/05/2013
		DK 201300075 U4	13/09/2013
		DK 201300119 U1	23/08/2013
		DK 201300119 U4	11/10/2013
		DK 201300133 U1	27/09/2013
		DK 201300133 Y4	17/01/2014
		EP 1843237 A2	10/10/2007
		EP 1859415 A1	28/11/2007
		EP 2083396 A2	29/07/2009
		EP 2083396 B1	28/11/2012
		SE 0500616 L	19/09/2006
		SE 530279 C2	15/04/2008
		US 2010148921 A1	17/06/2010
		US 8222993 B2	17/07/2012
		US 2009184801 A1	23/07/2009
		US 8593249 B2	26/11/2013
		US 2007229257 A1	04/10/2007
		US 2014020437 A1	23/01/2014
		US 2014022054 A1	23/01/2014
		WO 2006098690 A1	21/09/2006
US 8793784 B2	29/07/2014	US 8793784 B2	29/07/2014
		EP 2500872 A1	19/09/2012
EP 1450312 A2	25/08/2004	US 2004160305 A1	19/08/2004
US 7114178 B2	26/09/2006	US 7114178 B2	26/09/2006
		AU 2002308549 A1	03/12/2002
		DK 1423826 T3	08/09/2014
		EP 1423826 A1	02/06/2004
		EP 1423826 B1	09/07/2014
		EP 2320388 A1	11/05/2011
		ES 2507548 T3	15/10/2014
		KR 20040033285 A	21/04/2004
		PT 1423826 E	26/09/2014
		WO 02095689 A1	28/11/2002
US 8042163 B1	18/10/2011	None	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2015/050852

CLASSIFICATION OF SUBJECT MATTER

IPC
G07C 9/00 (2006.01)
H04L 9/32 (2006.01)
G06F 21/45 (2013.01)
H04W 12/08 (2009.01)