



- (51) International Patent Classification:
G06F 21/35 (2006.01) G07C 9/00 (2006.01)
- (21) International Application Number:
PCT/FI2017/050221
- (22) International Filing Date:
29 March 2017 (29.03.2017)
- (25) Filing Language: English
- (26) Publication Language: English
- (71) Applicant: NOKIA TECHNOLOGIES OY [FI/FI];
Karaportti 3, 02610 Espoo (FI).
- (72) Inventors: ROENNOW, Troels; 61 Ellis Road, Cambridge CB2 9BG (GB). PALYUTINA, Karina; 40 Francis Darwin Court, Cambridge CB4 3HA (GB). MARTÍN LÓPEZ, Enrique; 22b Carlyle Road, Cambridge CB4 3DN (GB). LI, H LI, Hongwei; 42 Green End Road, Cambridge CB4 1RY (GB). LACERDA-DE-MENEZES-DIETSCHI, Christina; 22 Lambourne road, Hardwick CB23 7XB (GB).
- (74) Agent: SEPPO LAINE OY; Itämerenkatu 3 A, 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, DJ, 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, 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, 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).

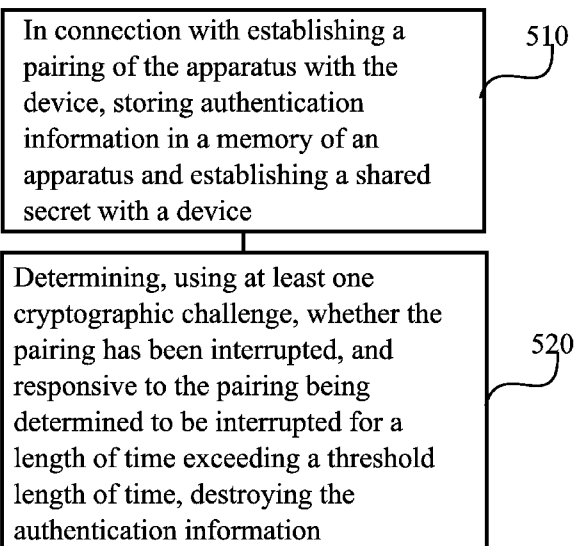
Declarations under Rule 4.17:

— of inventorship (Rule 4.17(iv))

Published:

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

(54) Title: HARDWARE BASED AUTHENTICATION



(57) Abstract: According to an example aspect of the present invention, there is provided an apparatus comprising a memory configured to store authentication information, at least one processing core configured to in connection with establishing a pairing of the apparatus with a device, store the authentication information in the memory and establish a shared secret with the device, and determine, using at least one cryptographic challenge, whether the pairing has been interrupted, and responsive to the pairing being determined to be interrupted for a length of time exceeding a threshold length of time, destroy the authentication information.

FIGURE 5

HARDWARE BASED AUTHENTICATION

FIELD

[0001] The present invention relates to hardware-based authentication, such as, for
5 example, secure card based authentication.

BACKGROUND

[0002] Controlling access to physical areas, such as rooms, and resources, such as
computers, industrial processes and medicines is necessary to ensure confidentiality,
10 protection against theft and safety. For example, where a room is used to tabulate an
election result or view confidential patient information, outsiders should be kept out to
prevent unauthorized persons from gaining access to information that is handled in the
room.

[0003] Industrial processes, on the other hand, may be isolated from outsiders to
15 protect the outsiders from dangers they might face, if admitted into premises where the
process is run. Chemical plants may use hazardous chemicals that are capable of damaging
health, and hospital X-ray rooms, for example, should be kept free of outsiders to prevent
the outsiders from being unnecessarily subjected to ionizing radiation. Where infectious
diseases are treated in an isolated ward, outsiders should be kept out to protect them from
20 risk of infection.

[0004] Resources that are potential targets for theft may likewise be stored in a
secured location, such as a room or safe. Examples of such resources include cash money,
medications, weapons and artwork.

[0005] Securing areas or resources may be accomplished with physical locks, which
25 may be opened by appropriate keys, as has been done for centuries. More recent solutions
include electronic access cards or tokens, which may contain digital information
configured to cause a locking device to grant access to a holder of the card or token, for
example by opening a door or unblocking access to a feature in a computer program.

[0006] Digital information on a token may comprise information identifying the intended holder of the token, and/or information defining an extent of access the intended holder is to be granted. One example of a token is a biometric passport, which is configured with information concerning a digital photograph of the holder, or, optionally,
5 information concerning a fingerprint of the holder.

SUMMARY OF THE INVENTION

10 [0007] According to a first aspect of the present invention, there is provided an apparatus comprising a memory configured to store authentication information, at least one processing core configured to in connection with establishing a pairing of the apparatus with a device, store the authentication information in the memory and establish a shared secret with the device, and determine, using at least one cryptographic challenge, whether
15 the pairing has been interrupted, and responsive to the pairing being determined to be interrupted for a length of time exceeding a threshold length of time, destroy the authentication information.

[0008] Various embodiments of the first aspect may comprise at least one feature from the following bulleted list:

- 20 • the memory comprises a secured memory, the at least one processor being configured to store the authentication information in the secured memory
- the apparatus is configured to receive the authentication information from a base unit
- the apparatus is configured to participate in an authenticating interaction in a state
25 where the pairing has been interrupted and when the interruption has lasted for less than the threshold length of time
- the apparatus is configured to require at least one of biometric authentication, pin-code authentication and two-factor authentication in connection with participating in the authenticating interaction
- 30 • the apparatus comprises a first battery and a second battery

- the at least one processing core is configured to use electrical power from the second battery when performing security operations
- the at least one processing core is configured to use electrical power from the second battery to destroy the authentication information responsive to a charge level of the first battery declining below a charge threshold
- the apparatus comprises a body sensor, and the at least one processing core is configured to destroy the authentication information responsive to a determination, based at least in part on the body sensor, that the apparatus has been removed from a user's body for a time period exceeding a second threshold length of time
- the authentication information comprises a public key – private key pair of a public-key cryptosystem.

[0009] According to a second aspect of the present invention, there is provided an apparatus comprising a memory configured to store authentication information, at least one processing core configured to, in connection with establishing a pairing of the apparatus with an access token, establish a shared secret with the access token, participate in maintaining the pairing by responding to at least one cryptographic challenge from the access token, and participate in an authenticating interaction, based at least partly on the authentication information, when the pairing is not present.

[0010] Various embodiments of the second aspect may comprise at least one feature from the following bulleted list:

- the authentication information comprises a public key – private key pair of a public-key cryptosystem
- the at least one processing core is configured to, in connection with responding to each of the at least one cryptographic challenge, calculate a hash value using at least the shared secret as input.

[0011] According to a third aspect of the present invention, there is provided a method, comprising in connection with establishing a pairing of an apparatus with a device, storing authentication information in a memory of the apparatus and establishing a shared secret with the device, and determining, using at least one cryptographic challenge, whether the pairing has been interrupted, and responsive to the pairing being determined to be interrupted for a length of time exceeding a threshold length of time, destroying the authentication information.

[0012] Various embodiments of the third aspect may comprise at least one feature from the following bulleted list:

- the memory comprises a secured memory, and the authentication information is stored in the secured memory
- 5 • receiving the authentication information from a base unit
- participating in an authenticating interaction in a state where the pairing has been interrupted and when the interruption has lasted for less than the threshold length of time
- requiring at least one of biometric authentication, pin-code authentication and two-
10 factor authentication in connection with participating in the authenticating interaction
- using a first battery and a second battery of the apparatus
- using electrical power from the second battery when performing security operations
- using electrical power from the second battery to destroy the authentication
15 information responsive to a charge level of the first battery declining below a charge threshold
- the apparatus comprises a body sensor, and the method further comprises destroying the authentication information responsive to a determination, based at least in part on the body sensor, that the apparatus has been removed from a user's
20 body for a time period exceeding a second threshold length of time
- the authentication information comprises a public key – private key pair of a public-key cryptosystem.

[0013] According to a fourth aspect of the present invention, there is provided a method comprising storing authentication information, in connection with establishing a
25 pairing of an apparatus with an access token, establishing a shared secret with the access token, participating in maintaining the pairing by responding to at least one cryptographic challenge from the access token, and participating in an authenticating interaction, based at least partly on the authentication information, when the pairing is not present.

[0014] Various embodiments of the fourth aspect may comprise at least one feature
30 from the following bulleted list:

- the authentication information comprises a public key – private key pair of a public-key cryptosystem

- in connection with responding to each of the at least one cryptographic challenge, calculating a hash value using at least the shared secret as input.

[0015] According to a fifth aspect of the present invention, there is provided a system comprising at least one first apparatus according to the first aspect and at least one
5 second apparatus according to the second aspect.

[0016] According to a sixth aspect of the present invention, there is provided an apparatus comprising means for, in connection with establishing a pairing of the apparatus with a device, storing authentication information in a memory of the apparatus and establishing a shared secret with the device, and means for determining, using at least one
10 cryptographic challenge, whether the pairing has been interrupted, and responsive to the pairing being determined to be interrupted for a length of time exceeding a threshold length of time, destroying the authentication information.

[0017] According to a seventh aspect of the present invention, there is provided an apparatus comprising means for storing authentication information, means for, in
15 connection with establishing a pairing of an apparatus with an access token, establishing a shared secret with the access token, means for participating in maintaining the pairing by responding to at least one cryptographic challenge from the access token, and means for participating in an authenticating interaction, based at least partly on the authentication information, in a state when the pairing is not present.

20 [0018] 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, in connection with establishing a pairing of an apparatus with a device, store authentication information in a memory of the apparatus and establish a shared secret with the device, and
25 determine, using at least one cryptographic challenge, whether the pairing has been interrupted, and responsive to the pairing being determined to be interrupted for a length of time exceeding a threshold length of time, destroy the authentication information.

[0019] According to a ninth aspect of the present invention, there is provided a non-transitory computer readable medium having stored thereon a set of computer readable
30 instructions that, when executed by at least one processor, cause an apparatus to at least store authentication information, in connection with establishing a pairing of an apparatus with an access token, establish a shared secret with the access token, participate in

maintaining the pairing by responding to at least one cryptographic challenge from the access token, and participate in an authenticating interaction, based at least partly on the authentication information, in a state when the pairing is not present.

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

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] FIGUREs 1A and 1B illustrate part of an example system in accordance with
10 at least some embodiments of the present invention;

[0022] FIGURE 2 illustrates state transitions 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;

15 [0024] FIGURE 4 illustrates signalling in accordance with at least some embodiments of the present invention;

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

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

EMBODIMENTS

[0027] A two-part authentication system is described, wherein a first part, which
25 may comprise a clip, has an independent authentication capability, and the first part is configured to participate in a pairing with a second part, which may comprise a token. The token may store authentication information, which is maintained in the token as long as the

pairing with the first part is not interrupted for a time period that exceeds a threshold length. In case the pairing is interrupted for a time period that exceeds in length the threshold, the authentication information in the token may be autonomously deleted by the token, to prevent misuse of a stolen token.

5 **[0028]** FIGURES 1A and 1B illustrate part of an example system in accordance with at least some embodiments of the present invention. A reader 130 comprises a sensor 135, which is configured to interact with tokens 110. While in the following discussion a hospital setting is used as an example, the skilled reader understands this is merely an example, and the technical principles of the invention may be applied more broadly.

10 **[0029]** Token 110 may store authentication information, which may comprise at least one, or more than one, of the following: identification information of a bearer of token 110, biometric information concerning the bearer, information defining access rights, and cryptographic information. Cryptographic information may comprise at least one encryption key, such as, for example, a symmetric-algorithm encryption key or at least one
15 public key – private key pair of a public-key cryptosystem. Examples of symmetric encryption algorithms include the advanced encryption standard, AES, and Blowfish algorithms. Examples of public-key cryptosystems include the Rivest-Shamir-Adleman, RSA, and ElGamal systems. In some embodiments, the cryptographic information may comprise only a private key or a public key of a public-key cryptosystem, enabling
20 cryptographic signing or encryption operations, respectively.

[0030] In token 110, the authentication information may be stored in a secure element, which may comprise a secure memory, for example. The secure element may be designed so that it is difficult for malicious attackers to gain access to the contents thereof. The secure element may be powered by a battery, for example a chargeable battery,
25 distinct from a battery used to power token 110 generally. In case the battery used to power token 110 generally is observed, by token 110, to decline in charge level below a charge threshold, destroying of the authentication information in the secure element may be performed, by token 110, using the battery that powers the secure element. Alternatively, the secure element may comprise volatile memory, which loses its information contents in
30 case power is lost. In such cases, a single battery may be used for token 110, since the authentication information is lost in connection with battery exhaustion with no need for specific actions to be taken.

[0031] To initialize the system, token 110 may be paired with clip 120. Clip 120 may be a suitable device that is capable of being paired with token 110. Clip 120 may be physically attachable to token 110, for example magnetically or by a snap. Clip 120 may comprise a memory with clip authentication information, enabling participation in an authenticating interaction with a reader, such as reader 130, independently of token 110. For example, the clip authentication information may enable default or basic level access to a facility, such as a hospital. The clip authentication information may comprise cryptographic information, for example, as described above in connection with token 110. The cryptographic information in clip 120 may be distinct and different from the cryptographic information in token 110, such that a different level of access may be gained with the authentication informations in the clip and the token, for example. Biometric authentication may be required in connection with an authenticating interaction. Alternatively to, or in addition to, biometric authentication, pin-code authentication and/or two-factor authentication may be required in connection with an authenticating interaction, for example.

[0032] “Clip” is herein used as a terminological choice by which it is not intended to impart physical limitations on a shape of this unit. Rather, any electronic device capable of performing the functions herein described as being performed by clip 120 is suitable to perform as clip 120. Clip 120 may be powered by a battery, for example, which may be rechargeable. In some embodiments, clip 120 may be powered by wireless energy from a reader device, in which case a separate battery in clip 120 may be unnecessary.

[0033] A user of the system may arrive at work, such as at a hospital, with clip 120 and without a token 110. She may use clip 120 to access the building and proceed to an authentication station, for example at a locker room where clothing is changed. At the authentication station a token 110 may be provided to the user, such that the user is for this action authenticated using biometric or in-person processing, for example. Alternatively to, or in addition to, biometric authentication, pin-code authentication and/or two-factor authentication may be employed, for example. A token 110 may be empty of authentication information prior to being taken into use to pair it with clip 120. Once the user is authenticated, token 110 may be furnished with suitable authentication information which may enable access to the hospital more extensively than the clip by itself. Clip 120 and token 110 may be furnished with a shared secret, which may comprise a randomly or pseudo-randomly generated bit sequence, for example. The shared secret may be generated

by clip 120 and token 110 when paired together, or the shared secret may be provided to token 110, which may provide it to clip 120 in connection with establishing the pairing between clip 120 and token 110. A linking station may function as a battery recharge device of token 110 and pairing facilitator for clip 120 and token 110. The linking station
5 may generate the shared secret and provide it to token 110 and/or clip 120, for example. The linking station is one type of base unit.

[0034] In one embodiment, the initialization is performed as follows:

- Token 110 may be attached to the linking station. The clip 120 may be attached to the linking station too
- 10 • The linking station requests the user to present a biometric signature such as a fingerprint, or another kind of authentication input, such as a pin code
- After verifying the identity of the user, the linking station transfers the authentication information to the token (private-public key pair of the token, personalized access rights, and possibly a random number SK). In one variant, the
15 linking station further transfers clip authentication information to the clip (private-public key pair of the clip, and possibly the same random number SK that would become a shared secret between clip 120 and token 110).
- Where random number SK is not written to clip 120, token 110 may now have a 1 minute period, for example, when it is ready to pair to clip 120. If not attached to a
20 clip the authentication information may be deleted from the token. Upon connecting to clip 120, token 110 would generate the random number SK which would be communicated to clip 120 and would become the shared (pairing) secret.

[0035] At the end of the day, the user may leave the facility, such as hospital, and return token 110. The user may keep clip 120, wherefore the authentication information on
25 token 110 will be destroyed automatically upon the user leaving token 110 behind, as described herein. Alternatively, the authentication information may be explicitly cleared at the end of the day.

[0036] Token 110 and clip 120 are illustrated in FIGURE 1A as attached together, wherein their pairing with each other may be maintained using a short-range
30 communication technology. Token 110 and clip 120 may be enabled to communicate with

each other, for example using near-field communication, NFC, or Bluetooth, both of these being examples of short-range communication technologies. Inter-Integrated Circuit, I²C, or universal asynchronous receiver/transmitter, UART, may be used. To maintain the pairing of token 110 with clip 120, token 110 may transmit to clip 120 a challenge, illustrated in FIGURE 1A as challenge 110C. Challenge 110C may be referred to as a pairing challenge.

[0037] Pairing challenge 110C may comprise, for example, a random number generated in token 110 for challenge 110C. Clip 120 may respond to challenge 110C by transmitting a pairing response 120R, which token 110 may assess as to its correctness. In case response 120R is correct, token 110 may maintain itself in a paired state. In case response 120R is incorrect or missing, token 110 may determine the pairing has been interrupted. Token 110 may transmit challenges to clip 120 periodically or randomly, such that token 110 is enabled to detect whether it has been removed from proximity of clip 120. Pairing challenge 110 together with pairing response 120R may be considered a pairing interaction. Token 110 participates in the pairing interaction by generating and transmitting the challenge, and clip 120 participates in the pairing interaction by generating and transmitting the response.

[0038] Where challenge 110C comprises a random number, response 120R may comprise a hash calculated with the random number from challenge 110C and the shared secret: hash (random number XOR shared secret) or hash (random number + shared secret). As another example, response 120R may comprise a cryptographic signature obtained from a private key of clip 120 and the random number from challenge 110C. To verify the signature, token 110 may have a public key of clip 120. A further example is where response 120R comprises an encrypted version of the random number from the challenge, the encrypting being performed using the shared secret as a symmetric-encryption algorithm key.

[0039] The communication interface between clip 120 and token 110 may be unencrypted, as using a cryptographic pairing interaction, as described above, renders the process inherently resilient. For example, computational power needed to reverse a hash function increases exponentially in the number of bits of the shared secret.

[0040] Where the pairing interaction is based on hashes or symmetric encryption, the shared secret between clip 120 and token 110 may comprise that each of these units stores

a copy of the same shared, secret data. On the other hand, where the pairing interaction is based on public-key cryptography, the shared secret may be divided between clip 120 and token 110, such that clip 120 stores a private key and token 110 stores a public key of the same key pair. Thus token 110 is enabled to verify a signature using the public key, and clip 120 is enabled to produce the signature using the private key. In both cases, the shared secret is established between the clip and the token. The cryptographic pairing challenge may thus be based on the shared secret.

[0041] In use, the user may use token 110 to access a resource or area that is controlled. FIGURE 1B illustrates a situation, where the user has removed token 110 from clip 120 in order to present token 110 to sensor 135. A close-range authentication interaction of token 110 with sensor 135 may then take place, for example, via NFC or Bluetooth. An authentication challenge may be issued by reader 130, which token 110 may respond to using the authentication information provided therein. For example, reader 130 may issue a random number to token 110, and token 110 may respond by signing the random number using a private key, or encrypting the random number using a symmetric encryption key, or by computing a hash, for example, as described above in connection with a pairing interaction, and providing an authentication response to reader 130 in return. Such a challenge-response communication may be referred to as an authentication interaction.

[0042] Token 110 may, in at least some embodiments, be configured to participate in authenticating interactions whether it is attached to clip 120 or no. For example where a communication interface between sensor 135 and token 110 has a range of a few meters, such as Bluetooth, the authenticating interaction may proceed and complete as the user merely walks past reader 130. Pairing interactions and authenticating interactions are examples of security operations.

[0043] Token 110 may be configured, as described above, to transmit challenges to clip 120 periodically or randomly, such that token 110 is enabled to detect whether it has been removed from proximity of clip 120. For example, a challenge may be transmitted every minute, every 30 seconds or every 10 seconds, for example. In case the response to the pairing challenge is not received in token 110, or the response is incorrect, token 110 may determine the pairing with clip 120 to be interrupted. The pairing may be interrupted in case the user has removed token 110 from the proximity of clip 120 to perform an

authentication interaction, for example. In such a case, the pairing will resume once token 110 is returned to the proximity of clip 120 and the interruption of the pairing will cease. The ceasing of the interruption of the pairing may be determined in token 110, for example by receipt of a valid response to a pairing challenge issued by token 110.

- 5 **[0044]** In some embodiments, once token 110 determines the pairing has been interrupted, token 110 will increase the frequency at which pairing challenges are issued, so that token 110 becomes aware of a resumed pairing with clip 120 as early as possible. The frequency of pairing challenges may be doubled, for example, in such an increase.

- 10 **[0045]** Token 110 may be furnished with a threshold length of time, to which token 110 may compare a length of an interruption of the pairing. The threshold may be selected to allow completing a normal authenticating interaction, for example by setting this threshold to 30 seconds, 1 minute or 2 minutes, for example.

- 15 **[0046]** In case token 110 determines that an interruption of the pairing with clip 120 has lasted for longer than the threshold length of time, token 110 may delete or otherwise render useless, that is, destroy, the authentication information in token 110. For example, token 110 may determine the interruption has lasted longer than the threshold length of time, in case a length of time between two failed pairing challenges exceeds the threshold length of time, such that there is no successful pairing challenge thereinbetween. A failed pairing challenge may comprise a pairing challenge issued by token 110 to which token 20 110 received no valid pairing response. Thus, in case token 110 is stolen, it will become inactive after the threshold length of time and the thief will thereafter not be able to abuse token 110 to access the resources controlled by token 110. Token 110 may destroy the authentication information by deleting it, or by overwriting it, at least in part, with other information, such as random bits.

- 25 **[0047]** In some embodiments, rather than increasing a frequency of pairing challenges as a response to a determination the pairing is interrupted, token 110 is configured to not issue any pairing challenges until shortly before, for example ten or fifteen seconds before, the threshold length of time has elapsed. This would serve to conserve battery resources in token 110.

- 30 **[0048]** In some embodiments, token 110 is configured to destroy the authentication information responsive to receiving several incorrect pairing responses purportedly from

clip 120. This prevents guessing to manipulate token 110 to remain in a “paired” state and prevent destruction of the authentication information. Pairing responses may also be incorrect if token 110 is brought into proximity of another clip than the one with which token 110 is paired, since this clip will not have the secret information used to compute the correct pairing responses.

[0049] In some embodiments, clip 120 is likewise configured to detect a pairing interruption, and to destroy authentication information in the clip. Clip 120 may be configured to destroy its authentication information after a longer time than the token, clip 120 may wait for 12 hours, for example, before destroying its authentication information.

[0050] In some embodiments, token 110 comprises a fingerprint reader, and the user is required to provide a fingerprint via the fingerprint reader in connection with an authenticating interaction performed with token 110. In some embodiments, clip 120 comprises a fingerprint reader, and the user is required to provide a fingerprint via the fingerprint reader in connection with an authenticating interaction performed with clip 120. In some embodiments, the fingerprint reader is in reader 130, rather than token 110 and/or clip 120.

[0051] In some embodiments, clip 120 has a body sensor, for example a body heat sensor or heartbeat sensor, to detect whether clip 120 is worn by a user. Responsive to a determination clip 120 is no longer worn, clip 120 may cease responding to pairing challenges from token 120, to thereby cause the token to destroy its authentication information. In such a case, clip 120 may also destroy the clip authentication information stored in clip 120. To facilitate operation of the heartbeat sensor, clip 120 may be worn as a wrist device, for example. In some embodiments, token 110 is configured to destroy the authentication information stored in token 110 responsive to an attempt to tamper with token 110.

[0052] FIGURE 2 illustrates state transitions of token 110 in accordance with at least some embodiments of the present invention. A token is in an inactive state 210 when it is not in use, in other words, it does not store authentication information of a user, and it is not paired with a clip 120. This may correspond, for example to a situation where the token is stored overnight.

[0053] A transition from inactive state 210 to paired state 220 may correspond to the token being taken into use, for example at the linking station described above. In connection with this state transition, the token may become paired with a clip, become furnished with the authentication information and the secret shared with the clip paired with the token.

[0054] In paired state 220, the token may transmit pairing challenges to the paired clip, for example via a short-range communication interface, and receive pairing responses from the clip, for example via the short-range communication interface, to maintain the pairing, as described above. In paired state 220, the token may participate in authentication interactions, as described above.

[0055] Once a pairing challenge fails, for example due to a missing pairing response or an incorrect pairing response, the token transitions from paired state 220 to pairing interrupted state 230. An incorrect pairing response may occur occasionally due to an air interface error in a short-range communication interface, for example, wherefore each incorrect pairing response is not necessarily an indication of foul play.

[0056] In pairing interrupted state 230, the token may participate in authenticating interactions, for example, if the user has momentarily removed the token from the paired clip to touch a reader device, to gain access to controlled resources. In the pairing interrupted state 230, the token may keep track of a duration of the interruption of the pairing. In case the pairing is resumed before the threshold length of time expires in interrupted state, the token returns to paired state 220. In case the threshold length of time does expire in the pairing interrupted state 230, the token may destroy the authentication information and return to inactive state 210, to prevent misuse of a stolen or lost token, as described above.

[0057] A resumption of the pairing may be determined by the token by receipt of a correct pairing response, for example. A frequency at which pairing challenges are transmitted from the token in pairing interrupted state 230 may be higher than in paired state 220.

[0058] An unauthorized person desiring access to the controlled resource or area would thus need to steal the clip and the token, together, inside the facility as the two are not, in at least some embodiments, present paired together outside of the facility. The clip

may be attached to the user's clothing, making its theft more difficult to accomplish unnoticed.

[0059] 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 token 110 or clip 120 of FIGURE 1. Comprised in device 300 is processor 310, which may comprise, for example, a microcontroller or 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-A, Cortex-M or Cortex-R processing core of 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.

[0060] 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. Memory 320 may comprise a secure element.

[0061] 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 a suitable communication 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 Bluetooth, wireless local area network, WLAN, and/or worldwide interoperability for microwave access, WiMAX, standards, for example.

- 5 **[0062]** 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.

- 10 **[0063]** 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 input a fingerprint in connection with an authenticating interaction.

- 15 **[0064]** 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
20 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.

- 25 **[0065]** Device 300 may comprise further devices 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
30 lacks at least one device described above.

[0066] Processor 310, memory 320, transmitter 330, receiver 340, NFC transceiver 350 and/or UI 360 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.

[0067] FIGURE 4 illustrates signalling in accordance with at least some embodiments of the present invention. On the vertical axes are disposed, from the left, linking station LS, clip 120, token 110 and finally reader 130 on the right. Time advances from the top toward the bottom.

[0068] In phase 410, clip 120 and token 110 are paired with each other, facilitated in this embodiment by linking station LS. The pairing may comprise, for example, as described above, that a shared secret is stored both in clip 120 and token 110. The pairing may comprise, as described above, provision of authentication information specific to the user in token 110.

[0069] Phase 420 comprises a pairing challenge-response transaction between clip 120 and token 110, which is used to maintain the pairing. Token 110 issues a pairing challenge 422, to which clip 120 responds by transmitting a pairing response, 424. Responsive to the response being correct, token 110 maintains itself in a paired state.

[0070] Pairing challenge 430, in the illustrated example, is not responded to, in other words, token 110 receives no response to pairing challenge 430. This may be due to clip 120 being out of range of a communication interface token 110 and clip 120 use to maintain the pairing, which, as described above, may comprise a short-range communication interface. Token 110 may determine the response has not arrived, for example, by determining the response has not arrived within a time limit configured in token 110 for this purpose. Responsively, in phase 435, token 110 determines the pairing with clip 120 has been interrupted.

[0071] During the pairing interruption, token 110 may participate in an authenticating interaction 440 with reader 130. Authenticating interaction 440 may

comprise an authentication challenge issued by reader 130, to which token 110 responds, wherein the authentication information in token 110 may be employed in deriving the response from information comprised in the challenge. Responsive to a correct authentication response, reader 130 may provide the user access to controlled resources,
5 for example.

[0072] Following the authentication interaction, the user may replace token 110 at clip 120. As proximity is thereby restored, the next pairing interaction 450 may succeed, in other words, token 110 may receive a correct pairing response 454 to pairing challenge 452 comprised in pairing interaction 450. As a response, token 110 may determine, phase 460,
10 the pairing with clip 120 has resumed and the interruption has ceased.

[0073] In the example illustrated in FIGURE 4, the interruption of the pairing of clip 120 with token 110 did not exceed the threshold length of time, wherefore token 110 did not destroy the authentication information stored therein.

[0074] FIGURE 5 is a flow graph of a method in accordance with at least some
15 embodiments of the present invention. The phases of the illustrated method may be performed in token 110, or in a control device configured to control the functioning thereof, when installed therein.

[0075] Phase 510 comprises, in connection with establishing a pairing of an apparatus with a device, storing authentication information in a memory of the apparatus
20 and establishing a shared secret with the device. Phase 520 comprises determining, using at least one cryptographic challenge, whether the pairing has been interrupted, and responsive to the pairing being determined to be interrupted for a length of time exceeding a threshold length of time, destroying the authentication information.

[0076] FIGURE 6 is a flow graph of a method in accordance with at least some
25 embodiments of the present invention. The phases of the illustrated method may be performed in clip 120, or in a control device configured to control the functioning thereof, when installed therein.

[0077] Phase 610 comprises storing authentication information. Phase 620 comprises, in connection with establishing a pairing of an apparatus with an access token,
30 establishing a shared secret with the access token. Phase 630 comprises participating in maintaining the pairing by responding to at least one cryptographic challenge from the

access token. Finally, phase 640 comprises participating in an authenticating interaction, based at least partly on the authentication information, when the pairing is not present.

[0078] 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.

[0079] 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.

[0080] 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.

[0081] 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.

[0082] 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.

[0083] 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

[0084] At least some embodiments of the present invention find industrial application in authentication solutions.

ACRONYMS LIST

AES	advanced encryption standard
I ² C	Inter-Integrated Circuit
NFC	near-field communication
UART	universal asynchronous receiver/transmitter

REFERENCE SIGNS LIST

110	Token
120	clip
130	Reader
135	Sensor
110C	pairing challenge
120R	pairing response
210, 220, 230	states in the diagram of FIGURE 2

300 – 360	Structure of the apparatus of FIGURE 3
410 – 460	Signaling phases of FIGURE 4
510 – 520	Phases of the method of FIGURE 5
610 – 640	Phases of the method of FIGURE 6

CLAIMS:

1. An apparatus comprising:
 - 5 – a memory configured to store authentication information;
 - at least one processing core configured to:
 - in connection with establishing a pairing of the apparatus with a device, store the authentication information in the memory and establish a shared secret with the device, and
 - 10 ▪ determine, using at least one cryptographic challenge, whether the pairing has been interrupted, and responsive to the pairing being determined to be interrupted for a length of time exceeding a threshold length of time, destroy the authentication information.
- 15 2. The apparatus according to claim 1, wherein the memory comprises a secured memory, the at least one processor being configured to store the authentication information in the secured memory.
- 20 3. The apparatus according to any of claims 1 – 2, wherein the apparatus is configured to receive the authentication information from a base unit.
- 25 4. The apparatus according to any of claims 1 – 3, wherein the apparatus is configured to participate in an authenticating interaction in a state where the pairing has been interrupted and when the interruption has lasted for less than the threshold length of time.
5. The apparatus according to claim 4, wherein the apparatus is configured to require at least one of biometric authentication, pin-code authentication and two-factor authentication in connection with participating in the authenticating interaction.
- 30 6. The apparatus according to any of claims 1 – 5, wherein the apparatus comprises a first battery and a second battery.

7. The apparatus according to claim 6, wherein the at least one processing core is configured to use electrical power from the second battery when performing security operations.
- 5 8. The apparatus according to any of claims 6 – 7, wherein the at least one processing core is configured to use electrical power from the second battery to destroy the authentication information responsive to a charge level of the first battery declining below a charge threshold.
- 10 9. The apparatus according to any of claims 1 – 8, wherein the apparatus comprises a body sensor, and the at least one processing core is configured to destroy the authentication information responsive to a determination, based at least in part on the body sensor, that the apparatus has been removed from a user's body for a time period exceeding a second threshold length of time.
- 15 10. The apparatus according to any of claims 1 – 9, wherein the authentication information comprises a public key – private key pair of a public-key cryptosystem.
11. An apparatus comprising:
- 20 – a memory configured to store authentication information;
- at least one processing core configured to:
- in connection with establishing a pairing of the apparatus with an access token, establish a shared secret with the access token;
- participate in maintaining the pairing by responding to at least one
- 25 cryptographic challenge from the access token, and
- participate in an authenticating interaction, based at least partly on the authentication information, when the pairing is not present.
12. The apparatus according to claim 11, wherein the authentication information comprises
- 30 a public key – private key pair of a public-key cryptosystem.
13. The apparatus according to any of claims 11 – 12, wherein the at least one processing core is configured to, in connection with responding to each of the at least one cryptographic challenge, calculate a hash value using at least the shared secret as input.

14. A method, comprising:

- in connection with establishing a pairing of an apparatus with a device, storing authentication information in a memory of the apparatus and establishing a shared secret with the device, and
- determining, using at least one cryptographic challenge, whether the pairing has been interrupted, and responsive to the pairing being determined to be interrupted for a length of time exceeding a threshold length of time, destroying the authentication information.

15. The method according to claim 14, wherein the memory comprises a secured memory, and the authentication information is stored in the secured memory.

16. The method according to any of claims 14 – 15, further comprising receiving the authentication information from a base unit.

17. The method according to any of claims 14 – 16, further comprising participating in an authenticating interaction in a state where the pairing has been interrupted and when the interruption has lasted for less than the threshold length of time.

18. The method according to claim 17, further comprising requiring at least one of biometric authentication, pin-code authentication and two-factor authentication in connection with participating in the authenticating interaction.

19. The method according to any of claims 14 – 18, comprising using a first battery and a second battery of the apparatus.

20. The method according to claim 19, further comprising using electrical power from the second battery when performing security operations.

21. The method according to any of claims 19 – 20, further comprising using electrical power from the second battery to destroy the authentication information responsive to a charge level of the first battery declining below a charge threshold.

22. The method according to any of claims 14 – 21, wherein the apparatus comprises a body sensor, and the method further comprises destroying the authentication information responsive to a determination, based at least in part on the body sensor, that the apparatus has been removed from a user's body for a time period exceeding a second threshold
5 length of time.

23. The method according to any of claims 14 – 22, wherein the authentication information comprises a public key – private key pair of a public-key cryptosystem.

10 24. A method comprising:

- storing authentication information;
- in connection with establishing a pairing of an apparatus with an access token, establishing a shared secret with the access token;
- participating in maintaining the pairing by responding to at least one cryptographic
15 challenge from the access token, and
- participating in an authenticating interaction, based at least partly on the authentication information, when the pairing is not present.

25. The method according to claim 24, wherein the authentication information comprises a
20 public key – private key pair of a public-key cryptosystem.

26. The method according to any of claims 24 – 25, further comprising, in connection with responding to each of the at least one cryptographic challenge, calculating a hash value using at least the shared secret as input.

25

27. A system comprising at least one first apparatus according to at least one of claims 1 – 10 and at least one second apparatus according to at least one of claims 11 – 13.

28. An apparatus comprising:

- 30 – means for, in connection with establishing a pairing of the apparatus with a device, storing authentication information in a memory of the apparatus and establishing a shared secret with the device, and

- means for determining, using at least one cryptographic challenge, whether the pairing has been interrupted, and responsive to the pairing being determined to be interrupted for a length of time exceeding a threshold length of time, destroying the authentication information.

5

29. An apparatus comprising:

- means for storing authentication information;
- means for, in connection with establishing a pairing of an apparatus with an access token, establishing a shared secret with the access token;
- 10 – means for participating in maintaining the pairing by responding to at least one cryptographic challenge from the access token, and
- means for participating in an authenticating interaction, based at least partly on the authentication information, in a state when the pairing is not present.

15 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:

- in connection with establishing a pairing of an apparatus with a device, store authentication information in a memory of the apparatus and establish a shared
- 20 secret with the device, and
- determine, using at least one cryptographic challenge, whether the pairing has been interrupted, and responsive to the pairing being determined to be interrupted for a length of time exceeding a threshold length of time, destroy the authentication information.

25

31. 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 authentication information;
- 30 – in connection with establishing a pairing of an apparatus with an access token, establish a shared secret with the access token;
- participate in maintaining the pairing by responding to at least one cryptographic challenge from the access token, and

- participate in an authenticating interaction, based at least partly on the authentication information, in a state when the pairing is not present.

32. A computer program configured to cause a method in accordance with at least one of
5 claims 14 - 26 to be performed.

1/6

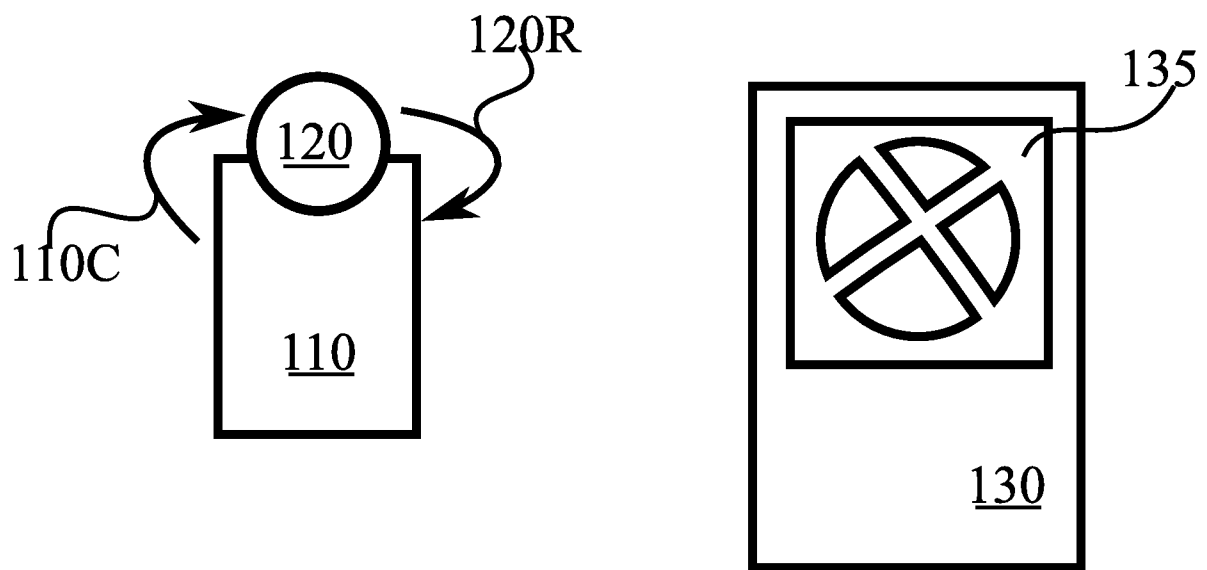


FIGURE 1A

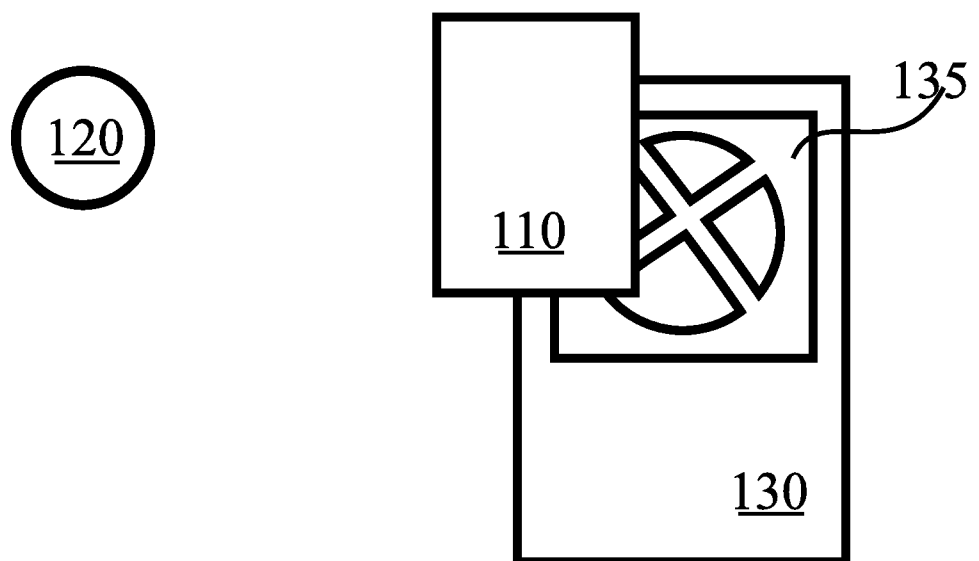


FIGURE 1B

2/6

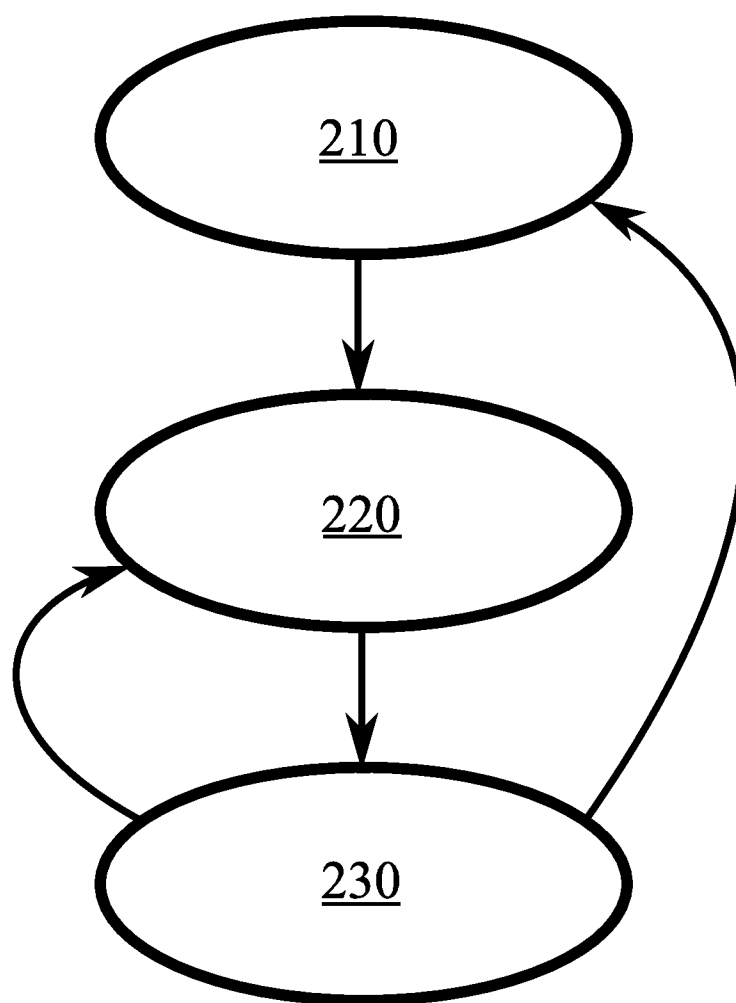


FIGURE 2

3/6

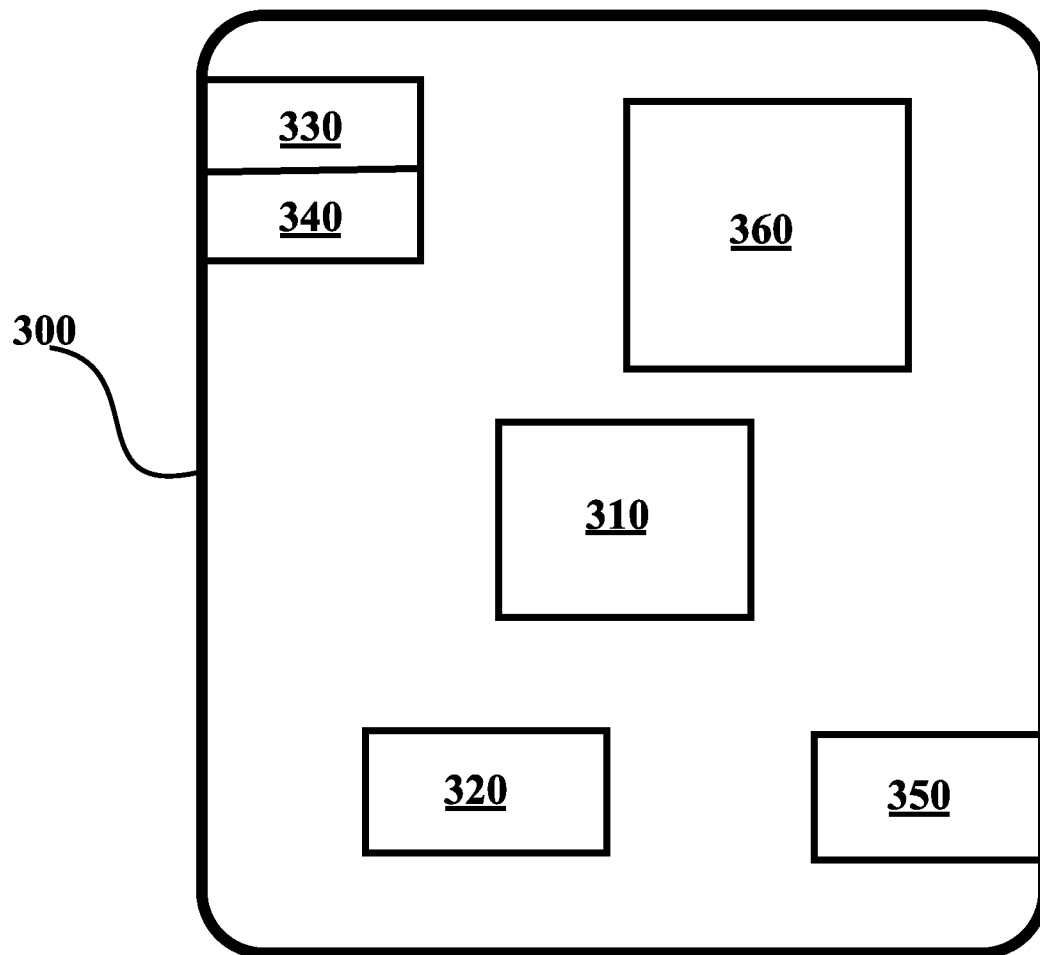


FIGURE 3

4/6

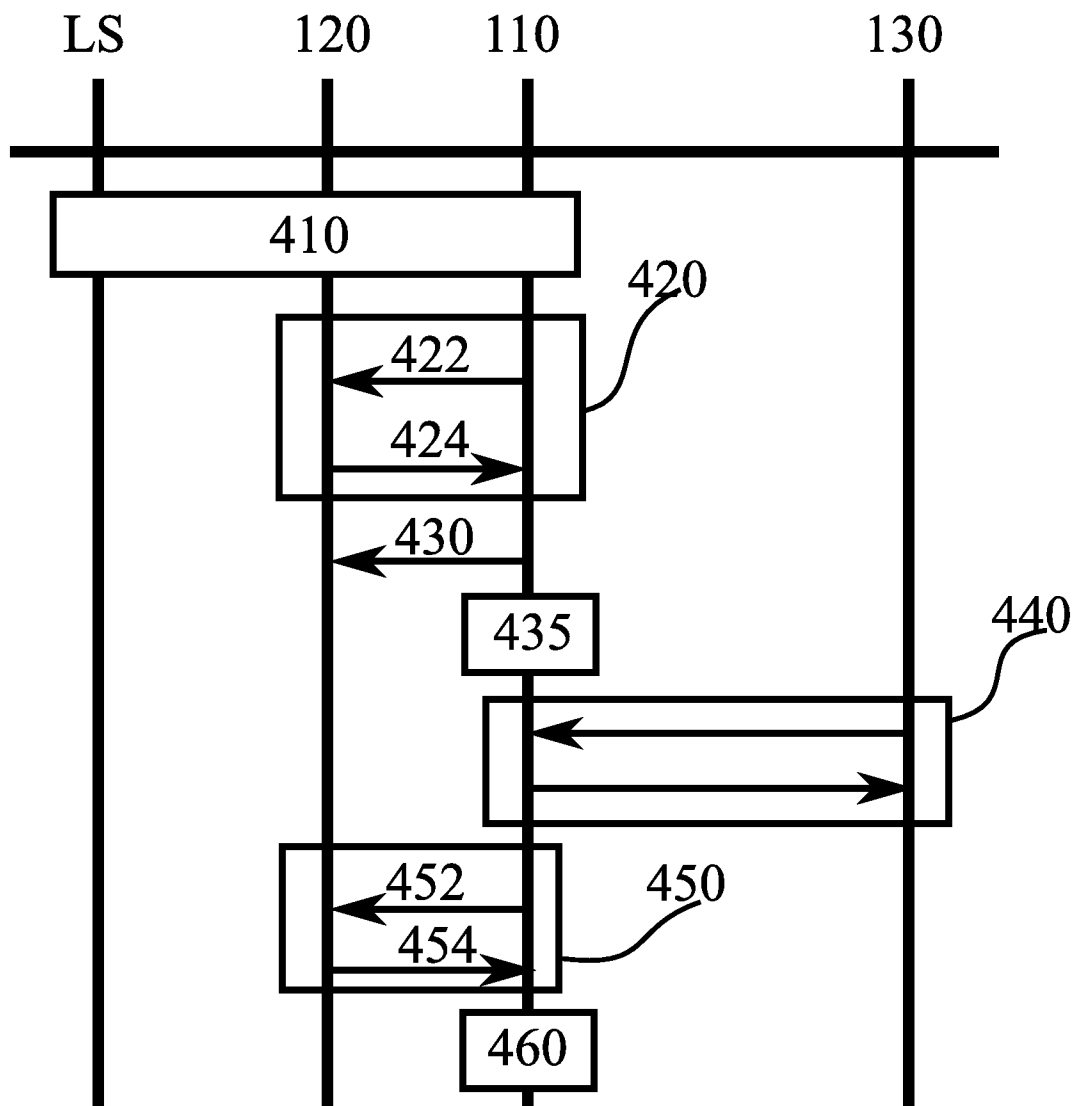


FIGURE 4

5/6

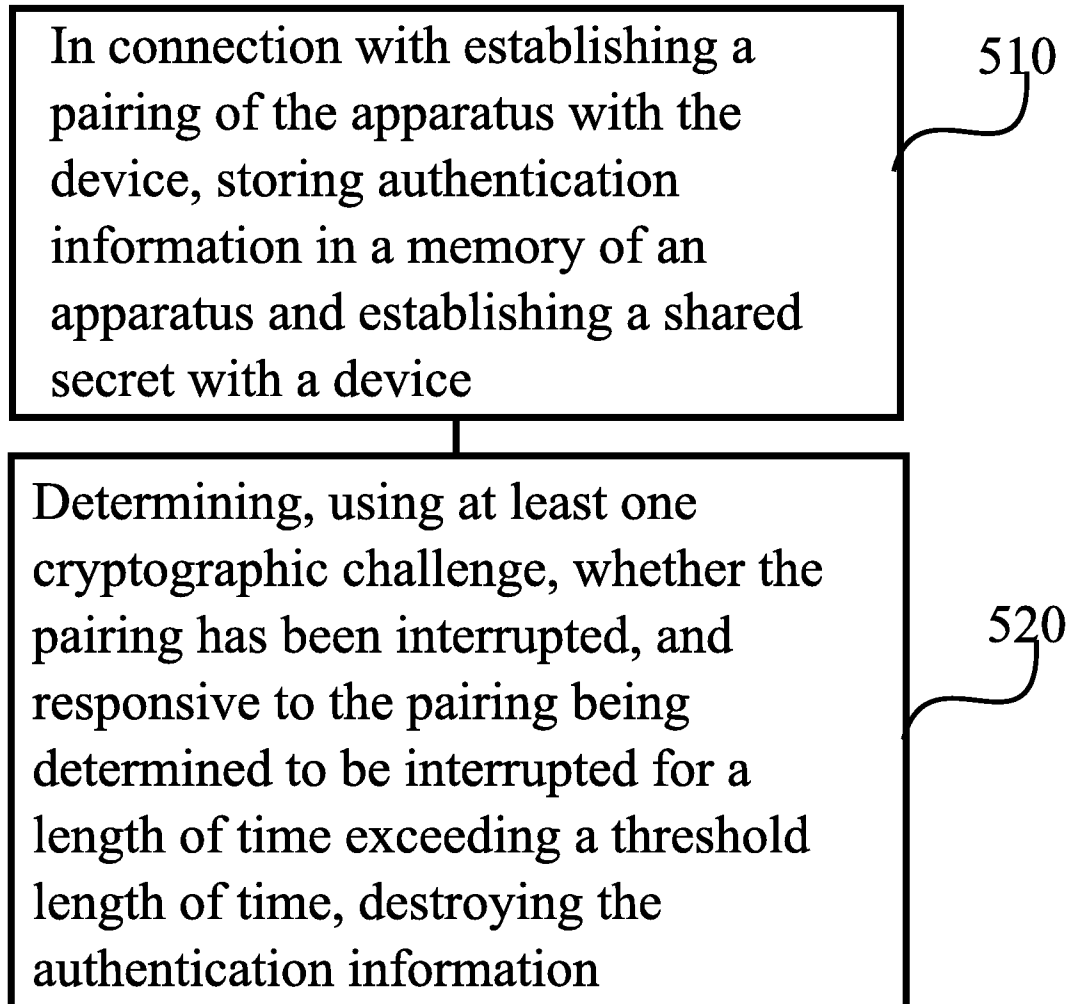


FIGURE 5

6/6

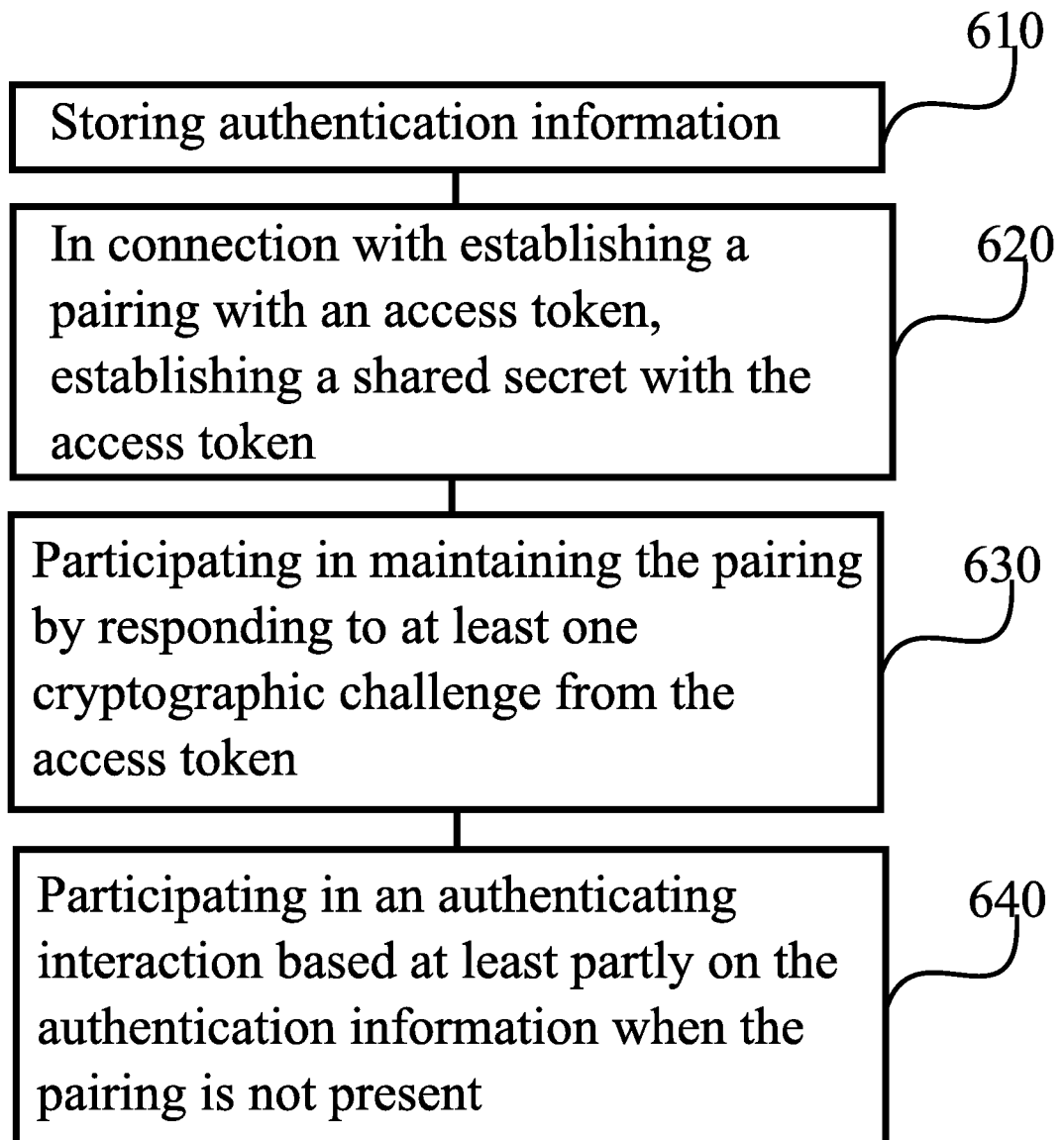


FIGURE 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI2017/050221

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: 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, WPIAP, XPAIP, XPESP, XPI3E, XPIEE, XPIOP, XPIPCOM, XPMISC, XPOAC, XPRD, XPTK, COMPDX, INSPEC, PUBCOMP, PUBSUBS, TDB, NPL

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014230019 A1 (CIVELLI JAY PIERRE [US] et al.) 14 August 2014 (14.08.2014) Fig. 2; paragraphs [0015], [0017], [0023], [0024], [0026]	1-32
A	US 2016092665 A1 (COWAN MELISSA A [US] et al.) 31 March 2016 (31.03.2016) Abstract	

☐ 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

02 August 2017 (02.08.2017)

Date of mailing of the international search report

03 August 2017 (03.08.2017)

Name and mailing address of the ISA/FI
Finnish Patent and Registration Office
P.O. Box 1160, FI-00101 HELSINKI, Finland
Facsimile No. +358 29 509 5328

Authorized officer
Vesa-Matti Louekoski
Telephone No. +358 29 509 5000

INTERNATIONAL SEARCH REPORT
Information on Patent Family Members

International application No.
PCT/FI2017/050221

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
US 2014230019 A1	14/08/2014	WO 2014126987 A1	21/08/2014
.....			
US 2016092665 A1	31/03/2016	TW 201626276 A	16/07/2016
.....			

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI2017/050221

CLASSIFICATION OF SUBJECT MATTER

IPC

G06F 21/34 (2013.01)

G07C 9/00 (2006.01)

G06F 21/35 (2013.01)