Innovation, Sciences et Développement économique Canada
Office de la Propriété Intellectuelle du Canada

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

CA 3014748 A1 2017/08/31

(21) 3 014 748

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2017/02/14
(87) Date publication PCT/PCT Publication Date: 2017/08/31
(85) Entrée phase nationale/National Entry: 2018/08/15
(86) N° demande PCT/PCT Application No.: IB 2017/050815
(87) N° publication PCT/PCT Publication No.: 2017/145002
(30) Priorités/Priorities: 2016/02/23 (GB1603122.1); 2016/02/23 (GB1603117.1); 2016/11/15 (GB1619301.3)

(51) Cl.Int./Int.Cl. *G06Q 20/38* (2012.01), *H04L 9/08* (2006.01), *H04L 9/30* (2006.01), *H04L 9/32* (2006.01)

(71) Demandeur/Applicant:
NCHAIN HOLDINGS LIMITED, AG

(72) Inventeurs/Inventors:
WRIGHT, CRAIG STEVEN, GB;
SAVANAH, STEPHANE, GB

(74) Agent: PARLEE MCLAWS LLP

(54) Titre : SECURITE D'UN DISPOSITIF PERSONNEL UTILISANT UNE CRYPTOGRAPHIE A COURBE ELLIPTIQUE POUR LE PARTAGE DE SECRETS

(54) Title: PERSONAL DEVICE SECURITY USING ELLIPTIC CURVE CRYPTOGRAPHY FOR SECRET SHARING

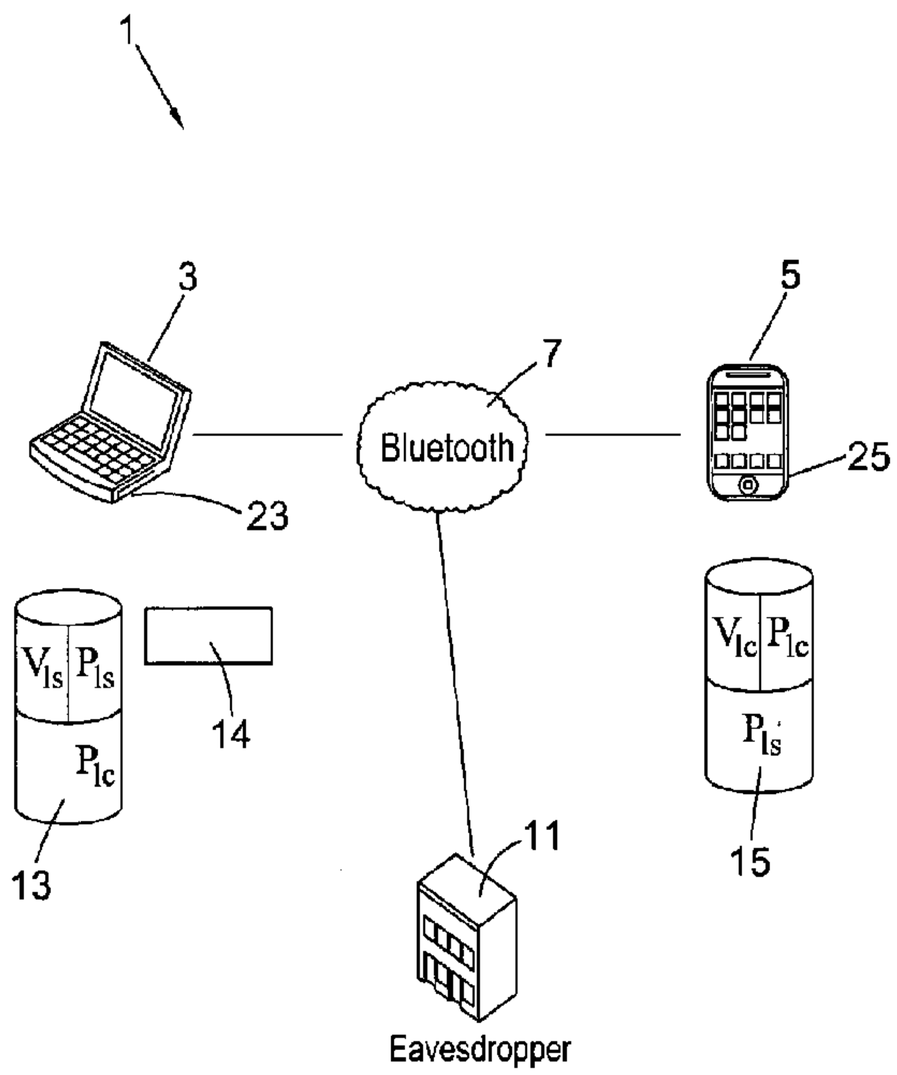


Fig. 1

(57) Abrégé/Abstract:
A method (400) of encrypting data at an electronic device (3) where the electronic device is associated with a key device (5). Each device is associated with an asymmetric cryptography pair, each pair including a first private key and a first public key. Respective second private and public keys may be determined based on the first private key, first public key and a deterministic key. A secret may be determined based on the second private and public keys. The data at the electronic device (3) may be encrypted using the determined secret or an encryption key that is based on the secret. Information indicative of the deterministic key may be sent to the key device (5) where the information may be stored.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 August 2017 (31.08.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/145002 A1

(51) **International Patent Classification**:
G06Q 20/38 (2012.01) ***H04L 9/32*** (2006.01)
H04L 9/30 (2006.01) ***H04L 9/08*** (2006.01)

(21) **International Application Number**:
PCT/IB2017/050815

(22) **International Filing Date**:
14 February 2017 (14.02.2017)

(25) **Filing Language**: English

(26) **Publication Language**: English

(30) **Priority Data**:

1603117.1	23 February 2016 (23.02.2016)	GB
1603122.1	23 February 2016 (23.02.2016)	GB
1619301.3	15 November 2016 (15.11.2016)	GB

(71) **Applicant**: **NCHAIN HOLDINGS LIMITED** [AG/AG]; Fitzgerald House, 44 Church Street, St. John's (AG).

(72) **Inventors**: **WRIGHT, Craig Steven**; c/o Urquhart-Dykes & Lord LLP, 7th Floor Churchill House, Churchill Way, Cardiff CF10 2HH (GB). **SAVANAH, Stephane**; c/o Urquhart-Dykes & Lord LLP, 7th Floor Churchill House, Churchill Way, Cardiff CF10 2HH (GB).

(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).

Published:

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

(54) Title: PERSONAL DEVICE SECURITY USING ELLIPTIC CURVE CRYPTOGRAPHY FOR SECRET SHARING

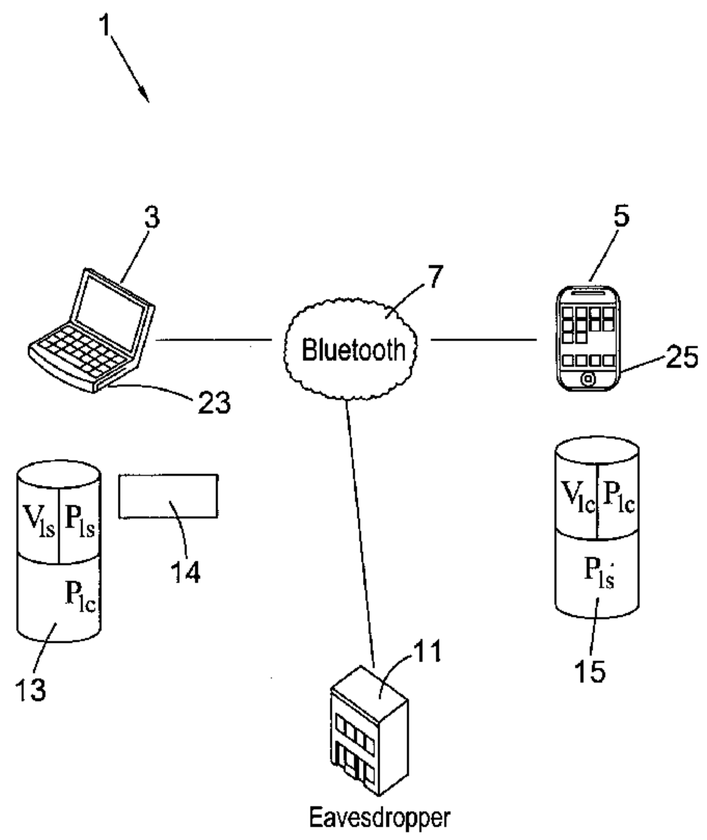


Fig. 1

(57) Abstract: A method (400) of encrypting data at an electronic device (3) where the electronic device is associated with a key device (5). Each device is associated with an asymmetric cryptography pair, each pair including a first private key and a first public key. Respective second private and public keys may be determined based on the first private key, first public key and a deterministic key. A secret may be determined based on the second private and public keys. The data at the electronic device (3) may be encrypted using the determined secret or an encryption key that is based on the secret. Information indicative of the deterministic key may be sent to the key device (5) where the information may be stored.

WO 2017/145002 A1

"Personal device security using Elliptic Curve Cryptography for secret sharing"

Technical Field

[0001] The present disclosure relates generally to the field of computer-related security and also encryption. More particularly, it provides a method, a system and a device for encrypting data stored on an electronic device. It is particularly suited for enhancing security on personal computing devices including, but not limited to, mobile phones, tablet devices or laptops. The present disclosure further relates to a method, a system and a device for decrypting the encrypted data.

Background

[0002] Cryptography involves techniques for protecting data on a hard disk of an electronic device, for example in the event that the electronic device is lost or stolen. An electronic device may include a laptop computer, a desktop computer, a tablet computer, a mobile communication device and any other form of computing device. The electronic device may be associated with a natural person, a group of people such as employees of a company, a system such as a banking system, etc.

[0003] In some cases, the data on a hard disk of the electronic device may be protected by a password, passphrase or a PIN. However, short codes such as 4-8 character PINs can easily be determined by trialling different combinations of characters. Passwords and passphrases may be more secure than PINs. However, the level of security depends on the user memorising a lengthy set of code words or a sentence.

[0004] In other cases, a cryptographic key may be used to protect the data on the hard disk of the electronic device. The cryptographic key may be stored on a USB drive which needs to be physically connected to the electronic device to transmit the cryptographic key. However, due to electromagnetic signals that are generated during the transmission of the cryptographic key from the USB drive to the electronic device, the transmitted key may still be obtained by a third party.

[0005] Therefore a problem in such cryptographic data protection is the transmission of the secret key to the electronic device.

[0006] Any discussion of documents, acts, materials, devices, articles or the like which has been included in the present specification is not to be taken as an admission that any or all of these matters form part of the prior art base or were common general knowledge in the field relevant to the present disclosure as it existed before the priority date of each claim of this application.

[0007] Throughout this specification the word "comprise", or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated element, integer or step, or group of elements, integers or steps, but not the exclusion of any other element, integer or step, or group of elements, integers or steps.

[0008] The following documents provide background material relating to the technological background of the present invention: WO2015/175854 A2, CN103440209 B, US2007055880, US2010023771, DE102010002241, US2012011362, US2012100833, US2012331287, WO2013053058, US8522011, US2014082358, US2015213433 and EP2975570.

Summary

[0009] The invention may provide a computer implemented method. It may provide a security method. It may provide a method of encrypting data at an electronic device (S), the electronic device being associated with a key device (C). The electronic device may be further associated with a first asymmetric cryptography pair having a first electronic device private key (V_{1S}) and a first electronic device public key (P_{1S}), and the key device may be associated with a second asymmetric cryptography pair having a first key device private key (V_{1C}) and a first key device public key (P_{1C});

[0010] The method may comprise the steps of:

- determining, at the electronic device, a deterministic key (DK);

- receiving, at the electronic device, the first key device public key (P_{1C}) from the key device;

- determining, at the electronic device, a second electronic device private key (V_{2S}) based on at least the first electronic device private key (V_{1S}) and the deterministic key (DK), and

- determining, at the electronic device, a second key device public key (P_{2C}) based on at least the first key device public key (P_{1C}) and the deterministic key (DK);

- determining a secret based on at least the second electronic device private key (V_{2S}) and the second key device public key (P_{2C});

- encrypting the data at the electronic device using the determined secret or an encryption key that is based on the determined secret; and/or

- sending information indicative of the deterministic key (DK) to the key device where the information can be stored.

[0011] The method may further comprise storing, at the key device, the information indicative of the deterministic key (DK).

[0012] The deterministic key (DK) may be based on a message (M). The method may comprise a step of generating the message (M) at the electronic device. The method may further comprise determining the deterministic key (DK) based on determining a hash of the message (M). The step of storing information indicative of the deterministic key on the key device may comprise storing the message (M) on the key device.

[0013] The method may comprise determining a second electronic device public key (P_{2S}) based on at least the first electronic device public key (P_{1S}) and the deterministic key (DK).

[0014] The method may also comprise: sending from the electronic device to the key device, a notice indicative of using a common elliptic curve cryptography (ECC) system with a common generator (G).

[0015] The first electronic device public key (P_{1S}) and the first key device public key (P_{1C}) may be based on elliptic curve point multiplication of the respective first electronic device private key (V_{1S}) and first key device private key (V_{1C}) and the common generator (G).

[0016] The method may comprise generating the first electronic device private key (V_{1S}) and the first electronic device public key (P_{1S}). For example, the first electronic device private key (V_{1S}) may be generated based on a random integer in an allowable range specified in the common ECC system; and the first electronic device public key (P_{1S}) may be generated based on elliptic curve point multiplication of the first electronic device private key (V_{1C}) and the common generator (G) according to the following formula:

$$P_{1S} = V_{1S} \times G$$

[0017] The second electronic device private key (V_{2S}) may be based on a scalar addition of the first electronic device private key (V_{1S}) and the deterministic key (DK) according to the following formula:

$$V_{2S} = V_{1S} + DK$$

[0018] The second electronic device public key (P_{2S}) may be based on at least the first electronic device public key (P_{1S}) with elliptic curve point addition to the deterministic key (DK). In a specific example, the second electronic device public key (P_{2S}) may be based on the first electronic device public key (P_{1S}) with elliptic curve point addition to the elliptic curve point multiplication of the deterministic key (DK) and the common generator (G) according to the following formula:

$$P_{2S} = P_{1S} + DK \times G.$$

[0019] The second key device public key (P_{2C}) may be based on at least the first key device public key (P_{1C}) with elliptic curve point addition to the deterministic key (DK). In a specific example, the second key device public key (P_{2C}) may be based on the first key device public key (P_{1C}) with elliptic curve point addition to the elliptic curve point multiplication of the deterministic key (DK) and the common generator (G) according to the following formula:

$$P_{2C} = P_{1C} + DK \times G$$

[0020] The method may comprise determining the encryption key based on the determined secret. For example, the encryption key may be based on the secret and identification

information of the electronic device. The identification information may comprise a serial number of the electronic device.

[0021] The method may comprise connecting the electronic device with the key device to be in communication with each other. For example, the electronic device may be connected to the key device via a wireless protocol, such as Bluetooth or a communications network, for example the internet, or a local communications network. Alternatively, the electronic device may be connected to the key device by virtue of a wire, for example via cable or a suitable port of the electronic device.

[0022] The method may further comprise storing, at a data storage associated with the electronic device, the first key device public key (P_{1C}).

[0023] Additionally or alternatively, the invention may provide a computer implemented method of decrypting data at an electronic device, the data being encrypted in accordance with the method of encrypting data as described above, the method of decrypted the data comprising:

receiving, at the electronic device, the information indicative of the deterministic key (DK), from the key device;

determining the secret based on the received information indicative of the deterministic key (DK); and

decrypting, at the electronic device, the encrypted data using the secret or the encryption key that is based on the secret.

[0024] The method may comprise authenticating the key device. For this, the method may comprise generating, at the electronic device, an authentication message (M_A) and sending the authentication message (M_A) to the key device.

[0025] The method may comprise generating, at the key device, a second asymmetric cryptography pair having a second key device private key (V_{2C}) and a second key device public key (P_{2C}). The second key device private key (V_{2C}) may be based on a deterministic authentication key (DK_A) and the first key device private key (V_{1C}). The second key device

public key (P_{2C}) may be based on the deterministic authentication key (DK_A) and the first key device public key (P_{1C}).

[0026] The method may comprise determining the deterministic authentication key (DK_A). For example, the deterministic authentication key (DK_A) may be determined based on the authentication message (M_A), such as by determining a hash of the message (M_A).

[0027] The method may include generating, at the key device, a signed authentication message (SM_A) based on the deterministic authentication key (DK_A) and the second key device private key (V_{2C}).

[0028] The method may further include: receiving, at the electronic device, the signed authentication message (SM_A) from the key device; validating the signed message (SM_A) with the second key device public key (P_{2C}); and authenticating the key device based on the result of validating the signed authentication message (SM_A).

[0029] The method of decrypting the data may comprise requesting, at the electronic device, the information indicative of the deterministic key (DK) from the key device. In embodiments in which the information indicative of the deterministic key (DK) comprises the message (M), in response to receiving the request at the key device, the key device may generate a signed message (SM) based on the message (M) and send the signed message (SM) to the electronic device. The signed message (SM) may be generated based on the message (M) and the first or second key device private key.

[0030] The method of decrypting the data may further comprise validating, at the electronic device, the signed message (SM) and retrieving the message (M) such that the secret can be determined, at the electronic device, for decrypting the data.

[0031] The invention may also provide a computer-implemented system for implementation any aspect or embodiment of the method(s) described above. It may provide a computer system for encrypting data at an electronic device, the computer system comprising:

- the electronic device being associated with a first asymmetric cryptography pair having a first electronic device private key (V_{1S}) and a first electronic device public key (P_{1S}),

- a key device being associated with a second asymmetric cryptography pair having a first key device private key (V_{1C}) and a first key device public key (P_{1C});

- wherein the electronic device comprises a processor configured to:

    - determine a deterministic key (DK);

    - receive the first key device public key (P_{1C}) from the key device;

    - determine a second electronic device private key (V_{2S}) based on at least the first electronic device private key (V_{1S}) and the deterministic key (DK), and

    - determine a second key device public key (P_{2C}) based on at least the first key device public key (P_{1C}) and the deterministic key (DK);

    - determine a secret based on at least the second electronic device private key (V_{2S}) and the second key device public key (P_{2C}); and

    - encrypt the data on the electronic device using the determined secret or an encryption key that is based on the determined secret;

- wherein information indicative of the deterministic key (DK) is stored on the key device.

[0032] The deterministic key (DK) may be based on a message (M). The processor may be configured to generate the message (M). The processor may further be configured to determine the deterministic key (DK) based on determining a hash of the message (M).

[0033] The processor may be configured to determine a second electronic device public key (P_{2S}) based on at least the first electronic device public key (P_{1S}) and the deterministic key (DK).

[0034] In the system, the electronic device may comprise an interface and the key device may comprise a key device interface to establish communication between the electronic device and the key device. For example, the electronic device may be connected to the key

device via a wireless protocol, such as Bluetooth or a communications network, for example the internet, or a local communications network. Alternatively, the electronic device may be connected to the key device by virtue of a wire, for example via cable or a suitable port of the electronic device.

[0035] The interface of the electronic device may be configured to send a notice indicative of using a common elliptic curve cryptography (ECC) system with a common generator (G) to the key device interface of the associated key device.

[0036] The first electronic device public key (P_{1S}) and the first key device public key (P_{1C}) may be based on elliptic curve point multiplication of respective first electronic device private key (V_{1S}) and first key device private key (V_{1C}) and a generator (G).

[0037] The processor may be configured to generate the first electronic device private key (V_{1S}) and the first electronic device public key (P_{1S}). For example, the first electronic device private key (V_{1S}) may be generated based on a random integer in an allowable range specified in the common ECC system; and the first electronic device public key (P_{1S}) may be generated based on elliptic curve point multiplication of the first electronic device private key (V_{1C}) and the common generator (G) according to the following formula:

$$P_{1S} = V_{1S} \times G$$

[0038] The second electronic device private key (V_{2S}) may be based on a scalar addition of the first electronic device private key (V_{1S}) and the deterministic key (DK) according to the following formula:

$$V_{2S} = V_{1S} + DK$$

[0039] The second electronic device public key (P_{2S}) may be based on at least the first electronic device public key (P_{1S}) with elliptic curve point addition to the deterministic key (DK). In a specific example, the second electronic device public key (P_{2S}) may be based on the first electronic device public key (P_{1S}) with elliptic curve point addition to the elliptic curve point multiplication of the deterministic key (DK) and the common generator (G) according to the following formula:

$$P_{2S} = P_{1S} + DK \times G.$$

[0040] The second key device public key (P_{2C}) may be based on at least the first key device public key (P_{1C}) with elliptic curve point addition to the deterministic key (DK). In a specific example, the second key device public key (P_{2C}) may be based on the first key device public key (P_{1C}) with elliptic curve point addition to the elliptic curve point multiplication of the deterministic key (DK) and the common generator (G) according to the following formula:

$$P_{2C} = P_{1C} + DK \times G$$

[0041] The processor may be configured to determine the encryption key based on the determined secret. For example, the encryption key may be based on the determined secret and identification information of the electronic device. The identification information may comprise a serial number of the electronic device.

[0042] The electronic device may comprise a data storage in which the first key device public key (P_{1C}) may be stored.

[0043] The key device may comprise a key device data storage for storing at least the information indicative of the deterministic key.

[0044] The computer system as described above further configured to decrypt data, the processor of the electronic device being configured to:

receive the information indicative of the deterministic key (DK), from the key device;

determine the secret based on the information indicative of the deterministic key (DK); and

decrypt the data using the determined secret or the encryption key that is based on the determined secret.

[0045] The processor may be configured to authenticate the key device. For this, the processor may generate an authentication message (M_A) and send the authentication message (M_A) to the key device.

[0046] The key device may comprise a key device processor that may be configured to generate a second asymmetric cryptography pair having a second key device private key (V_{2C}) and a second key device public key (P_{2C}). The second key device private key (V_{2C}) may be based on a deterministic authentication key (DK_A) and the first key device private key (V_{1C}). The second key device public key (P_{2C}) may be based on the deterministic authentication key (DK_A) and the first key device public key (P_{1C}).

[0047] The key device processor may further be configured to determine the deterministic authentication key (DK_A). For example, the deterministic authentication key (DK_A) may be determined based on the authentication message (M_A), such as by determining a hash of the message (M_A).

[0048] The key device processor may be configured to generate a signed authentication message (SM_A) based on the deterministic authentication key (DK_A) and the second key device private key (V_{2C}).

[0049] The processor of the electronic device may be configured to: receive the signed authentication message (SM_A) from the key device; validate the signed message (SM_A) with the second key device public key (P_{2C}); and authenticate the key device based on the result of validating the signed authentication message (SM_A).

[0050] The processor of the electronic device may request the information indicative of the deterministic key (DK) from the key device. In embodiments in which the information indicative of the deterministic key (DK) comprises the message (M), in response to receiving the request at the key device, the key device processor may generate a signed message (SM) based on the message (M) and send the signed message (SM) to the electronic device. The signed message (SM) may be generated based on the message (M) and the first or second key device private key.

[0051] The processor of the electronic device may further be configured to validate the signed message and retrieving the message (M) such that the secret can be determined for decrypting the data.

[0052] An electronic device for encrypting data, the electronic device being associated with a key device, wherein the electronic device is associated with a first asymmetric cryptography pair having a first electronic device private key (V_{1S}) and a first electronic device public key (P_{1S}), and the key device is associated with a second asymmetric cryptography pair having a first key device private key (V_{1C}) and a first key device public key (P_{1C}); the electronic device comprising a processing device configured to:

- determine a deterministic key (DK);
- receive the first key device public key (P_{1C}) from the associated key device;
- determine a second electronic device private key (V_{2S}) based on at least the first electronic device private key (V_{1S}) and the deterministic key (DK), and
- determine a second key device public key (P_{2C}) based on at least the first key device public key (P_{1C}) and the deterministic key (DK);
- determine a secret based on at least the second electronic device private key (V_{2S}) and the second key device public key (P_{2C}); and
- encrypt the data on the electronic device using the determined secret or an encryption key that is based on the determined secret;

- wherein information indicative of the deterministic key (DK) is sent to the key device where it can be stored.

A computer program comprising machine-readable instructions to cause a processing device of an electronic device to implement any one of the methods described above.

One or more embodiments or aspects of the invention may comprise or use a computer-implemented method of determining, at a first node (C), a common secret (CS) that is

common with the first node (C) and a second node (S). The first node (C) may be associated with a first asymmetric cryptography pair having a first node master private key (V_{1C}) and a first node master public key (P_{1C}), and the second node (S) may be associated with a second asymmetric cryptography pair having a second node master private key (V_{1S}) and a second node master public key (P_{1S}). The method may comprise:

- determining a first node second private key (V_{2C}) based on at least the first node master private key (V_{1C}) and a deterministic key (DK);

- determining a second node second public key (P_{2S}) based on at least the second node master public key (P_{1S}) and the deterministic key (DK); and

- determining the common secret (CS) based on the first node second private key (V_{2C}) and the second node second public key (P_{2S}),

wherein the second node (S) has the same common secret (S) based on a first node second public key (P_{2C}) and a second node second private key (V_{2S}), wherein:

- the first node second public key (P_{2C}) is based on at least the first node master public key (P_{1C}) and the deterministic key (DK); and

- the second node second private key (V_{2S}) is based on at least the second node master private key (V_{1S}) and the deterministic key (DK).

The deterministic key (DK) is based on a message (M).

Thus, the invention may provide techniques and devices for enhanced security of electronic devices and/or the data stored thereon. The invention may also provide an improved electronic device because of the enhanced security mechanisms of the invention.

Brief Description of Drawings

[0053] Examples of the present disclosure will be described with reference to:

[0054] Fig. 1 is a schematic diagram of an example system to encrypt data;

[0055] Fig. 2 is a flow chart of computer-implemented methods for registering the electronic device and the key device of Fig. 1;

[0056] Fig. 3 is a flow chart of a computer-implemented method for encrypting data at the electronic device of Fig. 1 using a secret;

[0057] Fig. 4 is a flow chart of a computer-implemented method of authenticating the key device of Fig. 1;

[0058] Fig. 5 is a flow chart of a computer implemented method of decrypting the encrypted data at the electronic device following authentication of the key device; and

[0059] Fig. 6 illustrates a schematic of an example processing device.

Description of Embodiments

Overview

[0060] A method, device and system to encrypt data at an electronic device will now be described.

[0061] Fig. 1 illustrates a computer system 1 that includes an electronic device 3 that is in communication with a key device 5. The electronic device 3 has an associated first processing device 23 and the key device 5 has an associated second processing device 25. The electronic device 3 may be a personal electronic device, such as a laptop computer, a desk computer, a tablet computer, a mobile communication device, a computer server or any other computing device capable of processing data. In this particular example as illustrated in Fig. 1, the electronic device 3 is represented by a laptop computer.

[0062] The key device 5 may be a further personal electronic device, such as a mobile communication device, a portable memory device, such as a USB drive or the like. In this particular example as illustrated in Fig. 1, the key device 5 is represented by a mobile communication device.

[0063] The electronic device 3 may be in communication with the key device 5 via a wireless protocol, such as Bluetooth or a communications network, for example the internet or a local communications network. Alternatively, the electronic device 3 may be physically connected to the key device 5, for example via a USB port of the electronic device or via a cable connection. In this particular example as illustrated in Fig. 1, the electronic device 3 is in communication with the key device 5 via Bluetooth 7.

[0064] The electronic device 3 is associated with a first asymmetric cryptography pair having an electronic device master private key (V_{1S}) and an electronic device master public key (P_{1S}). The key device 5 is associated with a second asymmetric cryptography pair having a key device master private key (V_{1C}) and a key device master public key (P_{1C}). The first and second asymmetric cryptography pairs may be generated during registration. Methods of registration 200, 300 performed by the electronic device 3 and the key device 5 will be described in further detail below with reference to Fig. 2. The public key for each device may be shared between the devices 3, 5 publicly, for example via Bluetooth 7.

Embodiments of the present invention may comprise a technique (or variation(s) thereof) which is generally provided as: determining, at a first node (C), a common secret (CS) that is common with the first node (C) and a second node (S), wherein the first node (C) is associated with a first asymmetric cryptography pair having a first node master private key (V_{1C}) and a first node master public key (P_{1C}), and the second node (S) is associated with a second asymmetric cryptography pair having a second node master private key (V_{1S}) and a second node master public key (P_{1S}); the method or technique comprising:

- determining a first node second private key (V_{2C}) based on at least the first node master private key (V_{1C}) and a deterministic key (DK);

- determining a second node second public key (P_{2S}) based on at least the second node master public key (P_{1S}) and the deterministic key (DK); and

- determining the common secret (CS) based on the first node second private key (V_{2C}) and the second node second public key (P_{2S}),

wherein the second node (S) has the same common secret (S) based on a first node second public key (P_{2C}) and a second node second private key (V_{2S}), wherein:

- the first node second public key (P_{2C}) is based on at least the first node master public key (P_{1C}) and the deterministic key (DK); and

- the second node second private key (V_{2S}) is based on at least the second node master private key (V_{1S}) and the deterministic key (DK).

The deterministic key (DK) may be based on a message (M).

[0065] In accordance with an illustrative embodiment of the present invention: to encrypt data at the electronic device 3, a secret is determined based on a technique similar to that described above. The secret is determined on a private cryptography key of the electronic device 3 and a public cryptography key of the key device 5. By determining the secret, data can be encrypted using an encryption key (E) that is based on the determined secret. In one or more examples, the secret may be used as the encryption key (E) . One of the advantages of this technique is that there is no need for transmitting or storing the secret or the encryption key (E) on any of the devices 3, 5. This provides a much more secure solution compared to prior art arrangements.

[0066] To encrypt the data using the secret at the electronic device 3, the method 400 is performed without communicating any of the private keys between the devices 3, 5 which will be described in further detail with reference to Fig. 3.

[0067] In general, the method of encrypting data performed by the electronic device 3 initially includes connecting the electronic device 3 with a key device 5 to communicate with the key device 5. The communication may be established through a wired connection or a wireless connection, such as Bluetooth 7.

[0068] The method further includes determining a deterministic key (DK) which may be based on a message (M) created by the electronic device 3. For example, the processing device 23 of the electronic device 3 may generate a message (M) and then uses a standard algorithm to create a hash of the message forming the deterministic key (DK).

[0069] The method further includes determining a second electronic device private key (V_{2S}) based on at least the electronic device master private key (V_{1S}) and the deterministic key (DK), and determining a second key device public key (P_{2C}) based on the key device master public key (P_{1C}) and the deterministic key (DK). A secret is then determined based on the second electronic device private key (V_{2S}) and the second key device public key (P_{2C}). Optionally, the method may include determining a second electronic device public key (P_{2S}) based on at least the electronic device master public key (P_{1S}) and the deterministic key (DK).

[0070] In a further method step, data can then be encrypted using an encryption key (E) that is based on the determined secret. As mentioned above, the determined secret itself may be used as encryption key (E), or the encryption key (E) may be determined based on the secret. Following encrypting the data on the electronic device, the secret may be erased and only the deterministic key (DK) or the message (M) may be sent to the key device 5 where it can be securely stored. The deterministic key (DK) or the message (M) stored on the key device 5 can subsequently be used to decrypt the encrypted data.

[0071] It will be appreciated that the data to be encrypted / decrypted may comprise one or more individual files, one or more folders comprising files or an entire hard drive of the electronic device. In some examples, the method may comprise prompting a user to select the files and/or folders that are to be encrypted / decrypted. In such case, the key device 5 may store information indicative of a deterministic key for each file and folder and link them accordingly.

Method of registration 200, 300

[0072] An example of methods of registration 200, 300 will be described with reference to Fig. 2, where method 200 is performed by the electronic device 3 and method 300 is performed by the key device 5. This includes establishing the first and second asymmetric cryptography pairs for the respective devices 3, 5.

[0073] The asymmetric cryptography pairs include associated private and public keys, such as those used in public-key encryption. In this example, the asymmetric cryptography pairs are generated using Elliptic Curve Cryptography (ECC) and properties of elliptic curve operations.

[0074] Standards for ECC may include known standards such as those described by the Standards for Efficient Cryptography Group (www.sceg.org). Elliptic curve cryptography is also described in US 5,600,725, US 5,761,305, US 5889,865, US 5,896,455, US 5,933,504, US 6,122,736, US6,141,420, US 6,618,483, US 6,704,870, US 6,785,813, US 6,078,667, US 6,792,530.

[0075] In the method 200, 300, this includes the electronic device 3 and the key device 5 settling 210, 310 to a common ECC system and using a common generator (G). In one example, the common ECC system may be based on secp256K1 which is an ECC system used by Bitcoin. The common generator (G) may be selected, randomly generated, or assigned.

[0076] In the specific example illustrated in Fig. 1 in which the electronic device 3 is a laptop computer and the key device 5 is a mobile communication device, communications between the respective devices 3, 5 are realised by an application programming interface (API) communicating with a dedicated application installed on the mobile communications device 5. For this, software may be downloaded and installed on the laptop computer which is compatible with the dedicated application installed on the mobile communication device.

[0077] In a specific example, the key device 5 may be provided with not only the software application for the key device but also with the software for the electronic device. In this way, when the key device is connected to the electronic device, the software can be installed on the electronic device by executing the installation from the key device.

[0078] Turning now to the method 200 performed by the electronic device 3, the method 200 includes settling 210 on the common ECC system and common generator (G). This may include sending information indicative of the common ECC system and common generator from the electronic device 3 to the key device 5, or receiving the information from a third device, such as remote server computer. For example, the electronic device 3 may send, via Bluetooth 7, a notice indicative of using the common ECC system with a common generator (G) to the key device 5. In turn, the key device 5 may settle 310 by sending a notice indicative of an acknowledgment to using the common ECC system and common generator (G).

[0079] The method 200 also includes generating 220, at the electronic device 3, a first asymmetric cryptography pair that includes the electronic device master private key (V_{1S}) and the electronic device master public key (P_{1S}). In this particular example, the electronic device master private key (V_{1S}) is determined based, at least in part, on a random integer in an allowable range specified in the common ECC system. The electronic device master public key (P_{1S}) is then determined based on elliptic curve point multiplication of the electronic device master private key (P_{1S}) and the common generator (G) according to the formula:

$$P_{1S} = V_{1S} \times G \qquad \text{(Equation 1)}$$

[0080] Thus the first asymmetric cryptography pair includes:

V_{1S} : The electronic device master private key that is kept secret by the electronic device.

P_{1S}: The electronic device master public key that is made publicly known.

[0081] The electronic device 3 may store the first asymmetric cryptography pair in a first data storage 13 associated with the electronic device 3. For security, the electronic device master private key (V_{1S}) may be stored in a secure portion of the first data storage 13 to ensure the key remains private.

[0082] In this example, the method 200 includes sending 230 the electronic device public master key (P_{1S}) to the key device 3. However, for encrypting the data on the electronic device 3, this step may not be necessary.

[0083] Turning now to the method 300 performed by the key device 5, in this specific example the key device 5 receives 320 the electronic device master public key (P_{1S}) and stores 330 the received electronic device master public key (P_{1S}) within a storage element of the key device 5.

[0084] Similar to the method 200, the method 300 at the key device 5 includes generating 340 a second asymmetric cryptography pair that includes the key device master private key (V_{1C}) and the key device master public key (P_{1C}). The key device master private key (V_{1C}) is

also a random integer within the allowable range specified in the common ECC system. In turn, the key device master public key (P_{1C}) is determined by the following formula:

$$P_{1C} = V_{1C} \times G \qquad \text{(Equation 2)}$$

[0085] Thus the second asymmetric cryptography pair includes:

V_{1C} : The key device master private key that is kept secret by the key device.

P_{1C}: The key device master public key that is made publicly known.

[0086] The key device 5 may store the second asymmetric cryptography pair in a second data store 15 of the key device. The method 300 further includes sending 330 the key device master public key (P_{1C}) to the electronic device 3 where it may be stored in storage 13.

[0087] In some alternatives, the respective public master keys may be received and stored at a third data store associate with a third device, such as a trusted third party. This may include a third party that acts as a public directory, such as a certification authority. Thus in some examples, the key device master public key (P_{1C}) may be requested and received by the electronic device 3 only when determining the secret is required.

[0088] The registration steps may only need to occur once as an initial setup. Afterwards, the master keys can be reused in a secure matter to determine the secret that is dependent, *inter alia*, on the deterministic key (DK).

Encryption of data at the electronic device 3

[0089] An exemplary method 400 of encrypting data at the electronic device 3 by determining a secret that is based on a private key of the electronic device 3 and a public key of the key device 5 will now be described with reference to Fig. 3. The secret may be used for one cycle only, each cycle being a full round of encryption and decryption of the data.

[0090] It will be appreciated that new private and public keys may be determined for both the electronic device and the key device for each cycle of encryption and decryption. The new private and public keys may for example be determined by re-hashing the message (M)

as described in further detail in the co-filed application as mentioned above which is herein incorporated by reference in its entirety. In this way, sub-keys may be created, wherein each sub-key is linked to the master key.

Generating a message (M) 410

[0091] In this example, the method 400 includes generating 410 a message (M) at the electronic device 3. The message (M) may be random, pseudo random, or user defined. In one example, the message (M) is based on Unix time and a nonce (and arbitrary value). For example, the message (M) may be provided as:

$$\text{Message (M)} = \text{Unix Time} + \text{nonce} \qquad \text{(Equation 3)}$$

[0092] In some examples, the message (M) is arbitrary. However it is to be appreciated that the message (M) may have selective values (such as Unix Time, etc.) that may be useful in some applications.

[0093] The method 400 includes sending 420 the message (M) via Bluetooth 7, to the key device 5 where the message (M) will be stored. Importantly, the message (M) may be sent to the key device 5 over an unsecure network as the message (M) does not include information on the private keys.

[0094] It will be appreciated that the message (M) may be communicated to the key device 5 at any time. For example, the message (M) may be sent to the key device 5 after the encryption of the data is completed.

Determining a deterministic key 430

[0095] The method 400 further includes the step of determining 430 a deterministic key (DK) based on the message (M). In this example, this includes determining a cryptographic hash of the message. An example of a cryptographic hash algorithm includes SHA-256 to create a 256-bit deterministic key (DK). That is:

$$DK = \text{SHA-256}(M) \qquad \text{(Equation 4)}$$

[0096] The selection of message may be arbitrary for the purpose of generating the encryption key (E) and will be newly selected for each encryption / decryption cycle. In this example, the message (M) is reduced to 160 bits by hashing in order to keep the message length short.

[0097] It is to be appreciated that other hash algorithms may be used. This may include other hash algorithms in the Secure Hash Algorithm (SHA) family. Some particular examples include instances in the SHA-3 subset, including SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256. Other hash algorithms may include those in the RACE Integrity Primitives Evaluation Message Digest (RIPEMD) family. A particular example may include RIPEMD-160. Other hash functions may be based on Zémor-Tillich hash function and knapsack-based hash functions.

Determining second private and public keys 440, 450, 460

[0098] The method 400 then includes determining 440, 450, 460 the following second keys based on the deterministic key (DK), i.e. the hash of the message (M).

[0099] The second electronic device private key (V_{2S}) is determined 440 based on the electronic device master private key (V_{1S}) and the hash of the message (M). This can be based on a scalar addition of the electronic device master private key (V_{1S}) and the hash of the message (M) according to the following formula:

$$V_{2S} = V_{1S} + \text{SHA-256}(M) \qquad \text{(Equation 5)}$$

[0100] The second electronic device public key (P_{2S}) is determined 450 based on the electronic device master public key (P_{1S}) and the hash of the message (M). This can be determined based on the following formula:

$$P_{2S} = P_{1S} + \text{SHA-256}(M) \times G \qquad \text{(Equation 6)}$$

[0101] The second key device public key (P_{2C}) is determined 460 based on the key device master public key (P_{1C}) and the hash of the message (M). This can be determined according to the following formula:

$$P_{2C} = P_{1C} + SHA\text{-}256(M) \times G \quad \text{(Equation 7)}$$

[0102] It should be noted that in this specific example in which elliptic curve cryptography is applied, 'G' refers to the generator, the operator '+' refers to elliptic curve point addition and the operator 'x' refers to elliptic curve point multiplication.

[0103] Furthermore, it should be noted that for the encryption of the data, it may not be necessary to determine the second electronic device public key P_{2S}. As will be described in further detail below, for determining the secret, the second electronic device public key P_{2S} may not be necessary.

Determine the secret 470

[0104] The electronic device 3 may then determine 470 the secret based on the determined second electronic device private key (V_{2S}) and the determined second key device public key (P_{2C}). The secret may be determined by the electronic device 3 according to the following formula:

$$CS = V_{2C} \times P_{2S} \quad \text{(Equation 8)}$$

The secret and encryption key

[0105] The secret may be used as a symmetric encryption key, or as the basis for determining a symmetric encryption key.

[0106] In this particular example, the method 400 includes a further step of determining 480 an encryption key (E) based on the determined secret. The encryption key (E) is further based on the electronic device's serial number to ensure that the encryption key (E) is specific to the electronic device 3. The encryption key (E) is determined according to the following formula:

$$E = SHA256\ (\ SHA256\ (salt + secret) + serial\ number\ ) \quad \text{(Equation 9)}$$

[0107] Where salt = message (M)

[0108] In this particular example, the concept of random salts is used to determine the encryption key (E). It will be appreciated that any suitable techniques to calculate an encryption key (E) based on the determined secret may be used (if any).

[0109] The method 400 further includes encrypting 490 the data, at the electronic device 3, using the determined encryption key (E). It will be appreciated that any suitable method for encrypting the data using the encryption key (E) may be used.

[0110] Importantly, the electronic device 3 does not need to store the encryption key (E) or the secret as this can be re-calculated based on the message (M) which is stored on a data storage of the key device 5.

Decryption of the encrypted data

[0111] Following the encryption of the data at the electronic device 3, a method of decrypting the encrypted data at the electronic device 3 will now be described with reference to Figs. 4 and 5. To decrypt the data, the electronic device 3 re-calculates the secret which was previously determined when the data was encrypted.

[0112] Initially, the electronic device 3 is connected to the key device 5 to be in communication with each other. The step of connecting the respective devices 3, 5 may include determining whether the respective software running on the devices is compatible and synchronised.

Authenticating 500 the key device 5

[0113] Before the encrypted data is decrypted at the electronic device 3, in this particular example, the key device 5 is initially authenticated by the electronic device 3.

[0114] A method of authenticating 500 the key device 5 will be described with reference to Fig. 4. The method of authenticating 500 the key device 5 may be part of the decryption cycle of the data at the electronic device 3.

[0115] The method 500 includes generating 510 an authentication message (M_A) at the electronic device 3 which will be used to authenticate that the key device 5 is the key device

5. It will be appreciated that the generated message (M_A) may solely be used for the authentication of the key device 5. However, in some examples, the authentication message (M_A) may form the message (M) as described with reference to Fig. 3 used in the encryption process for the next encryption-decryption cycle.

[0116] The method 500 includes receiving 520 the authentication message (M_A) at the key device 5 via Bluetooth 7 from the electronic device 3.

[0117] The key device 5 then determines 530 a deterministic authentication key (DK_A) based on the message (M_A). For example, the deterministic authentication key (DK_A) may be the hash of the authentication message similar to step 430 of method 400 and can be determined according to the following formula:

$$DK_A = \text{SHA-256}\ (M_A) \qquad \text{(Equation 10)}$$

[0118] The key device 5 then determines a new asymmetric cryptography pair based on the deterministic authentication key (DK_A). Specific to this example, the method 500 includes determining 540 a second key device private key V_{2C} according to the following formula:

$$V_{2C} = V_{1C} + \text{SHA-256}\ (M_A) \qquad \text{(Equation 11)}$$

[0119] The method 500 also includes determining 550 a second key device public key P_{2C} according to the following formula.

$$P_{2C} = P_{1C} + \text{SHA-256}\ (M_A) \times G \qquad \text{(Equation 12)}$$

[0120] The method 300 further includes generating 560 a signed message (SM_A) based on the authentication message (M_A) and the determined second key device private key (V_{2C}). Generating a signed message includes applying a digital signature algorithm to digitally sign the authentication message (M_A). In one example, this includes applying the second key device private key (V_{2C}) to the message in an Elliptic Curve Digital Signature Algorithm (ECDSA) to obtain the signed message (SM_A). The authentication message (M_A) may be signed according to the following formula:

$$SM_A = \text{Sig} - V_{2C} < M_A > \qquad \text{(Equation 13)}$$

[0121] Examples of ECDSA include those based on ECC systems with secp256k1, secp256r1, secp384r1, se3cp521r1.

[0122] The signed authentication message (SM_A) is subsequently sent 570 to the electronic device 3 for authentication of the key device 5.

[0123] The method 500 includes receiving 580 the signed authentication message (SM_A) from the key device 5. The electronic device 3 may then validate 590 the signature on the signed authentication message (SM_A) with the second key device public key (P_{2C}) that was determined at step 550.

[0124] Verifying the digital signature may be done in accordance with an Elliptic Curve Digital Signature Algorithm (ECDSA). Importantly, the signed authentication message (SM_A) that was signed with the second key device private key (V_{2C}) should only be correctly verified with the corresponding second key device public key (P_{2C}), since V_{2C} and P_{2C} form a cryptographic pair. Since these keys are deterministic of the key device master private key (V_{1C}) and the key device master public key (P_{1C}) that were generated at registration of the key device, verifying the signed authentication message (SM_A) can be used as a basis of authenticating that an alleged key device 5 sending the signed message (SM_A) is the same key device 5 as during registration.

Re-calculate the encryption key (E) to decrypt the encrypted data

[0125] Following successful authentication of the key device 5, the electronic device 3 decrypts the encrypted data by re-calculating the secret and thereby the encryption key (E). An exemplary method 600 of decrypting the encrypted data will now be described with reference to Fig. 5.

[0126] The method 600 includes requesting 610 the message (M) that was previously used in the encryption cycle and stored on the key device 5 as described in step 420 of method 400.

[0127] The method 600 then includes receiving 630 message (M). In this particular example, the message (M) is signed 620 by the key device 5 using the second key device private key (V_{2C}) before the message (M) is sent to the electronic device 3. The message (M) may be signed according to the following formula:

$$SM = Sig - V_{2C} < M > \quad \text{(Equation 14)}$$

[0128] The method 600 further includes verifying 650 the signed message (SM). This may be done by independently determining the second key device public key (P_{2C}) and then performing applying an Elliptic Curve Digital Signature Algorithm (ECDSA) to SM and P_{2C}. The second key device public key may be determined according to the following formula:

$$P_{2C} = P_{1C} + \text{SHA-256 (M) x G} \quad \text{(Equation 15)}$$

[0129] The method 600 then includes retrieving 660 the message (M) from the signed message (M) so that the electronic device 3 can re-calculate 670 the secret following steps 430 to 470 as described with reference to Fig. 3.

[0130] In a further step 680, the encryption key (E) is re-determined based on the secret and the electronic device's serial number as described with reference to step 480 of method 400. Once the encryption key (E) is determined, the data can be decrypted 690.

[0131] It will be appreciated that for decrypting the encrypted data, a method of authentication as described with reference to Fig. 4 may not be necessary for some embodiments.

Processing device

[0132] As noted above, the electronic device 3 and the key device 5 may be personal electronic devices, such as a laptop computer, tablet computer, mobile communication device, computer server etc. The electronic device may include a processing device 23, 25, a data store 13, 15 and a user interface 14.

[0133] Fig. 6 illustrates an example of a processing device 23, 25. The processing device 23, 25 may be used at the electronic device 3, or the key device 5. The processing device 23, 25 includes a processor 1510, a memory 1520 and an interface device 1540 that communicate with each other via a bus 1530. The memory 1520 stores instructions and data for implementing the method 200, 300, 400, 500 and 600 described above, and the processor 1510 performs the instructions from the memory 1520 to implement the method 200, 300, 400, 500 and 600. The interface device 1540, may include a communications module that

facilitates communication with the communications network, such as Bluetooth 7 and, in some examples, with the user interface 14 and peripherals such as data store 13, 15. It should be noted that although the processing device 1501 may be independent network elements, the processing device 1501 may also be part of another network element. Further, some functions performed by the processing device 1501 may be distributed between multiple network elements. For example, the electronic device 3 may have multiple processing devices 23 to perform method 200, 400 and parts of method 500, 600 in a secure local area network associated with the electronic device 3.

[0134] Where this disclosure describes that a user, issuer, merchant, provider or other entity performs a particular action (including signing, issuing, determining, calculating, sending, receiving, creating etc.), this wording is used for the sake of clarity of presentation. It should be understood that these actions are performed by the computing devices operated by these entities.

[0135] Signing may comprise executing a cryptographic function. The function has an input for a clear text and an input for a key, such as a private key. A processor may execute the function to calculate a number or string that can be used as a signature. The signature is then provided together with the clear text to provide a signed text. The signature changes completely if the message text or the key changes by a single bit. While calculating the signature requires little computational power, recreating a message that has a given signature is practically impossible. This way, the clear text can only be changed and accompanied by a valid signature if the private key is available. Further, other entities can easily verify the signature using the publicly available public key.

[0136] In most circumstances, encrypting and decrypting comprises a processor executing a cryptographic function to calculate an output string representing the encrypted message or the clear text message respectively.

[0137] Keys, tokens, metadata, transactions, offers, contracts, signatures, scripts, metadata, invitations, and the like refer to binary data represented as numbers, text or strings stored on data memory, such as variables in program code of type “string” or “int” or other types or text files.

[0138] An example of the peer-to-peer ledger is the bitcoin Blockchain. Transferring funds or paying fees in bitcoin currency comprises creating a transaction on the bitcoin Blockchain with the funds or fees being output from the transaction. An example of a bitcoin transaction includes an input transaction hash, a transaction amount, one or more destinations, a public key of a payee or payees and a signature created by using the input transaction as the input message and a private key of a payer to calculate the signature. The transaction can be verified by checking that the input transaction hash exists in a copy of the bitcoin Blockchain and that the signature is correct using the public key. To ensure that the same input transaction hash has not been used elsewhere already, the transaction is broadcast to a network of computing nodes ('miners'). A miner accepts and records the transaction on the Blockchain only if the input transaction hash is not yet connected and the signatures are valid. A miner rejects the transaction if the input transaction hash is already linked to a different transaction.

[0139] When two items are associated, this means that there is a logical connection between these items. In a database, for example, identifiers for the two items may be stored in the same records to make the two items associated with each other. In a transaction, identifiers for the two items may be included in the transaction string to make the two items associated with each other.

[0140] Authorising another entity may comprise calculating a signature string of a transaction using a private key and providing the signature string to the entity to allow the entity to use the signature to verify the transaction.

[0141] A user having an account with another entity may comprise the entity storing information about the user, such as email address, name and potentially public keys. For example, the entity may maintain a database, such as SQL, OrientDB, MongoDB or others. In some examples, the entity may also store one or more of the user's private keys.

[0142] It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the above-described embodiments, without departing from the broad general scope of the present disclosure. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive.

CLAIMS:

1. A computer implemented method of encrypting data at an electronic device (S), the electronic device being associated with a key device (C), wherein the electronic device is further associated with a first asymmetric cryptography pair having a first electronic device private key (V_{1S}) and a first electronic device public key (P_{1S}), and the key device is associated with a second asymmetric cryptography pair having a first key device private key (V_{1C}) and a first key device public key (P_{1C}); the method comprising:

- determining, at the electronic device, a deterministic key (DK);

- receiving, at the electronic device, the first key device public key (P_{1C}) from the key device;

- determining, at the electronic device, a second electronic device private key (V_{2S}) based on at least the first electronic device private key (V_{1S}) and the deterministic key (DK), and

- determining, at the electronic device, a second key device public key (P_{2C}) based on at least the first key device public key (P_{1C}) and the deterministic key (DK);

- determining a secret based on at least the second electronic device private key (V_{2S}) and the second key device public key (P_{2C});

- encrypting the data at the electronic device using the determined secret or an encryption key that is based on the determined secret; and

- sending information indicative of the deterministic key (DK) to the key device where the information can be stored.

2. The method of claim 1 further comprising: storing, at the key device, the information indicative of the deterministic key (DK).

3. The method of claim 1 or 2 wherein the deterministic key (DK) is based on a message (M).

4. The method of claim 3 comprising a step of generating the message (M) at the electronic device, and determining the deterministic key (DK) based on determining a hash of the message (M).

5. The method of any one of the preceding claims comprising a step of determining a second electronic device public key (P_{2S}) based on at least the first electronic device public key (P_{1S}) and the deterministic key (DK).

6. The method of any one of the preceding claims comprising: sending from the electronic device to the key device, a notice indicative of using a common elliptic curve cryptography (ECC) system with a common generator (G).

7. The method of claim 6 wherein the first electronic device public key (P_{1S}) and the first key device public key (P_{1C}) are based on elliptic curve point multiplication of the respective first electronic device private key (V_{1S}) and first key device private key (V_{1C}) and the common generator (G).

8. The method of claim 6 or 7 comprising a step of generating the first electronic device private key (V_{1S}) based on a random integer in an allowable range specified in the common ECC system; and generating the first electronic device public key (P_{1S}) based on elliptic curve point multiplication of the first electronic device private key (V_{1C}) and the common generator (G) according to the following formula:

$$P_{1S} = V_{1S} \times G$$

9. The method of any one of claims 6 to 8 comprising a step of generating the second electronic device private key (V_{2S}) based on a scalar addition of the first electronic device private key (V_{1S}) and the deterministic key (DK) according to the following formula:

$$V_{2S} = V_{1S} + DK$$

10. The method of any one of claims 6 to 9 comprising a step of generating the second electronic device public key (P_{2S}) based on at least the first electronic device public key (P_{1S}) with elliptic curve point addition to the deterministic key (DK).

11. The method of claim 10 wherein the second electronic device public key (P_{2S}) is based on the first electronic device public key (P_{1S}) with elliptic curve point addition to the elliptic curve point multiplication of the deterministic key (DK) and the common generator (G) according to the following formula:

$$P_{2S} = P_{1S} + DK \times G.$$

12. The method of any one of claims 6 to 11 comprising a step of generating the second key device public key (P_{2C}) based on at least the first key device public key (P_{1C}) with elliptic curve point addition to the deterministic key (DK).

13. The method of claim 12 wherein the second key device public key (P_{2C}) is based on the first key device public key (P_{1C}) with elliptic curve point addition to the elliptic curve point multiplication of the deterministic key (DK) and the common generator (G) according to the following formula:

$$P_{2C} = P_{1C} + DK \times G$$

14. The method of any one of the preceding claims comprising a step of determining the encryption key based on the determined secret and identification information of the electronic device.

15. The method of any one of the preceding claims comprising a step of storing, at a data storage associated with the electronic device, the first key device public key (P_{1C}).

16. A computer implemented method of decrypting data at an electronic device, the data being encrypted in accordance with the method of encrypting data as described above, the method of decrypted the data comprising:

receiving, at the electronic device, the information indicative of the deterministic key (DK), from the key device;

determining the secret based on the received information indicative of the deterministic key (DK); and

decrypting, at the electronic device, the encrypted data using the secret or the encryption key that is based on the secret.

17. The method of claim 16 comprising a step of generating, at the electronic device, an authentication message (M_A) and sending the authentication message (M_A) to the key device.

18. The method of claim 17 comprising a step of determining the deterministic authentication key (DK_A) by determining a hash of the message (M_A).

19. The method of any one of claims 16 to 18 comprising a step of generating, at the key device, a second asymmetric cryptography pair having a second key device private key (V_{2C}) and a second key device public key (P_{2C}).

20. The method of claim 18 and 19, wherein the second key device private key (V_{2C}) is based on the deterministic authentication key (DK_A) and the first key device private key (V_{1C}), and the second key device public key (P_{2C}) is based on the deterministic authentication key (DK_A) and the first key device public key (P_{1C}).

21. The method of claim 20 comprising:

generating, at the key device, a signed authentication message (SM_A) based on the deterministic authentication key (DK_A) and the second key device private key (V_{2C});

receiving, at the electronic device, the signed authentication message (SM_A) from the key device; and

validating the signed message (SM_A) with the second key device public key (P_{2C}); and authenticating the key device based on the result of validating the signed authentication message (SM_A).

22. The method of any one of claims 16 to 21 comprising:

requesting, at the electronic device, the information indicative of the deterministic key (DK) from the key device;

generating, at the key device, a signed message (SM) based on the message (M);

sending the signed message (SM) to the electronic device;

validating, at the electronic device, the signed message (SM); and

retrieving the message (M) such that the secret can be determined, at the electronic device, for decrypting the data.

23. A computer system for encrypting data at an electronic device, the computer system comprising:

- the electronic device being associated with a first asymmetric cryptography pair having a first electronic device private key (V_{1S}) and a first electronic device public key (P_{1S}),

- a key device being associated with a second asymmetric cryptography pair having a first key device private key (V_{1C}) and a first key device public key (P_{1C});

- wherein the electronic device comprises a processor configured to:

  - determine a deterministic key (DK);

  - receive the first key device public key (P_{1C}) from the key device;

  - determine a second electronic device private key (V_{2S}) based on at least the first electronic device private key (V_{1S}) and the deterministic key (DK), and

  - determine a second key device public key (P_{2C}) based on at least the first key device public key (P_{1C}) and the deterministic key (DK);

  - determine a secret based on at least the second electronic device private key (V_{2S}) and the second key device public key (P_{2C}); and

- encrypt the data on the electronic device using the determined secret or an encryption key that is based on the determined secret;

- wherein information indicative of the deterministic key (DK) is stored on the key device.

24. The computer system of claim 23 further configured to decrypt data, the processor of the electronic device being configured to:

receive the information indicative of the deterministic key (DK), from the key device;

determine the secret based on the information indicative of the deterministic key (DK); and

decrypt the data using the determined secret or the encryption key that is based on the determined secret.

25. An electronic device for encrypting data, the electronic device being associated with a key device, wherein the electronic device is associated with a first asymmetric cryptography pair having a first electronic device private key (V_{1S}) and a first electronic device public key (P_{1S}), and the key device is associated with a second asymmetric cryptography pair having a first key device private key (V_{1C}) and a first key device public key (P_{1C}); the electronic device comprising a processing device configured to:

- determine a deterministic key (DK);

- receive the first key device public key (P_{1C}) from the associated key device;

- determine a second electronic device private key (V_{2S}) based on at least the first electronic device private key (V_{1S}) and the deterministic key (DK), and

- determine a second key device public key (P_{2C}) based on at least the first key device public key (P_{1C}) and the deterministic key (DK);

- determine a secret based on at least the second electronic device private key (V_{2S}) and the second key device public key (P_{2C}); and

- encrypt the data on the electronic device using the determined secret or an encryption key that is based on the determined secret;

- wherein information indicative of the deterministic key (DK) is sent to the key device where it can be stored.

26. A computer program comprising machine-readable instructions to cause a processing device of an electronic device to implement the method of any one of claims 1 to 22.

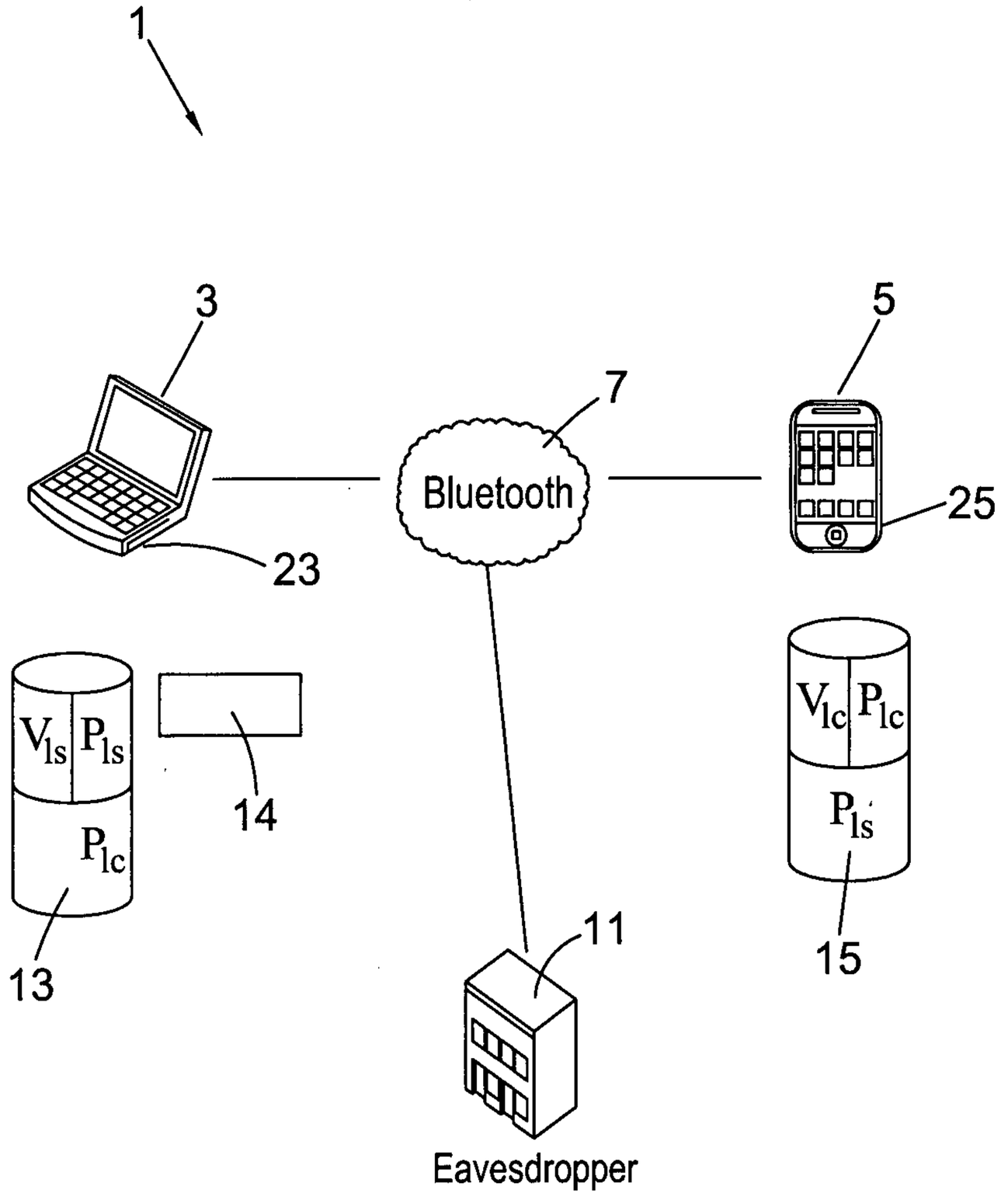

1
3
5
7
Bluetooth
25
23
V_{ls} P_{ls}
P_{lc}
13
14
11
Eavesdropper
V_{lc} P_{lc}
P_{ls}
15

Fig. 1

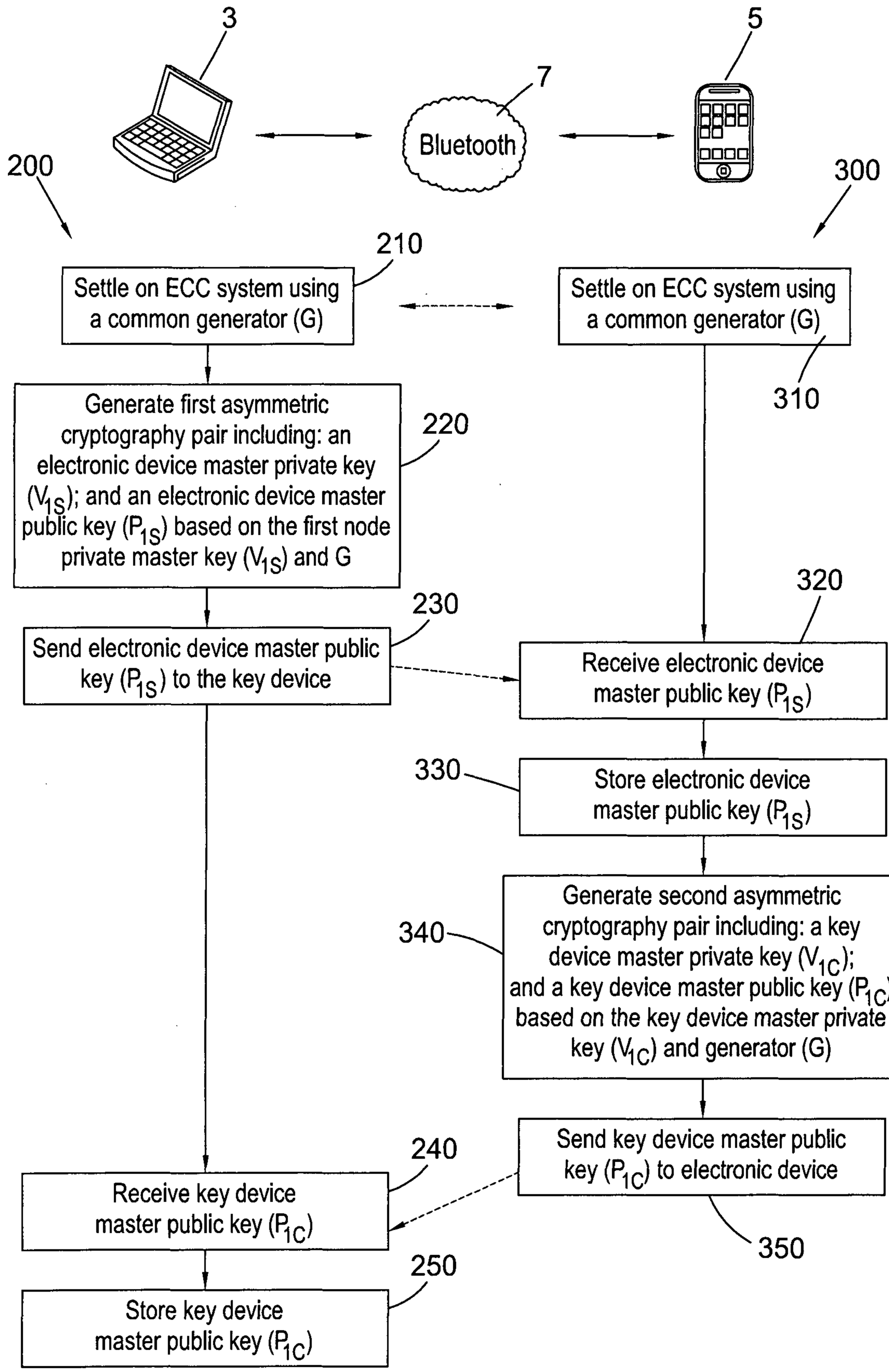

3
5
7
Bluetooth
200
300
210
Settle on ECC system using a common generator (G)
Settle on ECC system using a common generator (G)
310
Generate first asymmetric cryptography pair including: an electronic device master private key (V_{1S}); and an electronic device master public key (P_{1S}) based on the first node private master key (V_{1S}) and G
220
230
Send electronic device master public key (P_{1S}) to the key device
320
Receive electronic device master public key (P_{1S})
330
Store electronic device master public key (P_{1S})
340
Generate second asymmetric cryptography pair including: a key device master private key (V_{1C}); and a key device master public key (P_{1C}) based on the key device master private key (V_{1C}) and generator (G)
240
Send key device master public key (P_{1C}) to electronic device
350
Receive key device master public key (P_{1C})
250
Store key device master public key (P_{1C})

Fig. 2

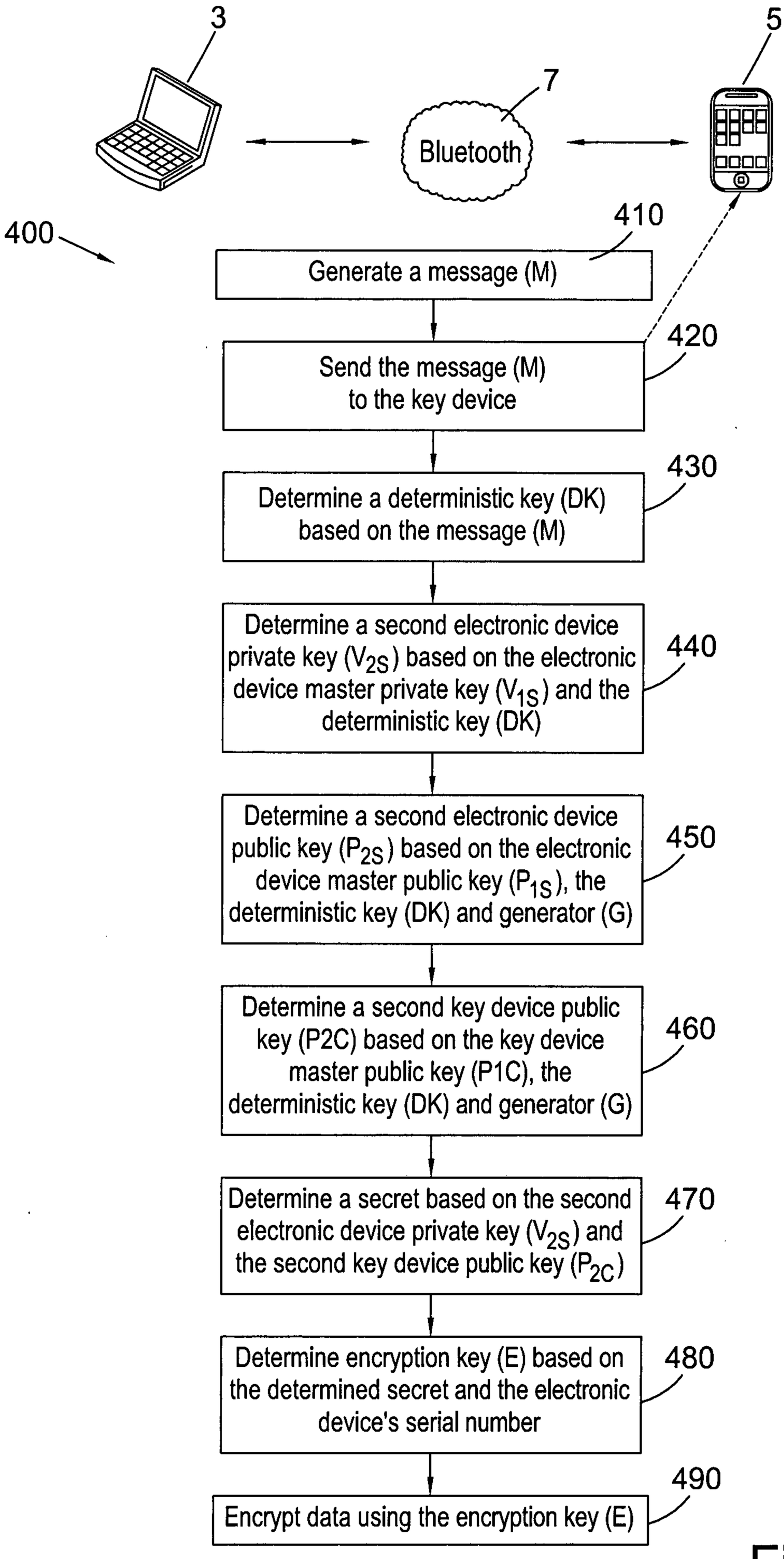
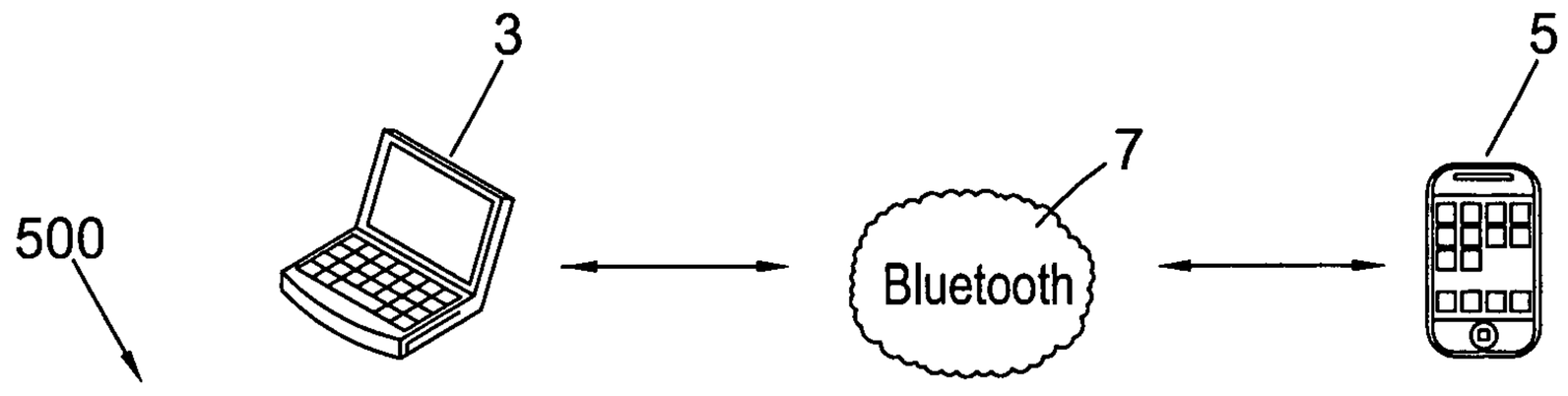

3
5
7
Bluetooth
400
410
Generate a message (M)
420
Send the message (M) to the key device
430
Determine a deterministic key (DK) based on the message (M)
440
Determine a second electronic device private key (V_{2S}) based on the electronic device master private key (V_{1S}) and the deterministic key (DK)
450
Determine a second electronic device public key (P_{2S}) based on the electronic device master public key (P_{1S}), the deterministic key (DK) and generator (G)
460
Determine a second key device public key (P2C) based on the key device master public key (P1C), the deterministic key (DK) and generator (G)
470
Determine a secret based on the second electronic device private key (V_{2S}) and the second key device public key (P_{2C})
480
Determine encryption key (E) based on the determined secret and the electronic device's serial number
490
Encrypt data using the encryption key (E)

Fig. 3


500
3
7
Bluetooth
5

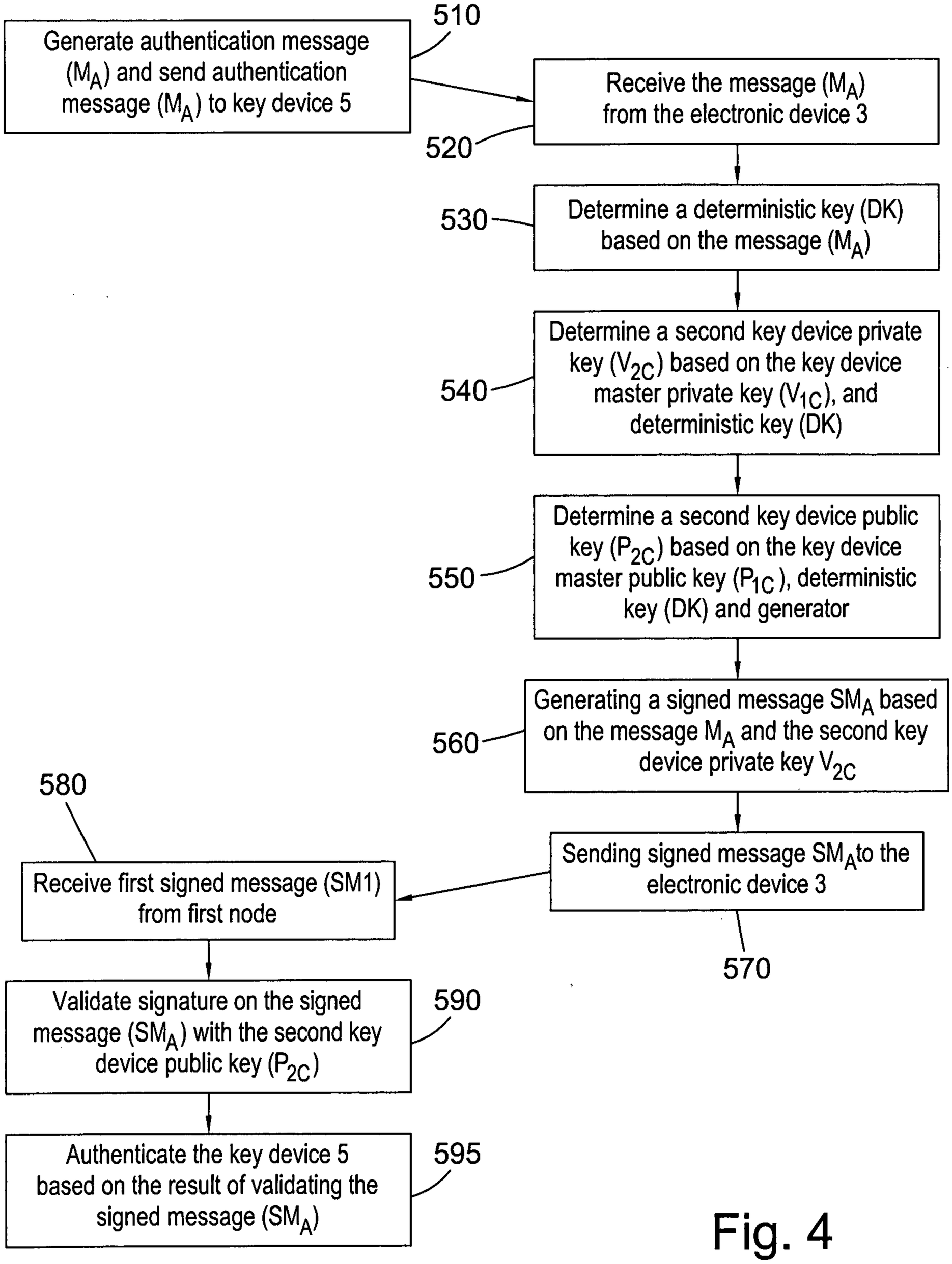

510
Generate authentication message (M_A) and send authentication message (M_A) to key device 5
520
Receive the message (M_A) from the electronic device 3
530
Determine a deterministic key (DK) based on the message (M_A)
540
Determine a second key device private key (V_{2C}) based on the key device master private key (V_{1C}), and deterministic key (DK)
550
Determine a second key device public key (P_{2C}) based on the key device master public key (P_{1C}), deterministic key (DK) and generator
560
Generating a signed message SM_A based on the message M_A and the second key device private key V_{2C}
570
Sending signed message $SM_A$to the electronic device 3
580
Receive first signed message (SM1) from first node
590
Validate signature on the signed message (SM_A) with the second key device public key (P_{2C})
595
Authenticate the key device 5 based on the result of validating the signed message (SM_A)

Fig. 4

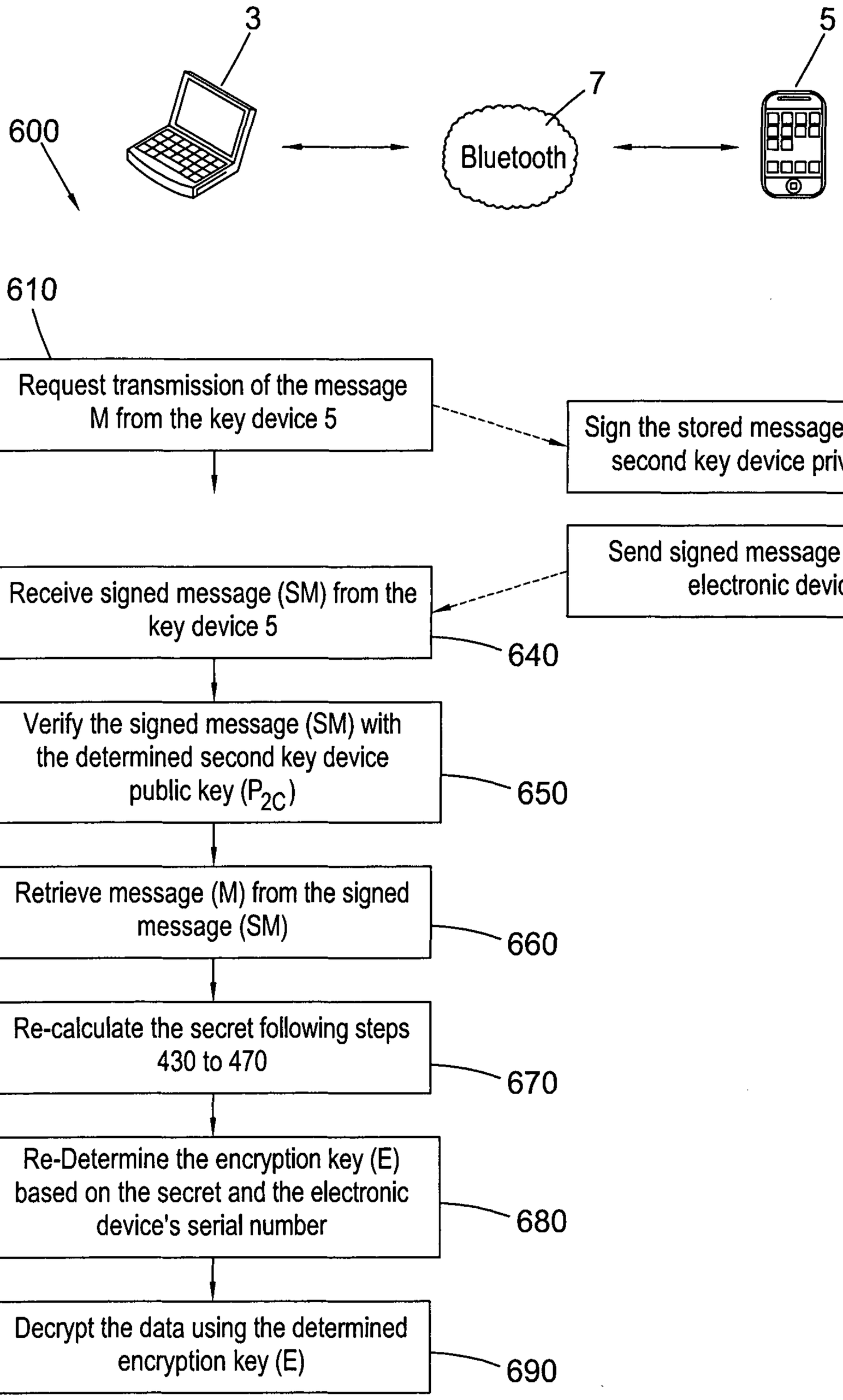

600
3
5
7
Bluetooth
610
Request transmission of the message M from the key device 5
620
Sign the stored message (M) using the second key device private key V_{2C}
Send signed message (SM) to the electronic device 3
630
Receive signed message (SM) from the key device 5
640
Verify the signed message (SM) with the determined second key device public key (P_{2C})
650
Retrieve message (M) from the signed message (SM)
660
Re-calculate the secret following steps 430 to 470
670
Re-Determine the encryption key (E) based on the secret and the electronic device's serial number
680
Decrypt the data using the determined encryption key (E)
690

Fig. 5

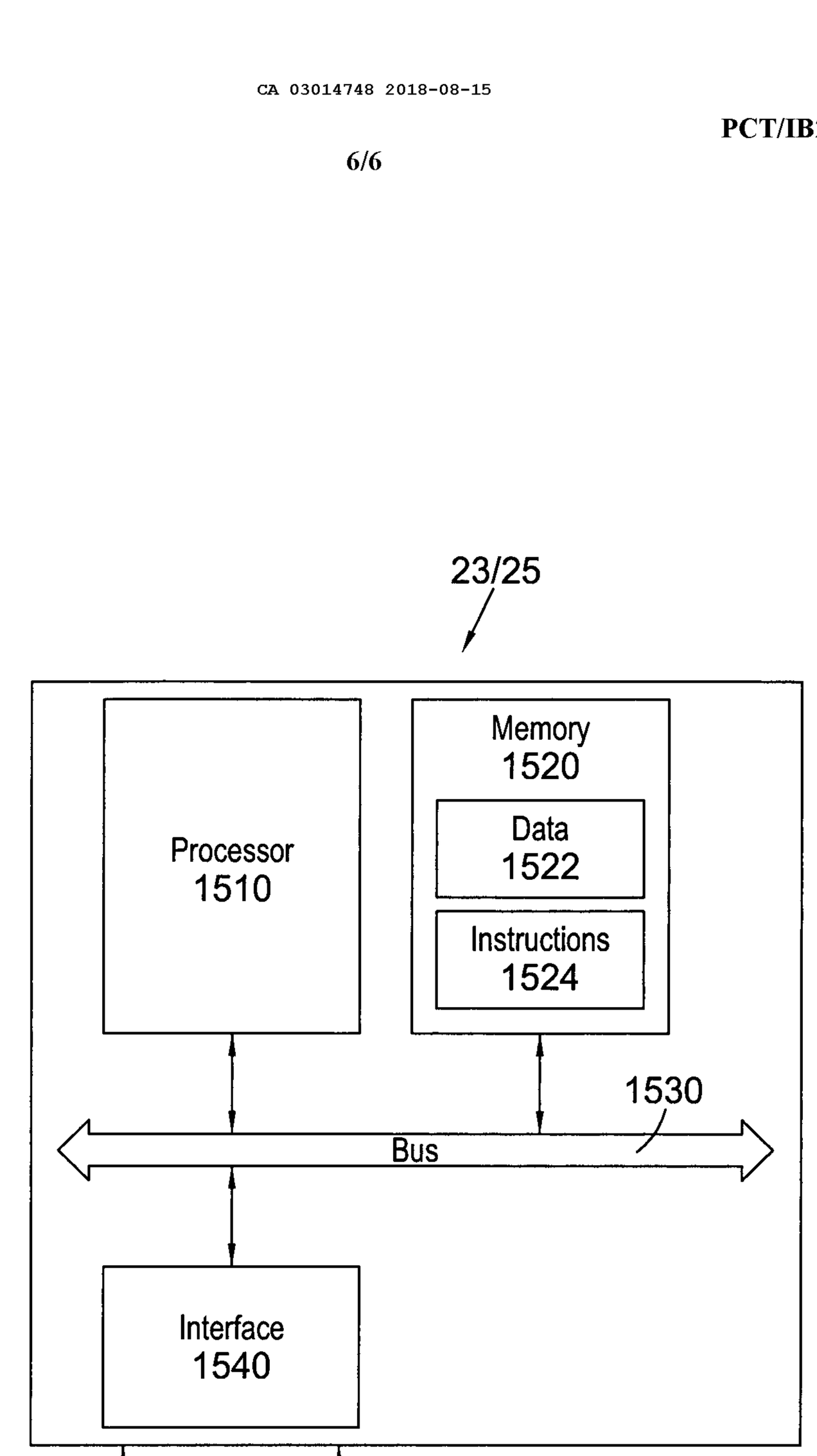

Processor
1510
Memory
1520
Data
1522
Instructions
1524
1530
Bus
Interface
1540
To/From User interface 14 and/or peripherals 13/15
To/From Network 7

Fig. 6

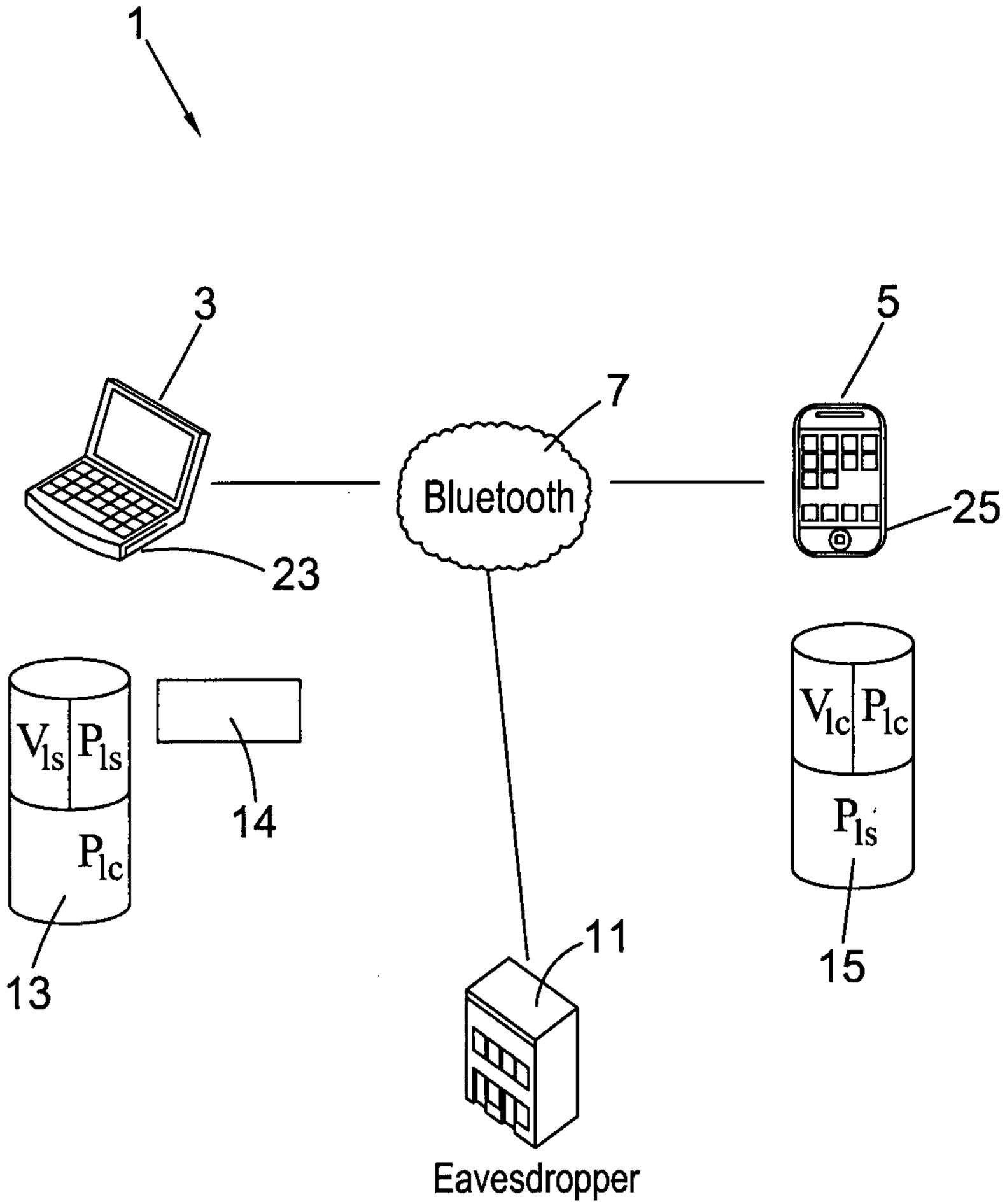

1
3
5
7
Bluetooth
25
23
V_{ls} P_{ls}
P_{lc}
13
14
V_{lc} P_{lc}
P_{ls}
15
11
Eavesdropper

Fig. 1