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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 November 2009 (26.11.2009)

PCT

(10) International Publication Number
WO 2009/141773 A2

(51) International Patent Classification:
H04L 29/06 (2006.01) ***H04W 12/02*** (2009.01)

(21) International Application Number:
PCT/IB2009/052003

(22) International Filing Date:
14 May 2009 (14.05.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
08104042.0 21 May 2008 (21.05.2008) EP

(71) Applicant *(for all designated States except US):* **NXP** B.V. [NIVNL]; High Tech Campus 60, 5656 AG Eindhoven (NL).

(72) Inventor; and
(75) Inventor/Applicant *(for US only):* **STOREZ, Antoine** [FR/FR]; c/o NXP Semiconductors Austria GmbH, Intellectual Property Department, Gutheil-Schoder-Gasse 8-12, 1102 Vienna (AT).

(74) Agent: ROEGGLA, Harald; c/o NXP Semiconductors Austria GmbH, Intellectual Property Department, Gutheil-Schoder-Gasse 8-12, 1102 Vienna (AT).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available):* AE, AG, AL, AM, **AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH,** CN, **CO, CR, CU, CZ, DE, DK, DM, DO, DZ,** EC, EE, EG, **ES, FI, GB, GD,** GE, **GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA,** NG, **NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, **FI,** FR, GB, GR, HR, HU, IE, IS, **IT, LT,** LU, LV, MC, MK, MT, NL, NO, PL, **PT,** RO, SE, SI, SK, TR), OAPI (BF, **BJ,** CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(U))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(Hi))*

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

(54) Title: METHOD AND DEVICE FOR ENCRYPTED ACTIVE NEAR FIELD COMMUNICATION

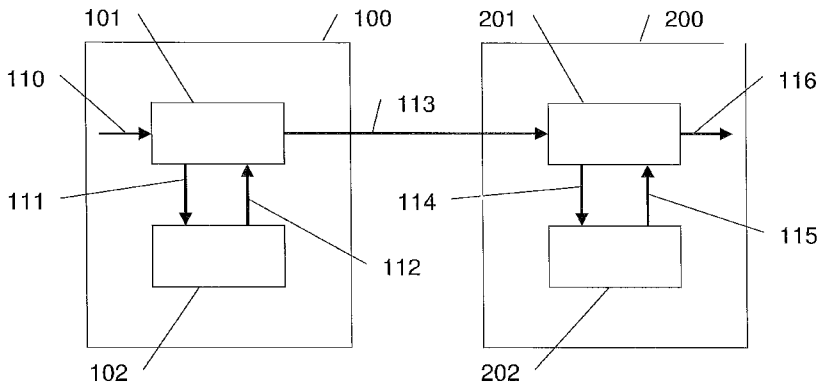

Fig. 1

(57) Abstract: An electronic device comprising a Near Field Communication circuit capable of sending and receiving data, and a cryptographic circuit capable ofencrypting and decrypting data. The electronic device is designed to encrypt data with the cryptographic circuit and transmit the encrypted data with the Near Field Communication circuit. The electronic device is further designed to receive encrypted data withthe Near Field Communication circuit and decrypt the encrypted data withthe cryptographic circuit.

WO 2009/141773 A2

METHOD AND DEVICE FOR ENCRYPTED ACTIVE NEAR FIELD COMMUNICATION

FIELD OF THE INVENTION

The present invention relates to a method and a device for performing an encrypted Near Field Communication in an active communication mode.

BACKGROUND OF THE INVENTION

Near Field Communication or NFC is a short-range high-frequency wireless communication technology which enables the exchange of data between devices over about ten centimeters distance. An NFC-enabled device can communicate with both smartcards and smartcard readers, as well as with other NFC-enabled devices. NFC may for example be employed in NFC-enabled mobile phones.

NFC communicates via magnetic field induction, where two loop antennas are located within each other's near field, effectively forming an air-core transformer. It operates within the radio frequency band of 13.56 MHz, with a bandwidth of about 2 MHz.

NFC supports two modes of operation. In passive communication mode, a first device provides a carrier field and a second device answers by modulating the carrier field provided by the first device. The second device may draw its operating power from the electromagnetic carrier field provided by the first device, thus making the second device act as a transponder.

In active communication mode, both the first and the second device communicate by alternately generating their own electromagnetic carrier field. The first device deactivates its electromagnetic carrier field while it is waiting for data to be sent by the second device. The second device deactivates its electromagnetic carrier field while it is waiting for data to be sent by the first device. Two active NFC devices can communicate and exchange information in peer-to-peer mode.

OBJECT AND SUMMARY OF THE INVENTION

It is an object of the present invention to provide a device and a method to encrypt data transmitted in peer-to-peer mode in order to support a secure communication.

To this end, an object of the invention is an electronic device comprising a Near Field Communication circuit capable of sending and receiving data, and a cryptographic circuit capable of encrypting and decrypting data. The electronic device is designed to encrypt data with the cryptographic circuit and transmit the encrypted data with the Near Field Communication circuit. The electronic device is further designed to receive encrypted data with the Near Field Communication circuit and decrypt the encrypted data with the cryptographic circuit.

A further object of the invention is a method for sending data with steps of encrypting data with a cryptographic circuit and transmitting the data with a Near Field Communication circuit.

A further object of the invention is a method for receiving data with steps of receiving data with a Near Field Communication circuit and decrypting the data with a cryptographic circuit.

A further object of the invention is a system comprising two electronic devices as defined above.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be further descibed with reference to examples of embodiments shown in the drawings to which, however, the invention is not restricted.

Figure 1 shows a schematic representation of two NFC-enabled electronic devices.

Figure 2 shows a schematic flow diagram of a method device for performing an encrypted Near Field Communication.

DESCRIPTION OF EMBODIMENTS

Figure 1 shows a schematic representation of a first electronic device 100 and a second

electronic device 200. The first and second electronic devices 100, 200 are designed to communicate via Near Field Communication (NFC). They can be referred to as NFC-enabled devices. The first and second electronic devices 100, 200 may for example be NFC-enabled mobile phones, NFC-enabled handheld computers, NFC-enabled notebook computers or any other NFC-enabled electronic devices.

The first electronic device 100 comprises a first NFC circuit 101. The second electronic device 200 comprises a second NFC circuit 201. The first NFC circuit 101 and the second NFC circuit 201 are designed to perform peer-to-peer Near Field Communication in active communication mode. The first NFC circuit 101 and the second NFC circuit 201 may be designed to also support card-emulation mode and/or reader mode. The first and second NFC circuits 101, 201 may be integrated circuits built into the first and the second electronic devices 100, 200.

The first electronic device 100 further comprises a first cryptographic circuit 102. The second electronic device 200 further comprises a second cryptographic circuit 202. The first cryptographic circuit 102 and the second cryptographic circuit 202 may be integrated circuits built into the first and the second electronic devices 100, 200. The first and the second cryptographic circuits 102, 202 may as well be SIM cards plugged or built into the first and the second electronic device 100, 200. The first and the second cryptographic circuits 102, 202 may as well be located on smartcards plugged or built into the first and the second electronic device 100, 200. The first and second cryptographic circuits 102, 202 may as well be realized as software programs that are executed by microprocessors built into the first and second electronic devices 100, 200.

The first electronic device 100 can transmit data wirelessly via NFC to the second electronic device 200 with the first NFC circuit 101. The second electronic device 200 is designed to receive data wirelessly transmitted via NFC by the first electronic device 100 with the second NFC circuit 201. Data can also be transmitted from the second electronic device 200 to the first electronic device 100. To this end, the second electronic device 200 can transmit data with the second NFC circuit 201. The first electronic device 100 can receive data with the first NFC circuit 101.

The data transfer between the first electronic device 100 and the second electronic device 200 may be secured by encrypting the data transmitted between the

first electronic device 100 and the second electronic device 200. Encryption and decryption of the transmitted data is performed by the first and second cryptographic circuits 102, 202.

Arrows 110 to 116 depict the flow of data in the case of an encrypted data transfer from the first electronic device 100 to the second electronic device 200. If the first and second electronic devices 100, 200 are mobile phones, the data set may for example be a telephone number that is stored in a memory component of the first electronic device 100. The owner of the first electronic device 100 chooses to transfer the telephone number to the second electronic device 200. The first electronic device 100 then passes the unencrypted data set that is to be sent to the second electronic device 200 in a direction 110 to the first NFC circuit 101.

The first NFC circuit 101 passes the unencrypted data set in a direction 111 to the first cryptographic circuit 102. The first cryptographic circuit 102 encrypts the unencrypted data set and passes the encrypted data set in a direction 112 to the first NFC circuit 101.

The first NFC circuit 101 then transmits the encrypted data set in a direction 113 to the second NFC circuit 201 of the second electronic device 200 via NFC.

The second NFC circuit 201 passes the encrypted data set in a direction 114 to the second cryptographic circuit 202. The second cryptographic circuit 202 decrypts the encrypted data set and passes the decrypted data set in a direction 115 to the second NFC circuit 201.

The second NFC circuit 201 then passes the decrypted data set in a direction 116 to the second electronic device 200. The second electronic device 200 may then further process the received data set. If the second electronic device 200 is a mobile phone and the transferred data set relates to a telephone number, the second electronic device may for example show the received data set on a display or save the received data set in a memory circuit of the second electronic device 200.

Data may also be transferred from the second electronic device 200 to the first electronic device 100. In this case the data flow takes place analogous to the description of figure 1, with the first and the second electronic devices 100, 200 interchanged. The second electronic device 200 takes the role of the first electronic

device 100 and the first electronic device 100 takes the role of the second electronic device 200. The first NFC circuit 101 takes the role of the second NFC circuit 201 and the second NFC circuit 201 takes the role of the first NFC circuit 101. The first cryptographic circuit 102 takes the role of the second cryptographic circuit 202 and the second cryptographic circuit 202 takes the role of the first cryptographic circuit 102.

Figure 2 depicts a schematic flow diagram of the procedural steps involved in an encrypted transfer of a data set from the first electronic device 100 to the second electronic device 200 via NFC. In a first step 300, the first electronic device 100 passes an unencrypted data set to the first NFC circuit 101 of the first electronic device 100. The unencrypted data set may for example be a telephone number or another contact information that shall be transferred from the first electronic device 100 to the second electronic device 200. The unencrypted data set may as well be a piece of information related to a payment or another money transfer. The unencrypted data set may as well be any other kind of digital data. The unencrypted data set may comprise any number of binary bits. The unencrypted data set may be grouped into one or more data packets of fixed or variable lengths. The unencrypted data set passed to the first NFC circuit 101 by the first electronic device 100 may as well be a continuous stream of data.

In a second step 301, the first NFC circuit 101 passes the unencrypted data set received in the first step 300 to the first cryptographic circuit 102. The first NFC circuit 101 may pass the unencrypted data set unmodified to the first cryptographic circuit 102. The first NFC circuit 101 may as well modify the unencrypted data set before passing it to the first cryptographic circuit 102. The first NFC circuit 101 may for example group the unencrypted data set into data packets of fixed or variable lengths. If the unencrypted data set is already grouped into data packets, the first NFC circuit 101 may change the size of the data packets of the unencrypted data set before passing it to the first cryptographic circuit 102.

In a third step 302, the first cryptographic circuit 102 encrypts the unencrypted data set received in the second step 301 to create an encrypted data set. The first cryptographic circuit 102 may encrypt the unencrypted data set using any kind of encryption algorithms. The first cryptographic circuit 102 may for example encrypt the data set using a 3DES algorithm, an AES algorithm, a TWOFISH algorithm, an RSA

algorithm, an ECC algorithm, or any other kind of encryption algorithm.

The first cryptographic circuit 102 may utilize a cryptographic key to encrypt the data set. The first cryptographic circuit 102 may for example use a private cryptographic key of the first electronic device 100 that is stored in a memory circuit of the first electronic device 100. The first cryptographic circuit 102 may as well use a public cryptographic key of the second electronic device 200 that is stored in a memory circuit of the first electronic device 100. This public key of the second electronic device 200 may have been previously transferred from the second electronic device 200 to the first electronic device 100. The first cryptographic circuit 102 may as well encrypt the unencrypted data set using a cryptographic key composed out of a private key of the first electronic device 100 and a public key of the second electronic device 200.

The encrypted data set may comprise any amount of binary bits. The encrypted data set may be grouped into data packets of fixed or variable lengths. The number of binary bits of the encrypted data set and/or the number of data packets of the encrypted data set may be equal to or different from the number of binary bits and/or the number of data packets of the unencrypted data set.

In a fourth step 303, the encrypted data set is passed from the first cryptographic circuit 102 to the first NFC circuit 101. The encrypted data set may be passed from the first cryptographic circuit 102 to the first NFC circuit 101 in groups of data packets. The encrypted data set may as well be passed from the cryptographic circuit 102 to the first NFC circuit 101 as a continuous data stream.

Steps 301, 302, 303 may also be repeated one or more times. In this case, the unencrypted data set received by the first NFC circuit 101 in the first step 300 is divided into a number of smaller data sets. The smaller set of unencrypted data are passed to the first cryptographic circuit 102, encrypted and passed back to the first NFC circuit 101 one after another.

In a fifth step 304, the encrypted data set is transmitted from the first NFC circuit 101 of the first electronic device to the second NFC circuit 201 of the second electronic device 200 by means of Near Field Communication. The encrypted data set is transmitted in active communication mode. The transmitted encrypted data set is received by the second NFC circuit 201 of the second electronic device 200.

In a sixth step 305, the encrypted data set received by the second NFC circuit 201 in the fifth 304 is passed from the second NFC circuit 201 to the second cryptographic circuit 202 of the second electronic device 200. The encrypted data set may be grouped into data packets before passing them to the second cryptographic circuit 202.

In a seventh step 306, the second cryptographic circuit 202 decrypts the encrypted data set to generate a decrypted data set. The second cryptographic circuit 202 may use the same cryptographic algorithm as the first cryptographic circuit 102 in the third step 302. The decrypted data set may preferably be identical to the original unencrypted data set that was encrypted by the first NFC circuit 101 in the third step 302. The decrypted data set may as well contain additional or less data than the original unencrypted data set.

For the decryption of the encrypted data set in the seventh step 306, the second cryptographic 202 may utilize a cryptographic key. If the first cryptographic circuit 102 of the first electronic device 100 has used a private cryptographic key of the first electronic device 100 to encrypt the data set in the third step 302, the second cryptographic circuit 202 of the second electronic device 200 may use a public cryptographic key of the first electronic device 100 to decrypt the encrypted data set. The public cryptographic key of the first electronic device 100 may have been previously transmitted from the first electronic device 100 to the second electronic device 200 before and may be stored in a memory circuit of the second electronic device 200.

If the first cryptographic circuit 102 of the first electronic device has used a public cryptographic key of the second electronic device 200 to encrypt the data set in the third step 302, the second cryptographic circuit 202 of the second electronic device may use a private cryptographic key of the second electronic device 200 that may be stored in a memory circuit of the second electronic device 200.

If the first cryptographic circuit 102 of the first electronic device has used a combination of a private cryptographic key of the first electronic device 100 and a public cryptographic key of the second electronic device 200 to encrypt the data set in the third step 302, the second cryptographic circuit 202 of the second electronic device 200 may use a combination of a public cryptographic key of the first electronic device 100 and a private cryptographic key of the second electronic device 200 to decrypt the

encrypted data set in step 306.

The encryption in step 302 and the decryption in step 306 may use any other kind of encryption and decryption scheme that allows encrypting the unencrypted data set and restoring the unencrypted data set from the encrypted data set.

In an eight step 307, the second cryptographic circuit 202 passes the decrypted data set to the second NFC circuit 201 of the second electronic device. The steps 305, 306, 307 may as well be repeated one or more times to decrypt the encrypted data set in sequential portions.

In a ninth step 308, the decrypted data set is passed from the second NFC circuit 201 to other circuits of the second electronic device 200 for further processing. The decrypted data set passed on by the second NFC circuit 201 in step 308 may be identical to the unencrypted data set passed to the first NFC circuit 101 in step 300. The decrypted data set may also contain additional data such as information related to the data transfer between the first electronic device 100 and the second electronic device 200. The decrypted data set may as well lack information of the unencrypted data set.

The encrypted Near Field Communication between the first electronic device 100 and the second electronic device 200 may be used to securely transfer data from the first electronic device 100 to the second electronic device 200 to ensure confidentiality. In this case, the first cryptographic circuit 102 uses a public key of the second electronic device 200 to encrypt the data set and the second cryptographic circuit 202 uses a private cryptographic key of the second electronic device 200 to decrypt the encrypted data set. This ensures that a third party that eavesdrop the transmission of the encrypted data set is unable to recover the original unencrypted data set without knowledge of the private cryptographic key of the second electronic device 200.

The encrypted Near Field Communication between the first electronic device 100 and the second electronic device 200 may as well be used to sign the transferred data set. In this case, the first cryptographic circuit 102 of the first electronic device 100 uses a private cryptographic key of the first electronic device 100 to encrypt the data set. The second cryptographic circuit 202 of the second electronic device 200 uses a public cryptographic key of the first electronic device 100 to decrypt the encrypted data set. In this case, the second electronic device 200 may be assured that the transmitted data set was transmitted by the first electronic device 100 and has not been

tempered or replaced by a third party.

The encrypted Near Field Communication between the first electronic device 100 and the second electronic device 200 may as well be used to ensure both authenticity and confidentiality of the transmitted data set by using combined cryptographic keys. In this case, the first cryptographic circuit 102 may for example use a combination of a private cryptographic key of the first electronic device 100 and a public cryptographic key of the second electronic device 200 to encrypt the data set. The second cryptographic circuit 202 may use a combination of a public cryptographic key of the first electronic device 100 and a private cryptographic key of the second electronic device 200 to decrypt the encrypted data set.

The encrypted Near Field Communication between the first electronic device 100 and the second electronic device 200 may for example be used to transfer contact data from the first electronic device 100 to the second electronic device 200. If the first and second electronic devices 100, 200 are mobile phones, the encrypted data transfer may for example be used to transmit a telephone number or a digital picture file from the first mobile phone to the second mobile phone.

The encrypted Near Field Communication may as well be used to transfer further cryptographic keys from the first electronic device 100 to the second electronic device 200 that may be used for further communication between the first electronic device 100 and the second electronic device 200.

The encrypted Near Field Communication between the first electronic device 100 and the second electronic device 200 may as well be used to establish a communication channel using another technology than NFC. The first electronic device 100 and the second electronic device 200 may for example exchange information necessary to establish a Bluetooth connection between the first electronic device 100 and the second electronic device 200.

The encrypted Near Field Communication between the first electronic device 100 and the second electronic device 200 may as well be used to transfer information related to a monetary transaction. The first electronic device 100 may for example transfer encrypted information to the second electronic device 200 that relates to a transfer of money from the owner of the first electronic device 100 to the owner of the second electronic device 200.

An application of encrypted Near Field Communication between the first electronic device 100 and the second electronic device 200 may require several encrypted data transfers from the first electronic device 100 to the second electronic device 200 and from the second electronic device 200 to the first electronic device 100. Each such data transfer between the two electronic devices 100, 200 may follow the procedure explained in the description of figure 2.

The first electronic device 100 and the second electronic device 200 may be capable of generating pairs of public and private cryptographic keys. The first and second electronic devices 100, 200 may comprise memory circuits that may be capable of storing one ore more private or public cryptographic keys. The first and second electronic devices 100, 200 may as well allow a user to enter new cryptographic keys. The cryptographic keys may for example be entered via a keyboard of the first and the second electronic devices 100, 200. The first and second electronic devices 100, 200 may as well use cryptographic keys that are stored on SIM cards or smartcards plugged or built into the first and second electronic devices 100, 200.

The encrypted Near Field Communication between the first electronic device 100 and the second electronic device 200 may as well employ symmetric cryptographic algorithms without public cryptographic keys.

Finally, it should be noted that the aforementioned embodiments illustrate rather than limit the invention, and that those skilled in the art will be capable of designing many alternative embodiments without departing from the scope of the invention as defined by the appended claims. In the claims, any reference signs placed in parentheses shall not be construed as limiting the claims. The word "comprising" and "comprises", and the like, does not exclude the presence of elements or steps other than those listed in any claim or the specification as a whole. The singular reference of an element does not exclude the plural reference of such elements and vice-versa. In a device claim enumerating several means, several of these means may be embodied by one and the same item of software or hardware. The mere fact that certain measures are recited in mutually different dependent claims does not indicate that a combination of these measures cannot be used to advantage.

CLAIMS

1. An electronic device (100) comprising:
- a Near Field Communication circuit (101) capable of sending and receiving data, and
- a cryptographic circuit (102) capable of encrypting and decrypting data, wherein
the electronic device (100) is designed to encrypt data with the cryptographic circuit (102) and to transmit the encrypted data with the Near Field Communication circuit (101), and
wherein the electronic device (100) is further designed to receive encrypted data with the Near Field Communication circuit (101) and to decrypt the encrypted data with the cryptographic circuit (102).

2. The electronic device (100) as claimed in claim 1, wherein the electronic device (100) is designed to transmit encrypted data to another electronic device (200).

3. The electronic device (100) as claimed in claim 1, wherein the electronic device (100) is designed to receive encrypted data from another electronic device (200).

4. The electronic device (100) as claimed in claim 1, wherein the cryptographic circuit (102) is designed to encrypt data with a private cryptographic key, wherein the electronic device (100) is designed to transmit a public cryptographic key.

5. The electronic device (100) as claimed in claim 1, wherein the electronic device (100) is designed to receive a public cryptographic key, wherein the cryptographic circuit (102) is designed to decrypt data with the public cryptographic key.

6. The electronic device (100) as claimed in claim 1, wherein the electronic device (100) is designed to receive a public cryptographic key, wherein the cryptographic circuit (102) is designed to encrypt data with the public cryptographic key.

7. The electronic device (100) as claimed in claim 1, wherein the electronic device (100) is designed to transmit a public cryptographic key, wherein the

cryptographic circuit (102) is designed to decrypt data with a private cryptographic key.

8. The electronic device (100) as claimed in claim 1, wherein the electronic device (100) is designed to receive a first cryptographic key and to combine the first cryptographic key with a second cryptographic key to form a third cryptographic key, wherein the cryptographic circuit (102) is designed to encrypt data with the third cryptographic key.

9. The electronic device (100) as claimed in claim 1, wherein the electronic device (100) is designed to receive a first cryptographic key and to combine the first cryptographic key with a second cryptographic key to form a third cryptographic key, wherein the cryptographic circuit (102) is designed to decrypt data with the third cryptographic key.

10. The electronic device (100) as claimed in claim 1, wherein the electronic device (100) is designed to generate a pair of private and public cryptographic keys.

11. The electronic device (100) as claimed in claim 1, wherein the electronic device (100) comprises a data storage that is capable of holding a cryptographic key.

12. A method for sending data with the following steps:
- Encrypting data with a cryptographic circuit (102); and
- Transmitting the data with a Near Field Communication circuit (101).

13. The method as claimed in claim 12, wherein the data is encrypted using a 3DES algorithm.

14. The method as claimed in claim 12, wherein the data is encrypted using an AES algorithm.

15. The method as claimed in claim 12, wherein the data is encrypted using a Twofish algorithm.

16. The method as claimed in claim 12, wherein the data is encrypted using an RSA algorithm.

17. The method as claimed in claim 12, wherein the data is encrypted using an ECC algorithm.

18. A method for receiving data with the following steps:
- Receiving data with a Near Field Communication circuit (101); and
- Decrypting the data with a cryptographic circuit (102).

19. A system comprising two electronic devices (100, 200) according to claim 1.

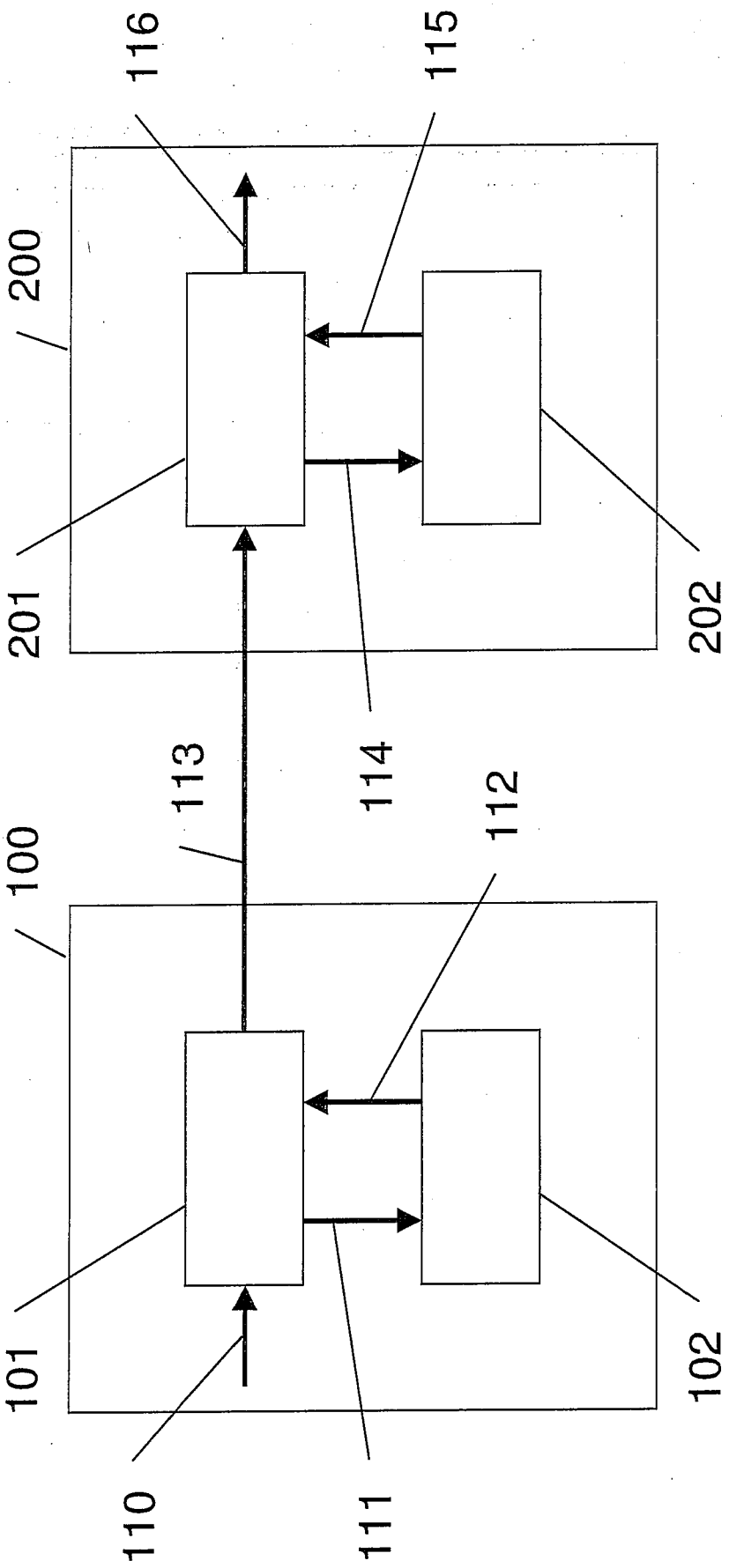

Fig. 1

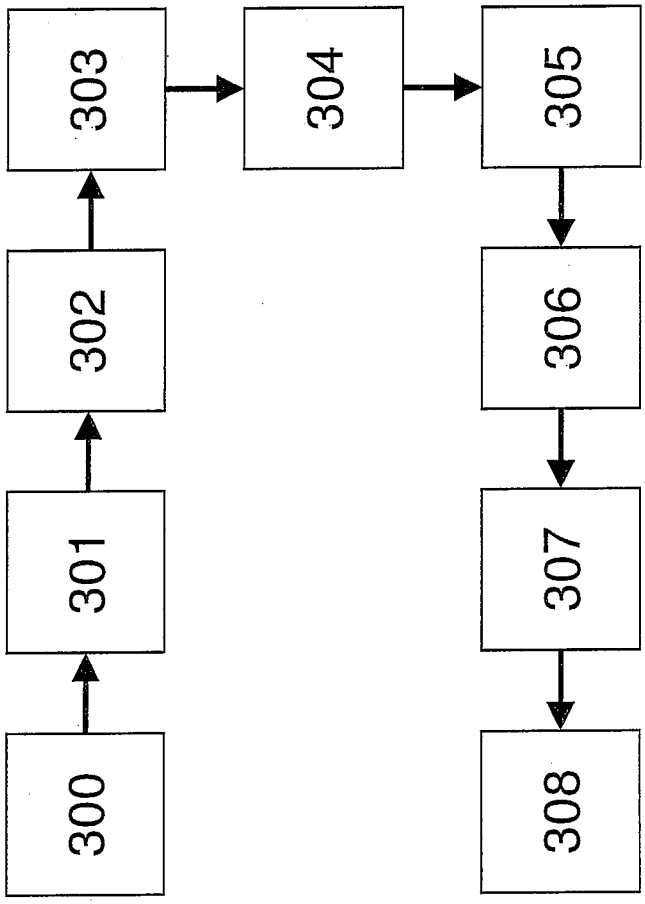

Fig. 2