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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 February 2003 (20.02.2003)

PCT

(10) International Publication Number
WO 03/015340 A1

(51) International Patent Classification^7: H04L 9/00

(21) International Application Number: PCT/FI02/00642

(22) International Filing Date: 18 July 2002 (18.07.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20011611 7 August 2001 (07.08.2001) FI

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **RÖNKKÄ, Risto** [FI/FI]; Aarikkalankatu 2 as. 4, FIN-33530 Tampere (FI). **SORMUNEN, Toni** [FI/FI]; Artturintie 6, FIN-33880 Lempäälä (FI). **KIIVERI, Antti** [FI/FI]; Peikontie 1 F 72, FIN-90550 Oulu (FI). **JAUHIAINEN, Antti** [FI/FI]; Pääskyläntie 3, FIN-90440 Kempele (FI).

(74) Agent: **TAMPEREEN PATENTTITOIMISTO OY**; Hermiankatu 12 B, FIN-33720 Tampere (FI).

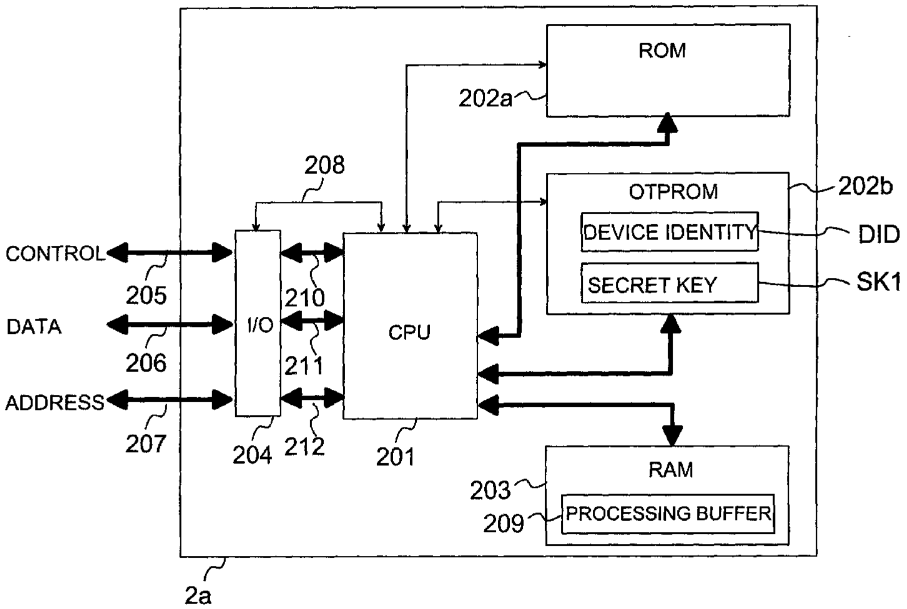
(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK (utility model), SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: A METHOD FOR PROCESSING INFORMATION IN AN ELECTRONIC DEVICE, A SYSTEM, AN ELECTRONIC DEVICE AND A PROCESSING BLOCK



(57) Abstract: The invention relates to a method for processing information in an electronic device (1) comprising at least one processing block (2a) for controlling the operation of the electronic device (1), and a memory (2d, 2e, 2f, 3a, 3b, 3c, 202a, 202b, 203). In the method at least a first private key (SK2) is used for processing information. At least a protected mode and a normal mode are established in the processing block (2a). Part of the memory (202a, 202b) can be accessed only in said protected mode. At least said first private key (SK1) is stored in the memory (202a, 202b) that is accessible in said protected mode.

A method for processing information in an electronic device, a system, an electronic device and a processing block

The present invention relates to a method for processing encrypted information in an electronic device according to the preamble of the appended claim 1. The invention also relates to a system according to the preamble of the appended claim 7, an electronic device according to the preamble of the appended claim 13, as well as to a processing block according to the preamble of the appended claim 15.

With an increase in the data processing properties of portable devices, more information can be stored in them, which may also be confidential or otherwise such information that must not be revealed to an outsider. The carrying of portable devices will, however, increase the risk that the portable device is lost or stolen, wherein an attempt must be made to protect the information stored in it with an encryption method. For portable devices, it is typically possible to determine a password which the user must enter in the device when the device is turned on before the device can be used normally. However, such a protection is relatively easy to pass, because the passwords that are used are normally relatively short, typically having a length of less than ten characters. On the other hand, even if no attempt were made to find out the password, the information contained in the device can be accessed for example by transferring the storage medium, such as a hard disk, into another device. If the information contained in the storage medium is not in encrypted format, the information stored in the storage medium can be easily found out.

It is known that information needed by the user or the device can be encrypted with one key, the encrypted information can be stored in the memory of the device, and it can be decrypted with another key. In asymmetric encryption, the key used in encryption is different from the key used in decryption. Correspondingly, in symmetric encryption, the key used in encryption is the same as the key used in decryption. In asymmetric encryption, these keys are normally called a public key and a private key. The public key is intended for encryption and the private key is intended for decryption. Although the public key may be commonly known, on the basis of the same it is normally not possible to easily determine the encryption key corresponding to the public key, wherein it is very difficult for an outsider to find out information encrypted with this public key. One example of a system based on the use of such a public key and a private key is the PGP system (Pretty Good Privacy), in which the user encrypts the information to be transmitted with the public key of the receiver, and the receiver will then open the encrypted information with his/her private key. However, there are considerable drawbacks in the systems of prior art. The key strings required by sufficiently secure systems are so long that even their storage in a safe way causes considerable costs. If the key string is too short, it will be relatively easy to break it up with modern data processing equipment. In other words, the private key can be defined on the basis of the content and the public key (known content attack). This problem is particularly significant in portable data processing and communicating devices, in which the limited processing capacity also prevents the use of long keys.

The US patent 6,169,890 discloses a method and device in which, after the user has been identified, it is possible to use a key stored in a SIM card for user identification in a communication network. The system is intended to be used for example in payment transactions, wherein the user performs payment transactions in his/her terminal which is arranged to communicate with a terminal of the payment system by means of the mobile communication network. Thus, the user enters his/her PIN code in the mobile station, and the user of the mobile station is identified on the basis of the code. The system comprises a database in which the mobile phone numbers of the users authorized to use the system have been stored. Thus, when the user contacts such a system, it is checked from the database on the basis of the number of the caller, whether the user is authorized to use the service. One drawback of such a system is that the PIN code used in the identification of the user is relatively short, typically four characters long, wherein it is relatively easy to find it out by means of methods known at present. When the length of the key is increased, the amount of memory required in the SIM card for storing the PIN code should be increased as well, which considerably raises the manufacturing costs of the SIM card. On the other hand, the act of storing the private key to such a memory which can be examined from outside the device, may present a significant safety risk, because when the device is lost or when it otherwise ends up in the hands of outsiders, the encrypted information may be found out on the basis of the encryption key stored in the device.

One purpose of the present invention is to bring about a method for processing encrypted information in such a manner that the decryption of information by analysing the device is not possible in practice. The invention is based on the idea that the processing block of the electronic device is set to operate at least in two different operating modes: a protected mode and a normal mode. The protected mode is arranged to be such that the information processed in the protected mode cannot be examined from outside the processing block. Thus it is possible to store an encryption key in the memory that can be used in the protected mode, said encryption key being used for encryption and decryption of information processed outside the protected mode in such a manner that this encryption key cannot be found out. More precisely, the method according to the present invention is primarily characterized in what will be presented in the characterizing part of the appended claim 1. The system according to the present invention is primarily characterized in what will be presented in the characterizing part of the appended claim 7. The electronic device according to the present invention is primarily characterized in what will be presented in the characterizing part of the appended claim 13. Further, the processing block according to the present invention is primarily characterized in what will be presented in the characterizing part of the appended claim 15.

The present invention shows remarkable advantages compared to solutions of prior art. The analysis of the electronic device according to the invention in a manner enabling the examination of the protected mode is, in practice, impossible without breaking the electronic device. Because the encryption key used in the protected mode is advantageously device-specific, there is no use of finding out the encryption key of a broken device. When the method according to the invention is applied, it is possible to use longer keys, because in the protected mode it is possible to encrypt and/or decrypt a long encryption key. The encrypted encryption key can be stored in an external memory which is more advantageous than a memory used in the protected mode.

In the following, the invention will be described in more detail with reference to the appended drawings, in which

Fig. 1 shows an electronic device according to a preferred embodiment of the invention in a reduced block chart,

Fig. 2 shows the structure of the processing block according to a preferred embodiment of the invention in a reduced manner,

Fig. 3 shows the function of the method according to a preferred embodiment of the invention in a flow chart,

Fig. 4 illustrates the identification of the user in a mobile communication system in a reduced chart, and

Fig. 5 shows a known principle on forming a digital signature.

The invention can be applied in an electronic device 1, in which it is possible to process information in at least partly encrypted format. Such electronic devices 1 include, for example, a mobile communication device, a computer, such as a personal computer (PC) or a portable computer, a personal digital assistant device (PDA), MP3 players, CD players, DVD players, video devices, digital TV sets, etc. The electronic device 1 according to an advantageous embodiment of the invention, shown in Fig. 1, comprises at least a control block 2, memory means 3, and a user interface 4 which can advantageously comprise a display, a keyboard and/or audio means. Furthermore, the electronic device according to Fig. 1 comprises mobile station means 5. The memory means 3 preferably comprise a read-only memory ROM and a random access memory RAM. At least a part of the read-only memory ROM is an electrically erasable programmable read-only memory EEPROM, such as a FLASH memory. The read-only memory ROM is used, for example, for storing program commands of the processor, for specific fixed setting data, or the like. The electrically erasable programmable read-only memory EEPROM can be used for example for storing the encryption key in the encrypted format, as will be presented below in this description.

Figure 2 shows, in a reduced manner, the structure of a processing block 2a of the control block 2 according to an advantageous embodiment of the invention. The processing block comprises a processor 201 (CPU, Central Processing Unit), and the program code controlling the function of the same can be partly stored in the read-only memory 202a, 202b, which can be a one-time programmable read-only memory (OTPROM) and/or reprogrammable read-only memory (for example EEPROM). Part of the boot program is advantageously stored in such a memory the contents of which cannot be changed after the program has been stored (OTPROM, ROM). This is necessary for example in such applications in which booting is conducted at least in two stages in such a manner that the preceding stage conducts the verification of the authenticity of the program code of the next stage before the execution of the program code of the next stage begins. A first private key SK1 used in connection with the method according to the invention is also stored in the read-only memory 202a, 202b, preferably in the one time programmable read-only memory 202b. The processing block 2a also contains a random access memory 203 which can be arranged in a manner known as such as a linear memory space and/or it can contain a random access memory for implementing the possible register structure of the processor. The processor 201 is not limited to any particular processor but it may vary in different applications, wherein the details of the memories 202a, 202b, 203 can differ from each other in different applications. The processing block 2a contains a connection block 204, by means of which the processing block 2a can be connected to the other functional blocks of the electronic device 1. Via the connection block 204 for example a control bus 210, a bus 211 and an address bus 212 of the processor are coupled to the respective external control bus 205, data bus 206 and address bus 207 of the processing block 2a. In this advantageous embodiment of the invention, the processing block 2a and the other functional blocks 2b to 2f of the control block are presented as discrete blocks. However, it is obvious that at least some of said other functional blocks 2b to 2f of the control block can be arranged as a single integrated block in connection with the processing block 2a in such a manner that they can be used in the protected mode.

In the following, the operation of the method according to a preferred embodiment of the invention in the electronic device 1 of Fig. 1 will be described with reference to the flow chart of Fig. 3. In connection with the turning on of the electronic device, conventional boot-up operations known as such are executed (block 301 in Fig. 3). Here, in connection with the boot-up the processing block 2a is advantageously set to the normal mode. Thus, the control line 208 of the connection block 204 is set to a state in which the internal buses 210, 211, 212 of the processing block 2a are coupled to the external buses 205, 206, 207 of the processing block 2a. The control line 208 is advantageously also used for controlling the function of the internal random access memory 203 of the processing block 2a in such a manner that in the normal mode of the processing block the contents of the random access memory 203 cannot be read from outside the processing block 2a.

At that stage when it is necessary to process encrypted information, the following steps are taken in this preferred embodiment of the invention. It is, for example, assumed that encrypted information has been received via the mobile station means 5, which information is first stored in connection with the reception (block 302) in the external receiving buffer (not shown) of the processing block 2a. The receiving buffer is established, for example, in the random access memory 2f of the control block. The storing is conducted in a manner known as such, for example by means of a storage program formed in the program code of the processor, advantageously in such a manner that the processing block 2a reads the information received from the mobile station means and transfers it to the receiving buffer allocated in the memory 2f. The received information also contains information thereon that said information or at least part of it is in encrypted format. Thus, the information indicating the part of the information that is encrypted is also transmitted to the processing block 2a, wherein on the basis of this information the processor can conduct the necessary measures to use the second private key for decryption.

To decrypt the information, the second private key stored in the reprogrammable read-only memory 3b is advantageously decrypted in the following manner. The encrypted second private key SK2 is read in the internal random access memory 203 of the processing block 2a, for example to a processing buffer 209 (block 303). Thereafter, to shift to protected mode, the processor 201 of the processing block 201 sets the control line 208 of the connection block to a state in which there is no connection from the internal buses 210, 211, 212 of the processing block 2a to the external buses 205, 206, 207 (block 304). Thus, the internal function of the processing block 2a cannot be detected by means of conventional analysing means. In this protected mode the processor 201 can still read the internal random access memory 203 of the processing block 2a. Thereafter the processor 201 executes a program code by means of which the second private key SK2 is decrypted by means of the first private key SK1 (block 305) stored in the read-only memory 202a, 202b of the processing block. After the decryption, the second private key SK2 can be stored (block 306) in the random access memory, for example in the internal random access memory 203 of the processing block 2a, or in the random access memory 2f, 3c outside the processing block.

The decryption of the information to be processed can be conducted by using the second private key SK2. The processing block is possibly set to the normal mode by changing the state of the control line 208 of the connection block (block 307). Thus, it is possible to read the received encrypted information in the processing buffer 209 formed in the internal random access memory 203 of the processing block 2a. The amount of information that can be read in the processing block at time can vary in different applications and different situations. In some cases it is possible to read all the encrypted information in the processing buffer 209, whereafter the read information is decrypted (block 308). In the decryption the second private key SK2 is now used, which second private key SK2 has been decrypted at an earlier stage.

The decryption of the information to be processed can be conducted either in the protected mode or in the normal mode. First, the function of the method is described in such a case where the decryption is conducted in the protected mode of the processing block 2a. Thus, the program code used in the decryption of information also has to be read advantageously in the random access memory 203 of the processing block 203, if it is not stored in the read-only memory 202a, 202b of the processing block 2a. If the program code used in the decryption is loaded from outside the processing block 2a, the authenticity of the program code must be verified before decryption. The processing block 2a is set to the normal mode and stored, encrypted information is read from the random access memory 2f, 3b in the internal read-only memory 203 of the processing block. Thereafter the processing block 2a is set to the protected mode, whereafter the processor 201 executes the program code used in the encryption of information from the internal memory 202a, 202b, 203. After the decryption the processing block 2a is set to the normal mode and the decrypted information is stored outside the processing block 2a in the random access memory 2f, 3c. Thereafter the next possible part of the encrypted information is subjected to corresponding processes for decryption and storing the information in the read-only memory 2f, 3c. The above-described process continues until the processed information has been decrypted.

If the second private key SK2 is in connection with the protected mode of the processing block 2a stored in such a memory which can be read in the normal mode of the processing block 2a, it may be possible that the second private key SK2 can be found out by analysing the device. This can be prevented in such a manner that before the processing block 2a is set from the protected mode to the normal mode, the second private key SK2 in the encrypted format is removed from such a random access memory which can be accessed in the normal mode. In practice, this means that the second private key SK2 is always decrypted when the processing block 2a has been set from the normal mode to the protected mode, and it is necessary to use this second private key SK2 for example for decryption of the encrypted information. In a corresponding manner, if the first private key SK1 has been copied from the read-only memory 202a, 202b to such a memory which can be read in the normal mode of the processing block 2a, the first private key SK1 is also removed from such a memory before the processing block 2a is set from the protected mode to the normal mode.

The internal read-only memory 202a, 202b of the processing block is relatively expensive when compared to the external read-only memory 2d, 2e, 3a, 3b, and thus the aim is to minimize the size of the internal read-only memory 202a, 202b. Thus, the code used in the decryption of the second private key SK2 is advantageously stored either in the read-only memory 2d, 2e of the control block or in the external read-only memory 3a, 3b, from which the program code is transferred to the internal random access memory 203 of the processing block 2a. The program code used in the decryption of the encrypted information is also advantageously stored in the read-only memory 202a, 202b of the processing block, or it is loaded from another read-only memory 2d, 2e, 3a, 3b of the electronic device 1 in the random access memory 203 before decryption. If the program code is loaded from outside the processing block, the program code verifying the authenticity of the program code is stored in the read-only memory 201 of the processing block. In a preferred embodiment of the invention the internal read-only memory 202a, 202b of the processing block 2a contains primarily the first private key SK1 stored therein.

In the method according to a second preferred embodiment of the invention, the decryption is primarily conducted outside the processing block 2 in the following manner. The processing block 2 decrypts the second private key SK2 in the protected mode in accordance with the above-presented principles, and stores this second private key in the external random access memory 2f, 3c of the processing block 2a in an unencrypted format. Thereafter, the information is decrypted in the normal mode of the processing block 2a. After this, the processing block 2a can be in the normal mode, because the access to the read-only memory 202, 202b used for storing the first private key SK1 has been denied. In this alternative the encrypted information does not have to be read in the internal random access memory 203 of the processing block 2a, but the operation can be implemented primarily in the external memory means 2f, 3c of the processing block 2a. The second private key SK2 stored in the random access memory 2f, 3c disappears from the random access memory 2f, 3c latest when the operating voltage of the electronic device 1 is switched off. Thus, there is no risk that an outsider could easily find out the second private key SK2 stored in the electronic device 1.

This second embodiment is advantageous especially in such applications in which the act of keeping the private keys secret does not require as high a level of protection as in the first preferred embodiment. Because in this method according to the second embodiment the second private key is not always decrypted when the processing block is set to the protected mode, less processing capacity is required from the processing block 2a. Thus, the method according to the second preferred embodiment can be used in such embodiments in which continuous decryption is necessary, for example in connection with the processing of an encrypted video signal, and in which the level of protection according to the second embodiment is sufficient.

Because the first private key SK1 stored in the internal read-only memory 201 of the processing block 2a is primarily used for decryption of the second private key SK2, the first private key SK1 can be relatively short. The invention, however, enables the act of increasing the length of the second private key SK2 without having to increase the amount of the internal read-only memory 202a, 202b of the processing block, that is considerably more expensive than the external memory. The first private key SK1 used in connection with the invention is advantageously a symmetric key, but it is obvious that the invention is not restricted solely to applications of this type. Typically, the minimum length of symmetric keys is approximately 100 bits and by comparison therewith, the minimum length of asymmetric keys is approximately ten times as long, i.e. ca 1000 bits.

The description hereinabove presents only one possible way of implementing the protected mode. It is, however, obvious that in practice the protected mode can also be implemented with another method in such a manner that the analysis of the internal function of the processing block 2a in the protected mode is extremely difficult or even impossible. Especially the examination of the internal read-only memory 202a, 202b of the processing block 2a from outside has to be made as difficult as possible. Furthermore when the solution according to the invention is used, it is, in practice, impossible to find out the first private key SK1 without breaking the device. On the other hand, the internal read-only memory 202a, 202b of the processing block can be divided into a protected area and an unprotected area, wherein it is possible to allow access to the unprotected area from outside the processing block 2a and/or the processor 201 can read the contents of this unprotected area also in the normal mode. In this case such information is stored in the protected area which can only be accessed by the processor 201 in the protected mode. In addition, it is obvious that the internal random access memory of the processing block 2a can also be divided into a protected and unprotected area, wherein there is no access to the protected area from outside the processing block 2a.

The invention can also be applied by using two or more processors (not shown) instead of one processor 201. Thus, at least one processor 201 is primarily used in the protected mode, and the other processors are used in the normal mode. The other processors do not have an access to read the memory 202a, 202b, 203 used by the processor operating in the protected mode. The necessary communication between the processor 201 of the protected mode and the other processors can in this embodiment be arranged for example by means of a dual port memory (not shown) or by determining in the random access memory 2f, 3c a memory space which can be processed by the processor of the protected mode and by at least one normal mode processor.

Hereinabove, an embodiment of the invention was described in which information was decrypted. In a corresponding manner, the invention can be applied for encryption of information to be transmitted and/or stored to a storage medium by means of the second private key SK2. In that case as well, the second private key SK2 is decrypted, if it has not been decrypted already. Thereafter the information can be encrypted with this second private key SK2 with measures substantially reverse to the decryption. Also in this situation the decryption can be performed either inside the processing block 2a by transferring the information to be encrypted entirely or partly to the internal random access memory 203 of the processing block 2a to be encrypted therein, or the encryption is conducted outside the processing block 2a. After the encryption the encrypted information is, for example, transmitted to the mobile communication network NW, or it is stored in a storage medium, such as the random access memory 2f, 3c or reprogrammable read-only memory 3b.

The invention is suitable to be used also in reliable identification of the user's electronic device 1, for example in a mobile communication system according to Fig. 4. Thus, the first private key SK1 stored in the internal read-only memory 202a, 202b of the processing block 2a is used for verifying the electronic device for example with a digital signature advantageously in the following manner. Advantageously, the second private key SK2 is stored in an encrypted format in the external read-only memory 3a, 3b of the processing block 2a. Thus, this second private key SK2 is decrypted by means of the first private key SK1 stored in the internal read-only memory 202a, 202b of the processing block 2a, as was presented earlier in this description. Thereafter the second private key SK2 can be used for example for forming a digital signature. The mobile station means of the electronic device 1 are utilized to communicate with a mobile services switching centre MSC in a way known as such via a base station system BSS. At the connection set-up stage identification information is established in the electronic device, for example from the device identity DID, and possibly from the international mobile equipment identity (IMEI). The identification information can be verified with a digital signature. The device identity DID is advantageously stored in the internal one time programmable read-only memory 202b of the processing block 2a. Thus, the processing block 2a is set to a protected mode and the device identity

DID is read in the random access memory 203. Thereafter a hash value is calculated from the device identity DID and possible other identification information for example by means of a hash function. The hash value is signed in a manner known as such by using the second private key SK2. Thereafter the processing block 2a is set to the normal mode and the identification information and the digital signature are transferred to the external random access memory 2f, 3c of the processing block. Now the identification data and the digital signature can be transmitted to the mobile communication network for the identification of the user's electronic device 1. The mobile communication network, for example a home location register HLR, contains information on the international mobile equipment identity IMEI and the public key PK corresponding to the second private key SK2 used in signing the identification information of the electronic device 1, by means of which public key it is possible to verify the authenticity of the digital signature. Thus, it is possible to rely on the identification data formed by means of the method according to the invention.

It is obvious that, for different uses, it is possible to store more than one private key SK1 in the read-only memory 202a, 202b of the processing block 2a. On the other hand, one private key SK1 stored in the read-only memory 202a, 202b of the processing block 2a can be used for encrypting several keys SK2 needed in the operation of the electronic device. Furthermore, the first private key SK1 can also be used for decryption of the device identity DID, if the device identity DID is not stored in the protected internal read-only memory 202a, 202b of the processing block 2a. Such keys and/or device identity can thus be stored in encrypted format in the external memory means 2d, 2e, 3 of the processing block 2a, wherein when such keys and/or device identity is used, decryption is performed according to the invention by means of the first private key SK1, as was already disclosed earlier in this description.

In encryption and decryption it is possible to use the same keys (symmetric encryption), or the keys can be different (asymmetric decryption), wherein the term public key and private key are generally used for the keys. The public key is intended for encryption and the corresponding private key is intended for decryption. There are a number of known encryption methods which can be applied in connection with the present invention. Symmetric encryption methods to be mentioned in this context include Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Rivest's Cipher 2 (RC2). An asymmetric encryption method is Rivest, Shamir, Adleman (RSA). Also so-called hybrid systems have been developed, employing both asymmetric encryption and symmetric encryption. In such systems, asymmetric encryption is normally used when the encryption key to be used in symmetric encryption is transmitted to the receiver, wherein the symmetric encryption key is used in the encryption of actual information.

For the transmission of public keys to be used in asymmetric encryption, a system has been developed which is called Public Key Infrastructure (PKI). This system comprises servers in which the public keys are stored and from which a user needing a key can retrieve the key. Such a system is particularly applicable for use by companies, wherein the company itself does not need to transmit its public key to anyone who wishes to transmit information to the company in an encrypted format.

For digital signatures, several systems have been developed, such as the RSA, DSA (Digital Signatures Algorithm), and ECC (Elliptic Curve Cryptography). These systems use algorithms which compress the information to be signed, including SHA-1 (Secure Hash Algorithm) and MD5 (Message Digest 5) to be mentioned in this context. Figure 6 shows the forming of a digital signature in a principle view. After this, data 501 to be signed is transmitted to a block executing a hash function. After this, the hash data formed by the hash function is signed 503 with a private key SK. The signature 504 is connected to the data 501 to be signed. At the stage of verifying the signed data, the data confirmed with the signature is led to a block 505 performing the hash function, for producing hash data 506. The signature is verified 507 by using a public key PK corresponding to the signatory's private key, after which the hash data 506 is compared 508 with the data formed in the verification 507 of the signature. If the data match, the signed data can be relied on with a high probability.

At the stage of manufacture of the electronic device 1 according to the invention, and/or at the stage of updating the software, the required confirmation data and programs are formed in the memory 2d, 2e, 3a, 3b preferably in the following way. The program codes required in the verifications are stored in the control block 2, including a boot program, a program for computing the digital signature, and encryption and decryption algorithm/algorithms. The manufacturer stores the first private key SK1 and possibly also the device identity DID in the read-only memory 202a, 202b of the processing block. At the stage of assembling the components (block 302), also the control block 2 is installed in the circuit card of the electronic device 1 (not shown). The manufacturer stores the other possible application programs for example in the programmable memory 3b and/or in the one time programmable memory 3a. After this, the electronic device 1 can be delivered to a dealer or a service provider, such as a mobile telephone operator.

Although it has been disclosed above that the first private key SK1 is stored in the read-only memory 202a, 202b of the protected mode, it is obvious that instead of the same it is possible to store other information in the read-only memory, on the basis of which the first private key SK1 can be established again. One such alternative is the storing of a seed number, wherein a program is established in the program code of the processor 201 to generate a first private key SK1 on the basis of this seed number.

It is obvious that the present invention is not limited solely to the above-presented embodiments, but it can be modified within the scope of the appended claims.

Claims:

1. A method for processing information in an electronic device (1) which comprises at least one processing block (2) for controlling the operation of an electronic device (1) and memory (2d, 2e, 2f, 3a, 3b, 3c, 202a, 202b, 203), and in which method at least a first private key (SK1) is used for processing the information, **characterized** in that at least protected mode and normal mode are established in the processing block (2a), that part of the memory (202a, 202b) is accessible only in said protected mode, and that information of at least said first private key (SK1) is stored in the memory (202a, 202b) that is accessible in said protected mode.

2. The method according to claim 1, **characterized** in that in said protected mode the transfer of information from the processing block (2a) is prevented to prevent the determination of the internal function of the processing block (2a).

3. The method according to claim 1 or 2, **characterized** in that at least one second private key (SK2) is established in the electronic device (1), said second private key being encrypted with said first private key (SK1) and stored in encrypted format in the memory (2d, 2e, 2f, 3a, 3b, 3c) that is accessible in an unprotected mode of the electronic device, wherein the second private key (SK2) can be decrypted with said first private key (SK1).

4. The method according to claim 2 or 3, **characterized** in that the electronic device (1) receives encrypted information, wherein to decrypt the encrypted information, said second private key (SK2) is decrypted with said first private key (SK1), and the information is decrypted with said decrypted second private key (SK2).

5. The method according to any of the claims 1 to 4, **characterized** in that when said first key (SK1) is used, the processing block (2a) is set in said protected mode.

6. The method according to any of the claims 1 to 5, **characterized** in that in the method an electronic device (1) is authenticated, which electronic device contains at least a device identity (DID) stored therein, and at least one second private key (SK2) which is encrypted with said first private key (SK1) which entails at least one public key (PK) wherein at least the following steps are taken in the authentication:

- decryption of said second private key (SK2),
- forming a digital signature on the basis of said device identity (DID) to verify the authenticity of the device identity, in which said second private key (SK2) is used, and
- verifying said digital signature with said public key (PK) to identify the electronic device (1).

7. A system for processing information in an electronic device (1) which comprises at least one processing block (2) for controlling the operation of an electronic device (1) and memory (2d, 2e, 2f, 3a, 3b, 3c, 202a, 202b, 203), and which system contains means for using at least a first private key (SK1) for processing information, **characterized** in that at least a protected mode and a normal mode are established in the processing block (2a), that the processing block (2a) comprises means (204, 208) for accessing part of the memory (202a, 202b) only in said protected mode, and that information of at least said first private key (SK1) is stored in the memory (202a, 202b) that is acessible in said protected mode.

8. The system according to claim 7, **characterized** in that the processing block (2a) comprises means (204, 208) for preventing the transfer of information from outside the processing block (2a) in said protected mode, wherein the determination of the internal function of the processing block (2a) is prevented in the protected mode.

9. The system according to claim 7 or 8, **characterized** in that at least one second private key (SK2) is established in the electronic device (1), said second private key being encrypted with said first private key (SK1) and stored in encrypted format in the memory (2d, 2e, 2f, 3a, 3b, 3c) that is acessible in the unprotected mode of the electronic device,

wherein the system comprises means (201) for decrypting said second private key (SK2) with said first private key (SK1).

10. The system according to claim 8 or 9, **characterized** in that the electronic device (1) comprises means (9) for receiving encrypted information, means (201) for decrypting said second private key (SK2) with said first private key (SK1), and means (201) for decrypting the encrypted information with said second decrypted private key (SK2).

11. The system according to any of the claims 7 to 10, **characterized** in that it comprises means (201, 204, 208) for setting the processing block (2a) in said protected mode when said first key (SK1) is used.

12. The system according to any of the claims 7 to 11, **characterized** in that it comprises means (BSS, MSC, HLR) for authenticating an electronic device (1), which electronic device (1) contains the at least one device identity (DID) stored therein and at least one second private key (SK2) which are encrypted with said first private key (SK1) that entails at least one public key (PK), wherein the system comprises means (201) for decrypting said device identity (DID) and said second private key (SK2), means (201, SK2) for forming a digital signature on the basis of said device identity (DID) to verify the authenticity of the device identity (DID) by using said second private key (SK2), and means (MSC, HLR, DID) for verifying said digital signature with said public key (PK) to authenticate the electronic device (1).

13. An electronic device (1) that comprises means for processing information, at least one processing block (2) for controlling the operation of an electronic device (1) and a memory (2d, 2e, 2f, 3a, 3b, 3c, 202a, 202b, 203), and means (2a) for using at least a first private key (SK1) for processing information, **characterized** in that at least a protected mode and a normal mode are established in the processing block (2a), that the processing block (2a) comprises means (204, 208) for accessing part of the memory (202a, 202b) only in said protected mode, and that information of at least said first private key (SK1) is stored in the memory (202a, 202b) that is accessible in said protected mode.

14. The electronic device according to claim 13, **characterized** in that at least a part of the memory (202a, 202b) used in said protected mode is a one time programmable read-only memory (202b).

15. A processing block (2a) that comprises at least one processor (201), memory (2d, 2e, 2f, 3a, 3b, 3c, 202, 203), and means (201, 202a, 202b, 203) for using at least a first private key (SK1) for processing information, **characterized** in that at least a protected mode and normal mode are established in the processing block (2a), that the processing block (2a) comprises means (204, 208) for accessing part of the memory (202a, 202b) only in said protected mode, and that information at least on said first private key (SK1) is stored in the memory (202a, 202b) that is accessible in said protected mode.

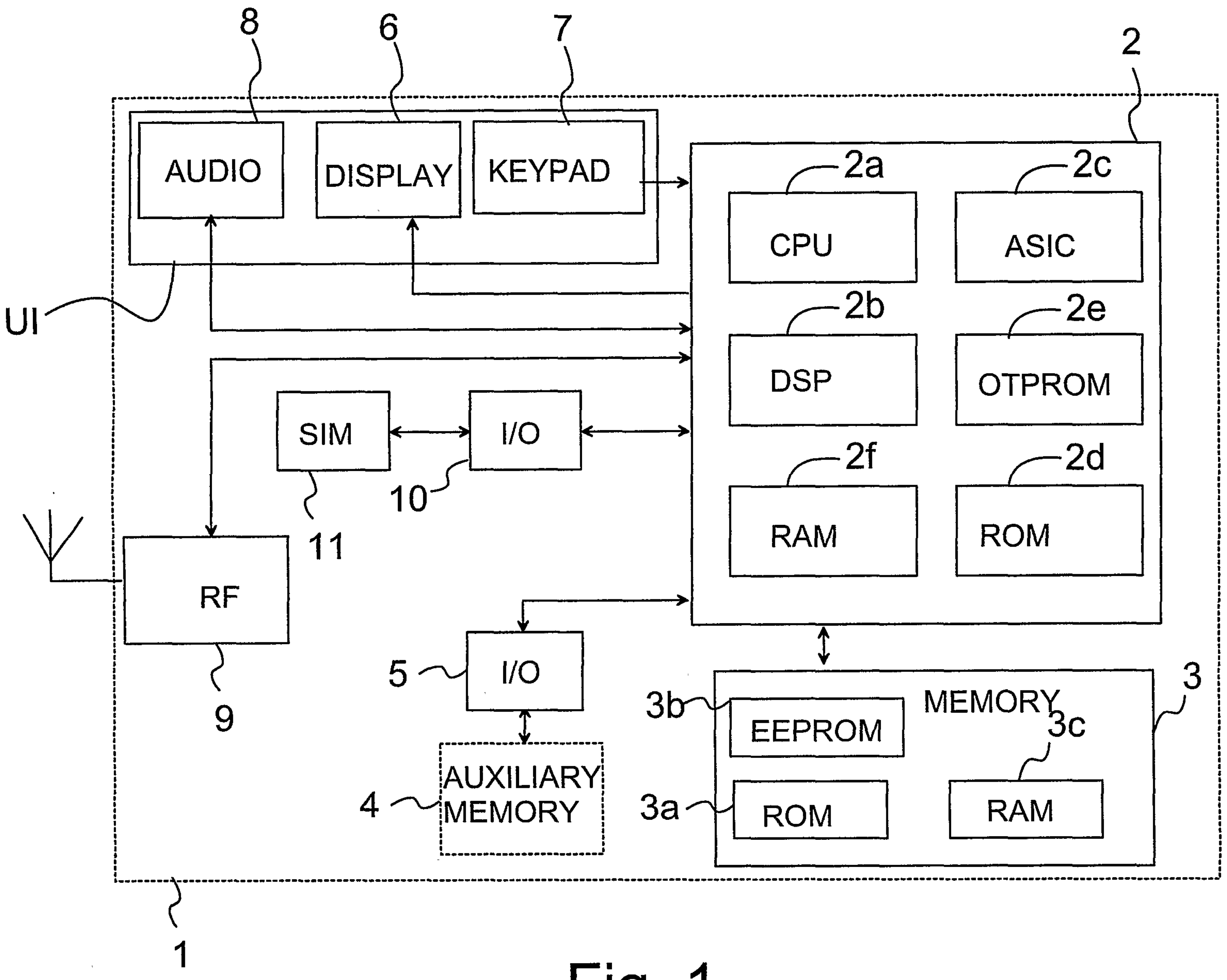

8
6
7
2
AUDIO
DISPLAY
KEYPAD
2a
2c
CPU
ASIC
UI
2b
2e
DSP
OTPROM
SIM
I/O
10
11
2f
2d
RAM
ROM
RF
9
5
I/O
3b
EEPROM
MEMORY
3c
3
4
AUXILIARY MEMORY
3a
ROM
RAM
1

Fig. 1

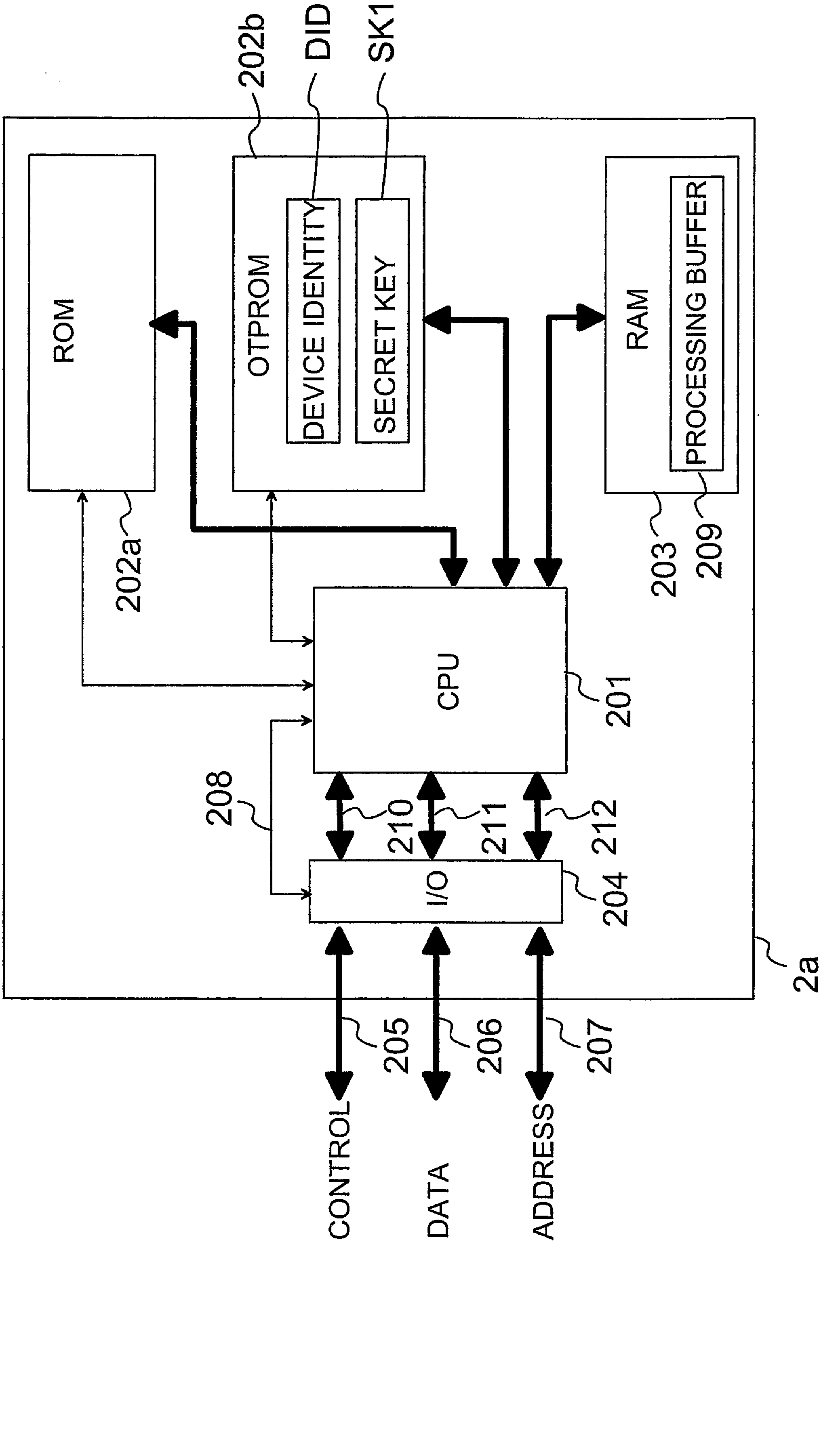

ROM
202a
OTPROM
202b
DEVICE IDENTITY
DID
SECRET KEY
SK1
RAM
PROCESSING BUFFER
203
209
CPU
201
I/O
204
208
210
211
212
205
206
207
CONTROL
DATA
ADDRESS
2a

Fig. 2

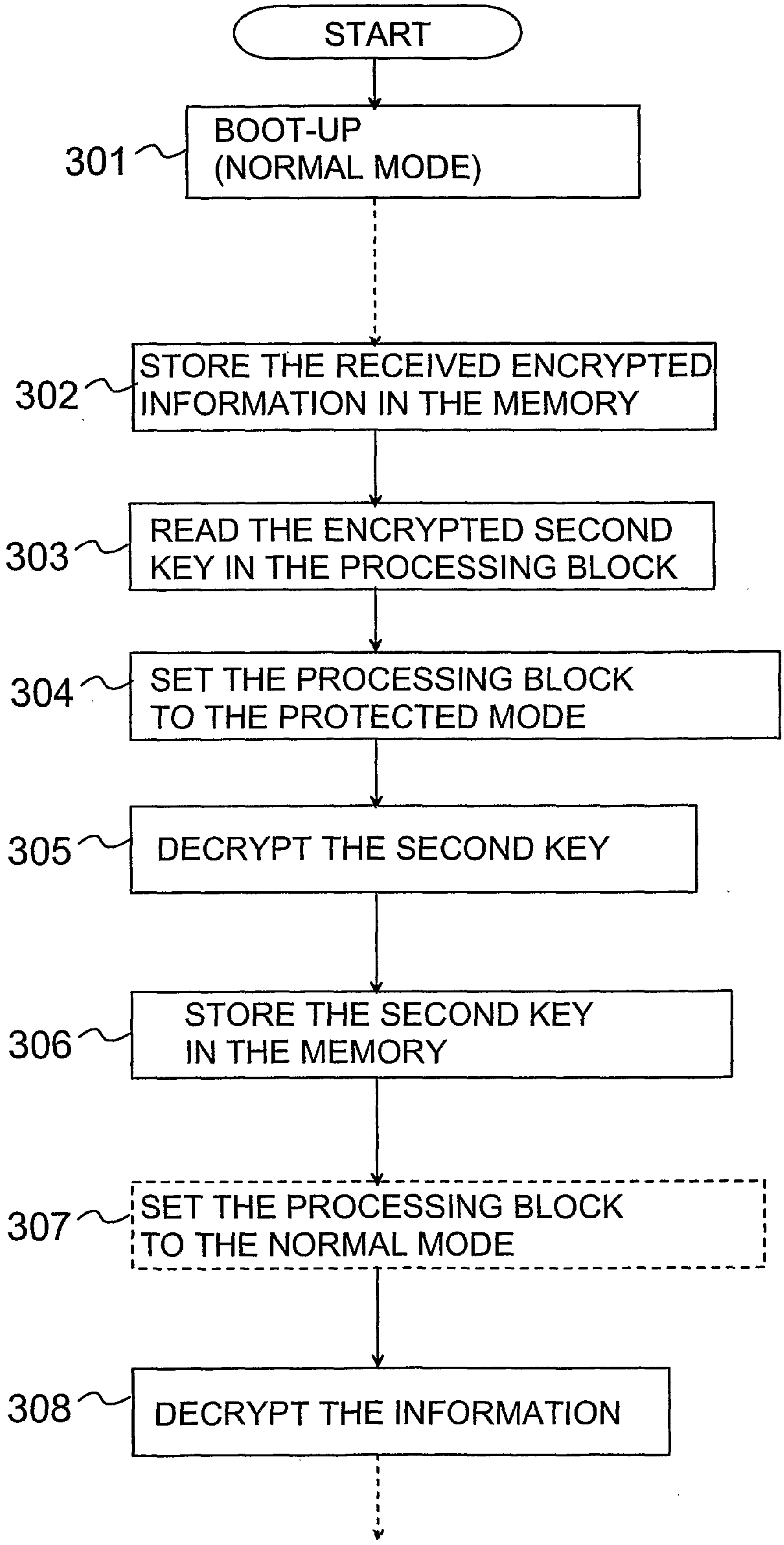

START
301
BOOT-UP (NORMAL MODE)
302
STORE THE RECEIVED ENCRYPTED INFORMATION IN THE MEMORY
303
READ THE ENCRYPTED SECOND KEY IN THE PROCESSING BLOCK
304
SET THE PROCESSING BLOCK TO THE PROTECTED MODE
305
DECRYPT THE SECOND KEY
306
STORE THE SECOND KEY IN THE MEMORY
307
SET THE PROCESSING BLOCK TO THE NORMAL MODE
308
DECRYPT THE INFORMATION

Fig. 3

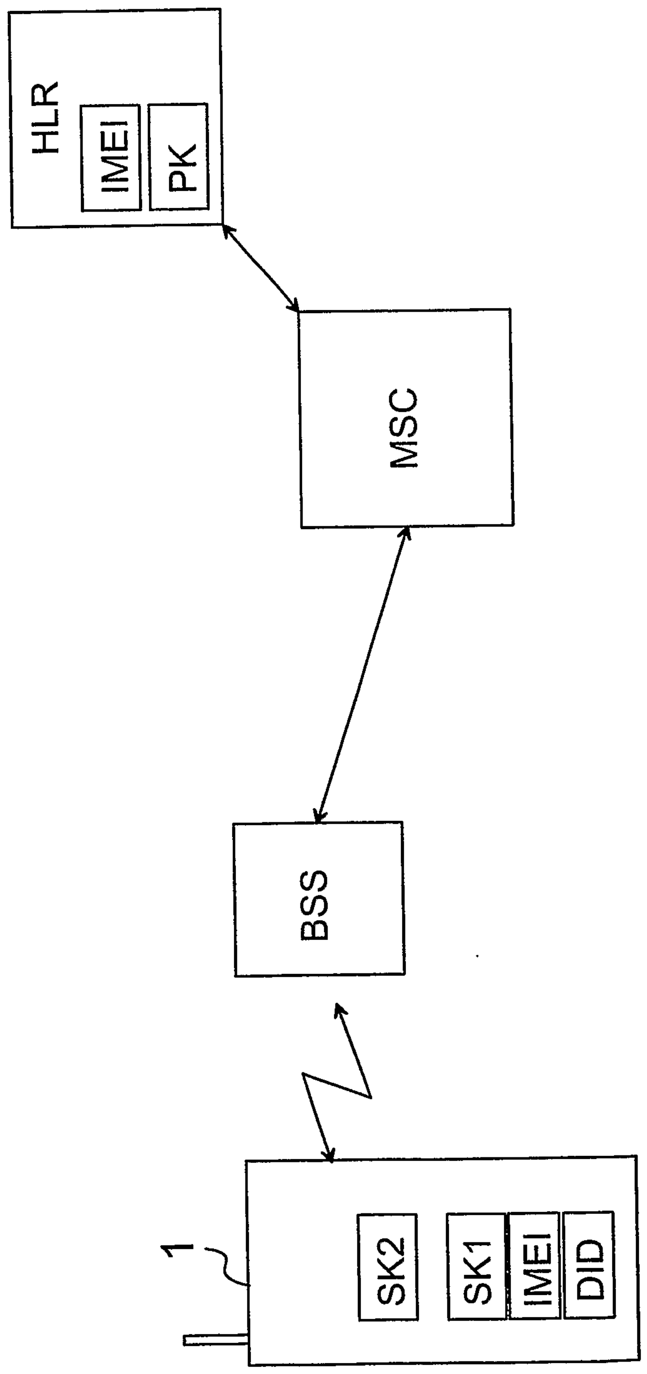


Fig. 4

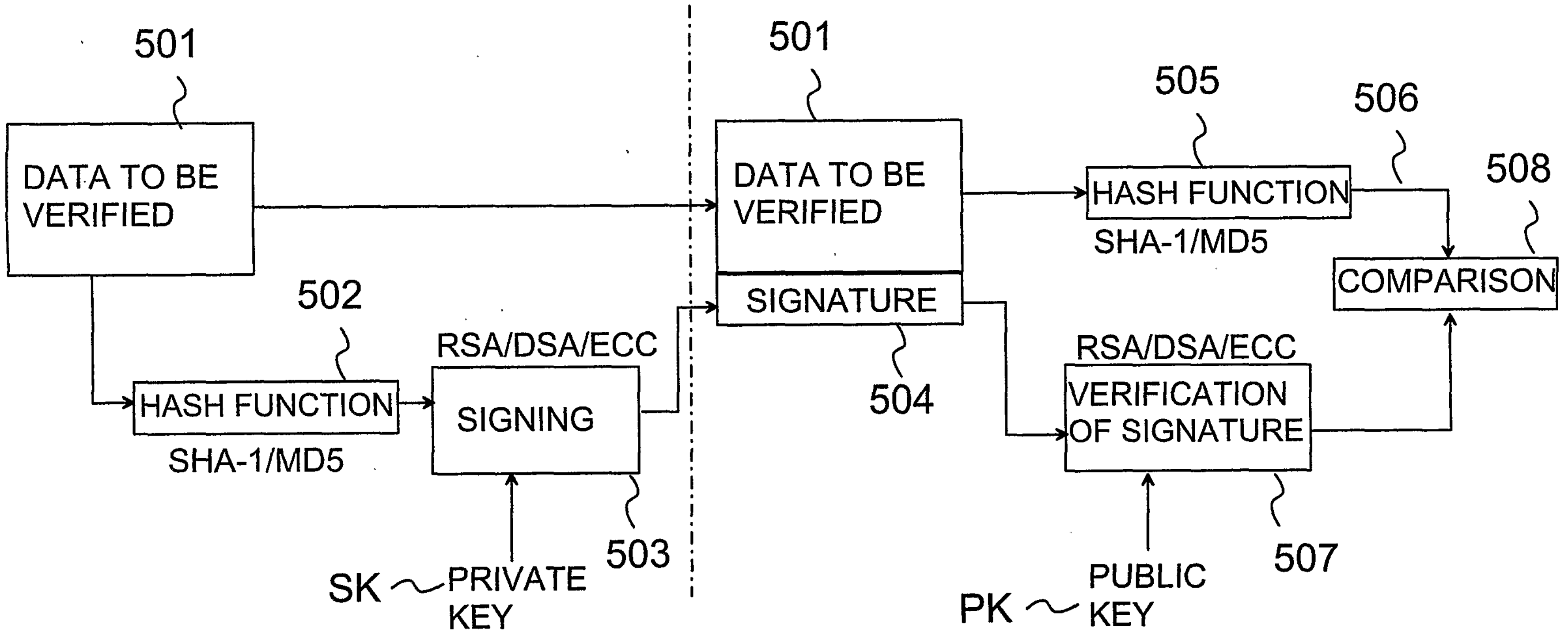

501
DATA TO BE VERIFIED
502
HASH FUNCTION
SHA-1/MD5
RSA/DSA/ECC
SIGNING
503
SK
PRIVATE KEY
501
DATA TO BE VERIFIED
SIGNATURE
504
505
HASH FUNCTION
SHA-1/MD5
506
508
COMPARISON
RSA/DSA/ECC
VERIFICATION OF SIGNATURE
507
PK
PUBLIC KEY

Fig. 5

INTERNATIONAL SEARCH REPORT

Inte ıal application No.
PCT/FI 02/00642

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 9/00

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L, G06F

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

SE,DK,FI,NO classes as above

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

EPO-INTERNAL, WPI DATA

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5224166 A (HARTMAN, JR., R.C.), 29 June 1993 (29.06.93), figure 2, abstract	1,7,13,15
A		2-6,8-12,14
	--	
X	WO 0017731 A1 (MCBRIDE, R.C.), 30 March 2000 (30.03.00), figure 2, abstract	1,7,13,15
A		2-6,8-12,14
	--	
A	US 5675645 A (SCHWARTZ, E.L.), 7 October 1997 (07.10.97), the whole document	1-15
	--	

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

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 28 October 2002	Date of mailing of the international search report 06-11-2002
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson /OGU Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

Int______nal application No.
PCT/FI 02/00642

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6169890 B1 (VATANEN, H.T.), 2 January 2001 (02.01.01), cited in the application	1-15

--

INTERNATIONAL SEARCH REPORT

Information on patent family members

30/09/02

International application No.
PCT/FI 02/00642

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5224166 A	29/06/93	DE 69327206 D,T	08/06/00
		EP 0583140 A,B	16/02/94
		JP 2085066 C	23/08/96
		JP 6112937 A	22/04/94
		JP 7107989 B	15/11/95
WO 0017731 A1	30/03/00	AU 1197300 A	10/04/00
		US 6292899 B	18/09/01
US 5675645 A	07/10/97	CA 2174299 A	19/10/96
US 6169890 B1	02/01/01	AT 159602 T	15/11/97
		DE 69314804 D,T	12/02/98
		EP 0669031 A,B	30/08/95
		SE 0669031 T3	
		ES 2107689 T	01/12/97
		FI 925135 A	12/05/94
		FI 934995 A	12/05/94
		GR 3025393 T	27/02/98
		NO 309346 B	15/01/01
		NO 951814 A	09/05/95
		RU 2116008 C	20/07/98
		WO 9411849 A	26/05/94