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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 March 2011 (10.03.2011)

PCT

(10) International Publication Number
WO 2011/027191 A1

(51) International Patent Classification:
G06F 21/00 (2006.01) *G06F 21/24* (2006.01)

(21) International Application Number:
PCT/IB2009/006827

(22) International Filing Date:
2 September 2009 (02.09.2009)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **TELENOR ASA** [NO/NO]; Snaroyveien 30, N-1331 Fornebu (NO).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SALLHAMMAR, Karin** [—/NO]; Ordforer J Nerviks Veg 3A, N-7540 Klaebu (NO). **ENGELHARDTSEN, Fritjof** [NO/NO]; Ringveien 16B, N-1386 Asker (NO). **HASLUM, Kjetil** [NO/NO]; Lokes Veg 30, N-7033 Trondheim (NO). **VIKEN, Brynjar** [NO/NO]; Innherredsveien 45B, N-7500 Stjordal (NO).

(74) Agents: **RENTSCH & PARTNER** et al.; Fraumünsterstrasse 9, Postfach 2441, CH-8022 Zurich (CH).

(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, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, 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, PE, 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, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

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

(54) **Title**: A METHOD, SYSTEM, AND COMPUTER READABLE MEDIUM FOR CONTROLLING ACCESS TO A MEMORY IN A MEMORY DEVICE

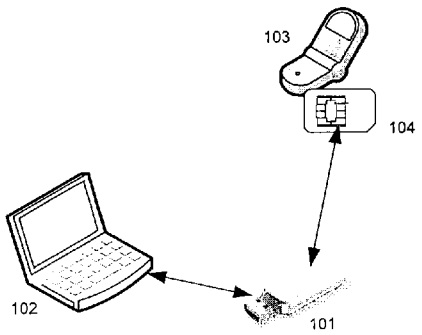

FIG. 1

(57) **Abstract**: A secure memory system is provided and includes a secure memory device and a secure element. The secure memory device includes a first memory, a secure memory that stores protected data, an access key request unit that requests an access key from a secure element external to the secure memory device using configuration information stored in the first memory, the configuration information configuring the request for the access key, an access key reception unit that receives an access key from the secure element in response to a condition defined in a security policy being fulfilled and that temporarily stores the received access key in a temporary memory, and an access controller that provides the requested access to the secure memory based on the received access key. The secure element includes a memory storing the access key, a reception interface that receives a request for the access key from the secure memory device, a determination unit that determines whether the condition defined in the security policy is fulfilled, and a providing unit that provides the access key to the secure memory device in response to the result of the determining by the determination unit.

WO 2011/027191 A1

TITLE OF INVENTION

A METHOD, SYSTEM, AND COMPUTER READABLE MEDIUM FOR CONTROLLING ACCESS TO A MEMORY IN A MEMORY DEVICE

BACKGROUND OF THE INVENTION

Field of Invention

[0001] The present invention relates to a method for controlling access to protected data. More specifically, the invention relates to a method in a memory device for controlling access to protected data stored in said memory device. The memory device may be configured to request and receive an access key from a secure element such as a smart card and provide access to the protected data using the received access key.

Description of Related Art

[0002] Removable memory devices such as for example USB flash drives and other types of removable memory such as Secure Digital, Memory Stick and COMPACTFLASH, are often used to store electronic documents, to transfer documents between a work computer and a home computer, to carry documents when traveling etc. This represents a security risk for private users as well as businesses. In particular, company confidential documents are often stored on devices that can easily be misplaced, lost or stolen.

[0003] A common way of protecting the content of such a device is therefore to encrypt the content of the device. However, the security of an encrypted memory device is often limited by the quality of the password that the user has chosen. Passwords with few characters and passwords based on common words are vulnerable to brute force and dictionary attacks. Passwords are therefore often combined with keyfiles. A keyfile will typically be a decryption key that allows decryption of protected data stored on the memory device. A keyfile is often part of a public key infrastructure (PKI). Such a keyfile must be securely stored, separate from

the memory device, and secure access to and distribution of keys may represent a challenge.

[0004] In organizations, removable memory devices may also represent a security risk due to their small size and ease of use. Unsupervised visitors and unfaithful employees can easily carry confidential information away from the organizations premises with minimal risk of detection. This problem has led organizations to simply not allow the use of removable memory devices, which of course also removes the advantage of their convenience for legitimate use.

[0005] There is consequently a need for solutions that improve the security of removable memory devices, while retaining the advantages and flexibility of use offered by these devices.

SUMMARY OF THE INVENTION

[0006] The present invention provides a method for controlling access to a memory in a secure memory device utilizing a central processing unit. The method includes receiving a first request for access to the memory, sending a second request for an access key to an external secure element, the access key availability based on a fulfillment of a condition defined in a security policy, receiving the access key, and providing the requested access to the memory based on the access key.

[0007] In a further aspect of the invention there is provided a secure memory device which includes a secure memory that stores protected data. Further, the secure memory device includes a first memory that holds and provides configuration information necessary for configuring a request for an access key that is sent to a secure element in response to a request for access to the secure memory and includes a temporary memory that receives and temporarily stores a received access key from the secure element in response to a condition defined in a security policy being fulfilled. Also included in the secure memory is an access controller that provides the requested access to the secure memory based on the received access key.

[0008] In a further aspect of the invention there is provided a secure memory device which includes a first memory, a secure memory that stores protected data,

an access key request unit that requests an access key from a secure element external to the secure memory device using configuration information stored in the first memory, the configuration information configuring the request for the access key, an access key reception unit that receives an access key from the secure element in response to a condition defined in a security policy being fulfilled and that temporarily stores the received access key in a temporary memory, and an access controller that provides the requested access to the secure memory based on the received access key.

[0009] In a further aspect of the invention there is provided a computer readable medium having stored thereon a program that when executed by a secure memory device performs a method of controlling access to a memory in the secure memory device. The method includes receiving a first request for access to the memory, sending a second request for an access key to an external secure element, the access key availability determined based on a fulfillment of a condition defined in a security policy, receiving the access key, and providing the requested access to the memory based on said access key.

[0010] In a further aspect of the invention there is provided a method for providing an access key from a secure element operable in a mobile device and executed using a central processing unit. The method includes receiving a request for an access key from an external secure memory device having a memory that stores protected data, determining whether a condition defined in a security policy is fulfilled, and providing the access key to the secure memory device in response to the result of the determining.

[0011] In a further aspect of the invention there is provided a secure element operable in a mobile device. The secure element includes a memory storing an access key, a reception unit that receives a request for the access key from an external secure memory device having a memory that stores protected data, a determination unit that determines whether a condition defined in a security policy is fulfilled, and a key providing unit that provides the access key to the secure memory device in response to the result of the determining by the determination unit.

[0012] In a further aspect of the invention there is provided a computer readable medium having stored thereon a program that when executed by a secure element performs a method of providing an access key from the secure element. The method includes receiving a request for an access key from an external secure memory device having a memory that stores protected data, determining whether a condition defined in a security policy is fulfilled, and providing the access key to the secure memory device in response to the result of the determining.

[0013] In a further aspect of the invention there is provided a mobile device. The mobile device includes a secure element having an access key, a first communication interface that receives a request for the access key from an external secure memory device having a memory that stores protected data, a determination unit that determines whether a condition defined in a security policy is fulfilled, and a providing unit that provides the access key to the secure memory device via the first communication interface in response to the result of the determining by the determination unit.

[0014] In a further aspect of the invention there is provided a policy server. The policy server includes a computer readable memory that stores a security policy, a central processing unit, and a transmission unit that provides an external secure element with an authentication requirement corresponding to the security policy requiring that a condition be satisfied before an access key is provided to a secure memory device from the external secure element.

[0015] In a further aspect of the invention there is provided a policy server. The policy server includes a computer readable memory that stores a security policy, a central processing unit, a policy transmission unit that provides an external secure element with the security policy requiring that a condition be satisfied in order that an access key can be provided to a secure memory device from the external secure element, and a condition approval unit that receives a request for approval from the external secure element generated based on the security policy and including condition information, that determines whether the condition is satisfied based on the condition information, and that transmits an approval response based on the determination.

[0016] In a further aspect of the invention there is provided a policy server. The policy server includes a computer readable memory, a central processing unit, a credential request reception unit that receives an access key request from a secure device having a memory that stores protected data, the credential request including a unique identification of a secure element, a condition information reception unit that sends a request to the secure element identified based on the unique identification for condition information and that receives the condition information from the secure element in response to the request, a determination unit that determines whether a condition is satisfied based on the condition information, and a credential providing unit that provides the secure device having the memory with the access key in response to a result of the determination unit.

[0017] Finally, in a further aspect of the invention there is provided a secure memory system. The system includes a secure memory device and a secure element. The secure memory device includes a first memory, a secure memory that stores protected data, an access key request unit that requests an access key from a secure element external to the secure memory device using configuration information stored in the first memory, the configuration information configuring the request for the access key, an access key reception unit that receives an access key from the secure element in response to a condition defined in a security policy being fulfilled and that temporarily stores the received access key in a temporary memory, and an access controller that provides the requested access to the secure memory based on the received access key. The secure element includes a memory storing the access key, a reception interface that receives a request for the access key from the secure memory device, a determination unit that determines whether the condition defined in the security policy is fulfilled, and a providing unit that provides the access key to the secure memory device in response to the result of the determining by the determination unit.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] A more complete appreciation of the invention and many of the attendant advantages thereof will be readily obtained as the same becomes better

understood by reference to the following detailed description when considered in connection with the accompanying drawings, wherein:

[0019] Figure 1 illustrates a first configuration of devices that can be utilized in an embodiment of the invention;

[0020] Figure 2 illustrates a second configuration of devices that can be utilized in an embodiment of the invention;

[0021] Figure 3 illustrates in a flow chart how the process of providing access to protected data in a memory can proceed;

[0022] Figure 4A – 4D are sequence diagrams showing how a memory device can cooperate with a secure element in accordance with embodiments of the invention;

[0023] Figure 5 illustrates a secure memory device consistent with the principles of the invention; and

[0024] Figure 6 illustrates a secure element consistent with the principles of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0025] The invention will now be described in further detail with reference to the embodiments and aspects which are illustrated in the accompanying drawings. While the following detailed description sets forth numerous specific details and exemplary embodiments in order to provide a thorough understanding of the present invention, it will be apparent to one of ordinary skill in the art that the present invention may be practiced without these specific details. In other instances, well-known methods, procedures, components, circuits, and networks have not been described in detail so as not to unnecessarily obscure aspects of the embodiments.

[0026] It will also be understood that, although the terms first, second, etc. may be used herein to describe various elements, actions or features, these terms should not be construed in a limiting manner. The terms are only used to distinguish one element from another. For example, a first request could be referred to as a

second request, and a second request could be referred to as a first request, without departing from the scope of the present invention. As such, except where it is clear from the context that a certain action depends on or is initiated by another action, the use of terms such as first and second does not imply that the action referred to as a first action has to be performed prior to a second action.

[0027] Reference is first made to FIG. 1, which illustrates a first configuration of devices that can be utilized in an embodiment of the invention. The illustration shows removable memory device 101 which can be connected to a portable computer, such as laptop computer 102. Also shown is a mobile telephone, or cellular phone, 103. According to the example illustrated in this drawing the mobile phone 103 is equipped with a Subscriber Identity Module (SIM) 104. The drawing also shows that in addition to the communication capability between memory device 101 and computer 102, the memory device is also capable of communicating with the SIM card 104. The communication link between the memory device 101 and the computer 102 can for example be physical, such as a Universal System Bus (USB), or it may be wireless, for example infrared or BLUETOOTH. The communication link between the removable memory device 101 and the SIM card may be a direct wireless connection, or it may utilize the communication capabilities of at least one of the computer 102 and the mobile phone 103. The communication link between the memory device 101 and the SIM card 104 will be discussed in further detail below.

[0028] When the removable memory 101 is connected to the computer 102, it becomes possible to request access to the memory from the computer. Those with ordinary skill in the art will realize that establishing a connection between the two devices and issuing commands or requests and responses between them may involve for example certain operations on the operating system and file system level. For example, the memory device file system may be mounted in the file structure of the computer 102, also known as mapping the device as a drive, or communication may otherwise be established and possibly authorized, for example through a handshake procedure. These procedures are well known to those with ordinary skill in the art, and will not be discussed in great detail here.

[0029] The memory device 101 may now receive a request for access to data stored in its memory from the computer 102. In accordance with aspects of the

invention the memory of the memory device may be protected such that only authorized requests will be given such access. Alternatively, the entire memory is not protected. Instead only certain areas, portions or partitions of the memory may be associated with a particular user and thus access to these parts of the memory may require certain credentials. Yet another possibility, which is consistent with the principles of the invention, is the alternative where the data itself is protected. For example one or more files or the entire file system of the memory device 101 may be encoded with an algorithm capable of obscuring data, for example an encryption or compression algorithm.

[0030] In some embodiments of the invention the data may be protected with several measures at the same time. For example, the memory device may only allow access to an authorized user, while in addition the file system or individual data items such as files can be encrypted, or a first credential may provide access to the memory device, while a second credential may provide access to the file system or individual data items.

[0031] Consistent with the principles of the invention, the memory device may now proceed to request some form of credentials confirming that the request for access to the memory should be authorized. This request may be sent to the SIM card 104. It should, however, be noted that this request for credentials may actually precede the request for access to the memory. For example, when the device is first connected to or mounted on the computer 102, a request for a credential may be sent from the memory device to the SIM card 104 before any request is actually received from the computer 102, and whether or not a request from the computer 102 will result in access to the memory being granted may depend on the successful receipt of a valid credential, for example a decryption key, before the request for access from the computer 102 is actually received.

[0032] According to aspects of the invention, whether or not the SIM card 104 responds by returning a valid credential to the memory device 101 may depend on one or more conditions being fulfilled. Such conditions will be discussed in further detail below, but a first example of a condition could be that a user will have to enter a correct code using the user interface of the mobile phone 103.

[0033] If it can be determined that the credential received from the SIM card 104 properly confirms that the request for access should be granted, the computer 102 will now be able to receive the requested data from the memory device.

[0034] Attention is now directed towards FIG. 2 which illustrates an embodiment wherein a memory device 201 is directly connected to a laptop computer 202 and communicates with a secure element in the form of a SIM card 204 over a wireless connection. The secure element is inserted or embedded in a mobile telephone 203. In accordance with this exemplary embodiment, the memory device 201 as well as the secure element 204 are configured with wireless communication capabilities such as for example wireless LAN, also known as WI-FI or IEEE 802.11, BLUETOOTH or ZIGBEE. In an alternative embodiment the secure element 204 could utilize wireless communication capabilities in the mobile telephone 203. In yet another embodiment the secure element 204 and the memory device 201 could communicate over a wired connection, for example by connecting the mobile telephone 203 to the laptop computer 202 with a cable. Other alternatives that are within the scope of the invention include communication utilizing network communication capabilities of the laptop computer 202 and the mobile telephone 203, for example as a combination of one or more of a wired or wireless LAN, the Internet and a cellular telephone network.

[0035] The example in FIG. 2 also includes a first server 205 and a second server 206. The laptop computer 202, the mobile telephone 203 and the servers 205, 206 are shown as connected to a network 210. The network 210 may be a combination of one or more communications networks as mentioned above.

[0036] The first server 205 can be configured to communicate with the secure element 204 in order to impose rules or conditions that must be met in order for the secure element 204 to respond to a memory device 201 by transferring a credential to the memory device. Examples of such rules or conditions could be one or more of a PIN code that must be entered correctly by a user of the mobile telephone 203, a determined location of the secure element 204, a determined location of the memory device 201, or a determined time. The first server 205 will be referred to as an access server, but can also be thought of as a security policy server or a trusted entity.

[0037] A requirement of a correct entry of a PIN code can also be implemented permanently, for example by storing the PIN code securely on the secure element 204 and always require correct entry of the PIN code prior to allowing any access to the credential stored in the secure element 204. This approach is well known to those with ordinary skill in the art, and is for example used to prevent unauthorized use of a stolen SIM card to connect a mobile telephone to a cellular network and thereby using a subscription owned by somebody else. In some embodiments of the invention, such a requirement stored permanently in the secure element 204 can be combined with requirements that are uploaded to the secure element 204 from the access server 205.

[0038] In some embodiments of the invention a condition, or security policy rule, uploaded to the secure element 204 from the access server 205 is a requirement that the secure element 204 is in an approved location when the credential is requested from it. A location can for example be defined as one or more coordinates and be representative of one or several areas, for example a work place or a user's home. The coordinates sent to the secure element 204 from the access server 205 can in some embodiments also be revoked or updated from the access server 205 by a second transmission which overwrites or cancels the first coordinates, or they can be associated with an expiry time.

[0039] The secure element 204 may be configured to receive and store the received coordinates. Upon receipt of a request for a credential from the memory device 201, the secure element may request and receive coordinates representative of its current location and compare current location with the stored coordinates in order to determine if it is located in an approved area. If the comparison results in a positive determination, the credential may be transferred to the memory device 201.

[0040] In some embodiments of the invention, the coordinates representative of the position of the secure element may be received from a GPS system embedded on the secure element itself. Such a system has for example been presented by BlueSky Positioning Ltd. Alternatively, the secure element may be configured to communicate with a GPS system included in the mobile telephone 203. In yet another embodiment, the location of the secure element can be determined based on capabilities of the cellular network over which the mobile telephone 203 is

communicating. Such services are being provided by network operators, and the functionalities may be handled from a positioning server or location server. The second server 206 shown in FIG. 2 illustrates such a location server.

[0041] Positioning services in networks are well known in the art and can for example be based on radio signal delay of the cell phone towers closest to the mobile telephone. More advanced methods may include measurement of signal phase or angle. Positioning may also simply be based on an identification of a cell phone tower or an operator of a mobile telephone network to which the cell phone is connected, or the Basic Service Set Identifier (BSSID) or Service Set Identifier (SSID) of a wireless access point which is in range of the secure element or the device hosting the secure element. WLAN positioning based on BSSID or SSID may, however, be less secure and possibly vulnerable to spoofing, where an intruder for example sets up a wireless access point to misrepresent a location.

[0042] An additional or alternative requirement that may be implemented in systems consistent with the principles of the invention is to impose requirements on the location of the memory device. The location of the memory device may not be directly available based on network positioning in the cellular network, but in some embodiments the memory device 201 may include an embedded GPS system. Alternatively, or in addition, it may be required that the memory device is able to communicate with a short range or relatively short range wireless communication system such as wireless LAN, BLUETOOTH, ZIGBEE, proximity card, radio frequency identification (RFID) or Near Field Communication (NFC, an extension of ISO 14443), all of which are well known to those with ordinary skill in the art. In embodiments where this requirement is implemented, the location of the memory device 201 may be transmitted to the secure element 204 together with the request for a credential, or as part of a handshake procedure between the memory device 201 and the secure element 204. Yet another alternative consistent with the principles of the invention is to base the position of the memory device on a positioning capability of the host device 202.

[0043] Yet another additional or alternative requirement that may be transmitted from the access server 205 to the secure element 204 is a limitation on when the credential can be delivered to the memory device 201. In a first

embodiment implementing this alternative, the credential is associated with an expiry time. According to this embodiment any request from the memory device after the expiry time has passed will be denied. An additional security measure that can be included in this embodiment is that the credential is automatically deleted from the secure element 204 after the credential expires.

[0044] In a second embodiment implementing this alternative, the limitation on when the credential can be delivered to the memory device 201 can be certain periods of time, for example certain hours of the day, days of the week etc. This limitation can serve to protect a memory device from unauthorized access during periods of time when a user can be assumed not to be working and the memory device 201 or the device holding the secure element 204, such as for example mobile telephone 203, may be unattended.

[0045] Communication between the memory device 201 and the secure element 204 is in the embodiment illustrated in FIG. 2 shown as a direct wireless link. In an aspect of this embodiment the wireless link is between similar communications capabilities in the memory device 201 and the secure element 204. The communications capability can for example be in the form of embedded transceivers using a well known protocol such as for example BLUETOOTH, WI-FI (IEEE 802.11) or ZIGBEE, proximity card, RFID or NFC (or ISO 14443). The secure element can alternatively use a communication capability of a device in which it is included, such as mobile telephone 203.

[0046] FIG. 3 illustrates in a flow chart how the process of providing access to protected data in a memory device can proceed. The process starts in an initial step 300. In a next step 301 the memory device, for example a USB memory stick 201, is connected to the host device, which may be a laptop computer 202. In a next step 302 the memory device is detected by the host device and a procedure for mounting or mapping the memory device in the file system of the host device is performed.

[0047] The process then moves on to step 303, where a request for access to data stored in the memory of the memory device is received from the host device. The memory device must then determine whether the requested data is protected. According to some embodiments of the invention, all data stored in the memory

device is protected, and the step of determining this may be unnecessary. In other embodiments some data can be protected while other data is freely accessible, and a determination must be made. Whether data is protected may be determined for example by whether the data is stored in a protected area of the memory or not, whether the data is encrypted or not, or whether the data is designated as protected for example by being associated with a particular user. If it is determined in step 304 that the requested data is not protected, the process may proceed to step 308. If, however, it is determined that the data is protected the process proceeds to step 305 where an appropriate credential is requested from the secure element.

[0048] The secure element may be a SIM card 204 installed in a mobile telephone 203, as illustrated in FIG. 2, but other alternatives are possible within the scope of the invention, for example a Universal Integrated Circuit Card (UICC) or some other form of smart card. Various methods of addressing the secure element are possible in different embodiments of the invention, as will be discussed in further detail below.

[0049] The processing of the request in the secure element will be described with reference to FIG. 4. In the memory device the process moves on to step 306 where it is determined whether the correct credential is received. A determination that a correct credential is not received may be a consequence of one or more of the following. One alternative may be that a valid credential must be received within a predefined period of time. If no credential is received within this period of time, either because of failure to connect to the secure element or because no valid response is received from the secure element, the determination in step 306 may be negative. A second alternative may be that a credential is received, but it fails to properly correspond with a user identified in the request received from the host device. A third alternative may be that a credential is received, but it fails to correspond with the memory device or a particular area of memory in the memory device. Yet another alternative is that a credential is received, but it fails to decrypt or otherwise provide access to the data requested in the request received from the host device. Embodiments of the invention may implement any combination of these and other requirements in order to determine whether the received credential is valid. The

credential may also be associated with an expiry time, in which case an expired credential may result in a negative determination in step 306.

[0050] If the determination in step 306 is negative, i.e. that no credential or an invalid credential is received, the process proceeds to step 309 where access to the requested data is refused. In some embodiments of the invention this may be done by responding to the initial request with an error message describing the failure. However, it is consistent with the principles of the invention to let the memory device remain passive and not respond to a failed request. After access has been refused, the process terminates in step 310.

[0051] If the determination in step 306 is positive, i.e. that a valid credential is properly received, the credential may be used to access the protected data in step 307. The process of accessing the data may involve decrypting the data if the data is encrypted and the received credential is a decryption key.

[0052] The process may then move on to step 308 where the requested data is sent to the host device in response to the initial request. The process then terminates in step 310.

[0053] After access has been provided in accordance with the process described with reference to FIG. 3, subsequent requests may automatically be granted based on the credential received during processing of the first request. However, it is consistent with the principles of the invention to require a new credential every time a request is received, or if a predefined period of time has passed since the receipt of the first credential.

[0054] As mentioned above, in an alternative embodiment of the invention the request for a credential from the secure element may be transmitted to the secure element as a result of the initial mounting of the device in step 302, i.e. before the request for access to data is received in step 303. According to this alternative, the credential may be used as part of the mounting process or immediately after the mounting process, and the step of receiving a request for any particular data stored on the memory device may be received after the credential has been requested and received from the secure element. In this embodiment, access to the protected data may automatically be granted in any subsequent request, i.e. the protected data has

been unlocked, or additional steps of for example decryption or access control may be performed when a request for any particular piece of data is received from the host device.

[0055] Turning now to FIG. 4, the process performed in the secure element when a request for a credential is received will be described. This process may typically be performed in the secure element between steps 305 and 306 in FIG. 3, i.e. initiated by the request for a credential in step 305 and completed when a correct credential is received (or denied) in step 306.

[0056] A number of embodiments are illustrated in FIG. 4, each being based on various conditions implemented as part of a security policy. In each illustrated embodiment the specified condition must be fulfilled in order for a credential to be sent as a response to the request. The embodiments are illustrated as sequence diagrams showing how the secure element may cooperate with the device in which it is inserted, as well as with one or more external servers. It should be noted that the examples illustrated in FIG. 4 do not include signals exchanged between the memory device and the host computer that concern the actual requested data stored on the memory device. Messages sent between the memory device and the secure element may, according to some embodiments, be relayed over a communications interface of the host computer. Simple message relaying is not included in the signal flow diagram of the drawings. Also, the various transmission media, addressing schemes and communications interfaces used will not be discussed with reference to FIG. 4. It should also be noted that all the examples in FIG. 4 assumes that the memory device and the secure element both include a minimum of processing capability and corresponding software. In other embodiments of the invention such capabilities may be borrowed from the host computer and the mobile phone, respectively.

[0057] FIG. 4A illustrates an example where the specified condition is that a user of the device 103, 203 holding the secure element 104, 204 must enter a PIN code. The secure element can for example be a SIM card 104, 204 inserted in a mobile telephone 103, 203, and the user can be prompted over the display of the mobile telephone 103, 203 to enter a correct PIN code using the user interface of the telephone 103, 203, for example a keyboard or touch screen.

[0058] According to the exemplary embodiment shown in FIG. 4A, the memory device 101 issues a request for a credential addressed to the secure element 104 for example a SIM card. When the request is received at the SIM card 104 a request for PIN code entry is issued by the secure element 104 to the device 103 hosting the secure element 104, which may e.g. be a mobile telephone 103, whereupon a prompt for PIN code entry may be displayed on a screen of the phone 103. The user may then enter the PIN code over a user interface of the mobile telephone 103, and the entered PIN code can be transferred to the secure element 104. In the secure element 104, the PIN code is verified before the requested credential is sent in response to the memory device 101. If the PIN code has been incorrectly entered, a refusal may instead be sent to the memory device 101. According to some embodiments the secure element 104 may issue several prompts for a correct PIN code entry before finally responding to the request for a credential by issuing a refusal.

[0059] In FIG. 4B a second embodiment is illustrated, wherein the specified condition is a password or passphrase distributed by a policy server 205. The password may in some embodiments be associated with an expiry time, after which it will no longer be valid.

[0060] In this embodiment, a password is first transmitted from a policy server 205 to the secure element 204 to be securely stored there. The password may be encrypted in order to prevent unauthorized access. Some time after the password has been received and stored, a request for a credential is received from a memory device 201. It should be noted that the password is not the credential. The credential, which may e.g. be a decryption key, is already securely stored in the secure element 204.

[0061] When the request for a credential has been received by the secure element 204, the secure element 204 may be configured to determine whether a valid password is present. This will be the case provided that a password has been received from the policy server 205 and that the password has not expired. After this has been determined, the secure element 204 issues a request for user input of the password to the mobile telephone 203 holding the secure element 204. The user can then be prompted to enter the password using the user interface of the mobile phone

205, whereupon the entered password is transferred from the telephone 203 to the secure element 204. In the secure element the user entered password will be compared with the password received from the policy server, and if a correct password has been entered, the requested credential can be sent in a response to the memory device 201. Otherwise, a refusal can be transmitted to the memory device 201, or the user may be prompted to enter the password again.

[0062] The example illustrated in FIG. 4C is one wherein a condition for responding with the requested credential is that the secure element is in a predetermined location, as determined by a positioning service. According to this example, the security policy is not distributed in its entirety by the policy server 205 to be stored in the secure element 204. Instead, the policy server 205 distributes a policy description defining which data should be transmitted to the policy server 205 in a request which the policy server 205 responds to by authorizing or denying the transmission of the credential to the requesting memory device 201. According to the illustrated example, the security policy includes instructions to transmit data representing the location of the secure element.

[0063] According to the example illustrated in FIG. 4C, the security policy described above is first transmitted from the policy server to the secure element 204, where it is stored. When a request for a credential is received from a memory device 201, the secure element 204 examines the received security policy and determines that it needs to report its location to the policy server 205. Several alternatives can be contemplated for providing the location of the secure element, including a GPS received embedded in the secure element and a GPS receiver located in the mobile phone 203. According to the embodiment illustrated in FIG. 4C, however, the location of the secure element is obtained from a location server 206. The location server 206 may use radio frequency (RF) positioning utilizing capabilities of the cellular network over which the mobile telephone 203 is communicating. Consequently, the secure element 204 issues a request for positioning to the mobile telephone 203. The mobile telephone 203 connects with the location server 206 over the mobile telephone network and requests its position from the server 206. The location server 206 processes the request, by obtaining necessary information from the cellular network and calculates an estimated position for the mobile telephone,

and thereby also for the secure element. This processing may involve communication with other elements of the cellular network not illustrated in the figures.

[0064] It should be noted that a request for positioning issued by the secure element 204 may be issued to the mobile telephone 203 as such, or only in the sense that the mobile telephone acts as a communication device but without any access to the content of the request, which may be addressed directly to the location server 206 using SMS, bearer independent protocol (BIP) or even a direct TCP/IP connection, depending on the capabilities of the secure element. Alternatively, the request may be issued to a service residing in software in the telephone 203. The former alternative may provide an end-to-end secure channel between the secure element 204 and the location server 206. The latter alternative may be less secure, but fewer capabilities may be required from the secure element 204 while the software on the telephone 203 may be configured to issue the request to the location server 206 and to interpret and forward any response received from the server 206 to the secure element 204. The signal flow illustrated in FIG. 4C is intended to cover both of these alternatives.

[0065] The calculated position is received by the mobile telephone 203 where it is forwarded to the secure element 204, either transparently or as part of a service running on the telephone, as described above. The secure element 204 will now be able to forward its position and any other information required by the security policy to the policy server 205 in a request for approval. The policy server receives the request for approval and may determine, based on the received information, whether approval should be given. If the policy server 205 determines that the reported position is consistent with policy requirements for this particular secure element 204, or for a user identified in the request for approval, and that any other requirements defined in the security policy are fulfilled, an approval is sent to the secure element 204. Otherwise, a message indicating that approval is denied may be sent from the policy server 205 to the secure element 204. Provided that approval is received, the secure element 204 can now respond by sending the requested credential to the memory device 201.

[0066] Consistent with principles of the invention, several alternatives to the embodiment illustrated in FIG. 4C are possible. For example, the calculated position may be reported directly from the location server 206 to the policy server 205. The reported position and the request for approval received from the secure element 204 can both be identified by a number uniquely identifying the secure element, for example by an IMSI number which is a subscriber identification number stored in SIM cards in mobile phones, or a TMSI number which is a temporary identity sent between a mobile terminal and a network. In another embodiment, the location or locations are pre-approved by the policy server 204 and part of the security policy transmitted from the policy server 205 to the secure element 204. The secure element 204 can then determine approval based on the position received from the location server 206 without involving the policy server 205.

[0067] In the exemplary embodiment illustrated in FIG. 4D, there is no direct communication between the memory device 201 and the secure element 204, and the security policy is implemented centrally in the policy server 205. The process is initiated when a memory device requests a credential in order to authorize access to protected data. However, according to this embodiment the request for the necessary credential is sent to the policy server 205. The policy server 205 proceeds by requesting necessary information from the secure element 204. According to a first embodiment the policy server already possesses the necessary credential, and the request sent to the secure element may be a request for a correct entry of a password or PIN code, the location of the secure element, or some other information required by the security policy stored in the policy server 205. According to a second embodiment, the necessary credential is stored in the secure element, and the request sent to the secure element is a request for the credential as well as any other information required by the security policy. In either case a request for data is sent to the secure element 204.

[0068] The secure element 204 responds by transmitting the requested data to the policy server, provided that the requested data is available and that any requirements held by the secure element 204 or the mobile phone 203 are fulfilled, such as the proper entry of a password or PIN code by a user of the mobile phone 203. Processing in the secure element 204 may also involve communication with the

mobile phone 203 and a localization server 206 in order to obtain the position of the secure element 204. This communication is not illustrated in FIG. 4D, but may correspond to that illustrated in FIG. 4C. If the requested data is not available, or if a requirement cannot be fulfilled, the secure element may respond with a refusal, or alternatively no response is sent at all.

[0069] When the policy server 205 receives a response from the secure element 204, the received data may be processed in order to verify that the response fulfills the requirements of the security policy. If this is found to be the case, the necessary credential can be sent from the policy server 205 to the memory device 201.

[0070] The embodiments described above represent non-limiting examples only. Additional alternatives are possible; for example, two or more of the conditions described above can be combined. As such, one embodiment may require that a PIN code or a password is correctly entered by a user of the mobile phone, while the secure element must be located in a particular location. Another embodiment may require that the mobile phone is in a particular location and at a predetermined time of the day or the week, and provided that the credential has not expired.

[0071] Also, several different signal paths may be combined. For example, the memory device may send the request for a credential directly to the secure element, while the secure element responds by communicating with the policy server which forwards the necessary credential directly to the memory device. In another embodiment, the memory device may receive data from the secure element and forward this to the policy server for approval, whereupon the policy server responds by returning the credential which in accordance with this embodiment is stored centrally.

[0072] It will be readily understood that in embodiments where the policy server is directly involved in the authorization process before the credential is released to the memory device, the security policy may be changed at any time and a given user or secure element may have their access rights renewed or revoked at any time. Consistent with principles of the invention, access rights may also be revoked actively or passively when the credentials are stored in the secure element.

[0073] According to a first embodiment implementing this feature, the policy server may actively attempt to contact the secure element and change or delete the security policy or the credential stored in the secure element. This may have the advantage of having immediate effect, but a possible disadvantage is that if the policy server is unable to contact the secure element the revocation cannot be implemented.

[0074] In a second embodiment of this feature, the secure element may be configured to regularly contact the policy server to verify that already received security policies are still in effect or to request any updated security policy. If the secure element fails to reach the policy server it may permanently or temporarily suspend all authorization and not release any credential unless communication with the policy server can be reestablished. This may have the advantage of not depending on communication with the policy server, but revocation is only implemented depending on the predetermined intervals at which the secure element is scheduled to contact the policy server.

[0075] The two alternatives may, of course, be combined for added security.

[0076] Reference is now made to FIG. 5, which illustrates an exemplary embodiment of the memory device 101, 201 consistent with the principles of the invention. The memory device includes a number of modules or components, which may be implemented in hardware, in software, or as a combination of both. As such, the memory device may also include for example an application-specific integrated circuit (ASIC) or a field-programmable gate array (FPGA).

[0077] A central processing unit (CPU) 501 is included and configured to execute instructions stored in a first memory 502 in order to enable the memory device to operate in accordance with the invention. In an alternative embodiment of the invention the memory device does not include a CPU, and instead processing capacity of the host device 102, 202 is used to execute instructions stored in the memory 502. In yet another alternative embodiment, there are no instructions stored in memory 502, or memory 502 is not even included in the memory device. Instead the necessary instructions can be stored and executed on the host device 102, 202.

[0078] The memory 502 may include random access memory (RAM) as well as permanent memory, or Read Only Memory (ROM), and may operate to hold instructions, as well as temporary storage of a received credential such as a key file. In some embodiments of the invention the memory 502 may also serve as an unprotected memory area that is available to a user of the host device even if a credential cannot be obtained.

[0079] A second, secure memory 503 can be configured to act as the secure part of the memory device and hold the protected data. According to a first embodiment, this secure memory 503 is part of the same physical memory and file system as the first memory 502, but the data stored here is encrypted or otherwise encoded for obscurity. According to an alternative embodiment, the secure memory is a separate part of the file system but part of the same physical memory. The file system may then implement different access restrictions with respect to this part of the file system. According to yet another alternative embodiment, the secure memory 503 is a physical memory module separate from the first memory module 502, and security measures may be implemented in hardware as well as in software.

[0080] The memory device 101, 201 illustrated in FIG. 5 further includes an access controller 504. The access controller 504 may be configured to provide access to the secure memory 503 when a credential is received in response to a request sent to the secure element 104, 204. The access controller 504 may for example be configured to decrypt encrypted data stored in the secure memory 503 using the received credential which for example may be a decryption key. The access controller 504 may also be a part of a file system which is configured to perform access control list authorization based on the received credential.

[0081] The access controller 504 is shown as a separate module in FIG. 5, but it will be understood by those with skill in the art that while the access controller 504 can be implemented as a separate hardware module in the memory device 101, 201, it may also be implemented as a software module which, as such, can be executed by the CPU 501 and thus provide the functionality of an access controller 504.

[0082] The access controller may be in communication with a first communication interface 505 which provides communication with the host device

102, 202. The host device 102, 202 may for example be a desktop computer or a laptop computer, but other alternatives are consistent with the principles of the invention, such as for example a PDA, a set top box, a television or some other device capable of connecting to a memory device 101, 201. The communication interface 505 may for example follow the Universal Serial Bus (USB) standard. Other alternatives include Secure Digital, Memory Stick and COMPACTFLASH, and even short range wireless such as BLUETOOTH or infrared. Well known infrared communication protocol standards have been specified by the Infrared Data Association (IrDA).

[0083] The communication interface 505 may include hardware which may include a physical connector or a wireless transmitter/receiver. In addition the communications interface may include computer code including instructions that, when executed, perform in accordance with the protocol(s) used by the communication interface 505. These instructions may be executed by the CPU 501, or by dedicated hardware circuits that are part of the communication interface 505.

[0084] According to some embodiments, the communication interface 505 may be associated with an internet protocol (IP) address, making it possible to communicate with the memory device 101, 201 over communication interface 505 remotely, for example from the policy server 205.

[0085] Further, there may be provided a secure channel controller 506 and a radio frequency (RF) interface module 507. The radio frequency interface 507 can be implemented as a radio transmitter operating in accordance with a communication standard. Examples of communication standards include, for example, IEEE 802.11 (a set of standards often referred to as WI-FI or WLAN), BLUETOOTH, ZIGBEE, proximity card, RFID, NFC (ISO 14443) and IEEE 802.16 (WiMAX), but mobile telephone technologies such as GSM or UMTS also represent alternatives that are consistent with the principles of the invention. The RF interface 507 can be used for communication between the memory device 101, 201 and the secure element 104, 204. Since the communication channel between the memory device 101, 201 and the secure element 104, 204 is used to provide the memory device, particularly the access controller 504, with the credential necessary for access to the secure memory 503, the secure channel controller 506 can be used to set up a secure

channel between the memory device and the secure element, e.g. by providing authentication and encryption. The secure element may be implemented as a software module with computer code instructions. These instructions may be executed by the CPU 501 or by dedicated hardware that may be part of the secure channel controller 506.

[0086] According to some embodiments, it may be considered unnecessary to encrypt or authenticate the channel between the memory device 101, 201 and the secure element 104, 204, in which case the secure channel controller may not be provided.

[0087] As described above with reference to FIG. 4, communication between the various devices can progress directly between the devices involved, or over intermediate devices. As such, communication between the memory device 101, 201 and the secure element 104, 204 may be established directly over a wireless communication channel established between the RF interface 507 and a corresponding interface provided in or in communication with the secure element. In alternative embodiments, the communication channel may be established over the host device 102, 202, utilizing communication capabilities of the host device. Embodiments implementing this alternative may not have to include the radio interface 507, and instead the communication channel can be established over the communication interface 505. The secure channel controller 506 may still be included and may be configured to authenticate and encrypt the communication channel between the memory device 101, 201 and the secure element 104, 204 which according to this embodiment is established over interface 505 and the host device 102, 202.

[0088] The various modules of the memory device 101, 201 may communicate with each other over a communication bus 508.

[0089] Turning now to FIG. 6, an exemplary embodiment of a secure element 104, 204 will be discussed in further detail. The secure element 104, 204 includes a number of modules or components which may be implemented in hardware, in software, or as a combination of both.

[0090] The secure element 104, 204, which may for example be a SIM card or a smartcard, includes a central processing unit 601. The device may also include a coprocessor (not shown) to improve the speed of encryption and decryption computations.

[0091] The secure element 104, 204 may further include a memory system which includes three types of memory. A first part of the memory system, as illustrated in FIG. 6, is a persistent memory, or Read Only Memory (ROM) 602, which may be used to store the operating system and other basic software such as encryption algorithms. A second part of the memory is a volatile memory, or Random Access Memory (RAM) 603, used as a working memory during computation and response. The RAM 603 does not store data persistently, and when power is no longer supplied to secure element 104, 204, any contents of the RAM 603 is lost. A third part of the memory can be an Electrical Erasable Programmable Read Only Memory (EEPROM) 604. Data stored in this memory is not lost when power is no longer supplied to the secure element 104, 204, and unlike the ROM 601 it can be reprogrammed by applications. However, this memory will typically be a lot slower than RAM, and it can only be read from and written to a limited number of times.

[0092] An input communication interface 605 that is controlled by the CPU 601 may be configured to communicate with the device in which the secure element is installed, such as a mobile phone 103, 203. The communication interface 605 can include one or more signal connectors depending, for example, on the communications standards or protocols implemented on the secure element. As such an input output connection I/O can be used to communicate directly with the system of the device 103, 203. If the secure element 104, 204 implements USB, two USB connections D+ and D- may be included. Another connection may be dedicated to communication using Single Wire Protocol (SWP) which may be used to implement a secure connection between the secure element and an NFC chip in the device 103, 203. According to some embodiments of the invention the communication interface 605 may be configured with its own Internet Protocol (IP) address which makes it possible to address the secure element directly. Data may be exchanged between the secure element 104, 204 and other parts of the system over a communication capability of the mobile phone 103, 203. However, according

to some embodiments a wireless communication module 607 may also be included. In a first embodiment the wireless communication capability is a short range or relatively short range wireless communication capability such as wireless LAN (IEEE 802.11), BLUETOOTH, ZIGBEE, proximity card, RFID, NFC (ISO 14443) or IEEE 802.16 (WiMAX). Other embodiments may include long range communication capabilities such as GSM or UMTS. Such a communication capability may include an on chip transmitter and receiver.

[0093] The communication interface 605 may also receive a clock signal CLK externally from the device in which the secure element is installed.

[0094] The secure element may include connectors for receiving power Vcc and a reset signal RST, which is standard on SIM cards and most other smartcards. However, the invention is not limited in this respect, and can also be implemented with secure elements which provide their own power and clock signals.

[0095] A security module 606 can be configured to implement the security policy in the secure element 104, 204. The security module 606 may be implemented as a separate module, or as a combination of hardware and software residing in the memory system 602, 603, 604 of the secure element 104, 204. The security module may include a credential that can be transmitted to a memory device 101, 201 in response to a request, as well as instructions and algorithms used to carry out a security policy. The security policy and the credential may be stored in the security module 606 when the secure element 104, 204 is first configured, it may be received as part of a transmission from a policy server 205, or a combination of both.

[0096] The various components of the secure element may be connected over a communication bus 608, or they may be individually wired to communicate with each other.

[0097] Furthermore, the policy server 205 may include a credential request reception unit, a condition information reception unit, a determination unit, a credential providing unit, a policy transmission unit, a condition approval unit and a transmission unit. These units are implemented by a combination of the hardware and software elements discussed above with regard to the policy server 205.

[0098] The mobile telephone 103/203 may include a first communication interface, a determination unit and a providing unit. These units and interface are implemented by a combination of the hardware and software elements discussed above with regard to the mobile telephone 103/203.

[0099] The secure element 104/204 may include a reception unit, a determination unit and a key providing unit. These units are implemented by a combination of the hardware and software elements discussed above with regard to the secure element 104/204.

[00100] The memory device 101/201 may include an access key request unit, an access key reception unit and an access controller. These units are implemented by a combination of the hardware and software elements discussed above with regard to the memory device 101/201.

[00101] In the foregoing specification, a number of details and features have been set forth for the purpose of illustration and description. They are not intended to be exhaustive, and those with ordinary skill in the art will appreciate that the invention can be embodied in other specific forms without departing from the spirit or the essential characteristics thereof. For example, there are many alternative possibilities to exactly which elements should be implemented in a security policy, or in which sequence an exchange of the various requests and responses could take place within the scope of the invention, and they have not all been explicitly mentioned. Thus the scope of the invention is indicated by the appended claims, and changes and design choices that fall within their meaning and the range of equivalents thereof are intended to be embraced by the invention.

WHAT IS CLAIMED

1. A method for controlling access to a memory in a secure memory device utilizing a central processing unit, the method comprising:

receiving a first request for access to said memory;

sending a second request for an access key to an external secure element, said access key availability based on a fulfillment of a condition defined in a security policy;

receiving said access key;

providing the requested access to said memory based on said access key.

2. The method according to claim 1, wherein said first request is received over a first, physical communication interface.

3. The method according to claim 2, wherein said second request is sent over said first interface.

4. The method according to claim 2, wherein said second request is sent over a second, wireless interface.

5. The method according to claim 1, wherein said first request is a request for data that is encrypted and said access key is a decryption key enabling decryption of said data.

6. The method according to claim 1, wherein said condition is one or more requirements stored in said secure element.

7. The method according to claim 6, wherein said one or more requirements are updateable by a policy server.

8. The method according to claim 6, wherein said one or more requirements are updateable via a user interface associated with said secure element.

9. The method according to claim 6, wherein said one or more requirements are chosen from the group consisting of:

a correct entry of a PIN code;

a determined location of the secure element;

a determined location of the secure memory device; and

a determined current time.

10. The method according to claim 1, wherein said second request is sent as a result of said memory device being connected to a host device, and said first request is received from said host device.

11. The method according to claim 1, wherein said second request is sent as a result of said first request being received.

12. The method according to claim 1, wherein said secure element is addressed directly using an IP address.

13. The method according to claim 1, wherein said secure element is addressed indirectly by sending said second request to a remote server, said second message including a unique identification of said secure element.

14. The method according to claim 13, wherein said unique identification is chosen from the group consisting of: ICC identification (ICC-ID) and Mobile Station ISDN number (MSISDN).

15. The method according to claim 1, wherein said memory device is uniquely associated with said secure element.

16. The method according to claim 1, wherein data stored in said memory is uniquely associated with said secure element.

17. The method according to claim 1, wherein said processor is provided as part of said secure memory device.

18. The method according to claim 1 wherein said processor is provided as part of a host device.

19. A secure memory device, comprising:

a secure memory configured to store protected data;

a first memory configured to hold and provide configuration information necessary for configuring a request for an access key that is sent to a secure element in response to a request for access to said secure memory;

a temporary memory configured to receive and temporarily store a received access key from said secure element in response to a condition defined in a security policy being fulfilled;

an access controller configured to provide the requested access to the secure memory based on the received access key.

20. A secure memory device, including:

a first memory;

a secure memory configured to store protected data;

an access key request unit configured to request an access key from a secure element external to the secure memory device using configuration information stored in the first memory, the configuration information configuring the request for the access key;

an access key reception unit configured to receive an access key from the secure element in response to a condition defined in a security policy being fulfilled and to temporarily store the received access key in a temporary memory; and

an access controller configured to provide the requested access to the secure memory based on the received access key.

21. The secure memory device of claim 20, further comprising a first communication interface configured to provide communication with a host device and to receive said request for access.

22. The secure memory device of claim 20, wherein the access key request unit is configured to request the access key in response to a request for access to the secure memory.

23. The secure memory device of claim 1, wherein the first memory is a non-secure memory accessible by the access key request unit without an access key.

24. The secure memory device of claim 20, wherein

said secure memory is configured to store data that is encrypted, and

said access key is a decryption key enabling decryption of said data.

25. The secure memory device of claim 20, further comprising:

a second, wireless communication interface configured to provide communication with the secure element.

26. A computer readable medium having stored thereon a program that when executed by a secure memory device performs a method of controlling access to a memory in the secure memory device, the method comprising:

receiving a first request for access to the memory;

sending a second request for an access key to an external secure element, the access key availability determined based on a fulfillment of a condition defined in a security policy;

receiving the access key; and

providing the requested access to the memory based on said access key.

27. A method for providing an access key from a secure element operable in a mobile device and executed using a central processing unit, comprising:

receiving a request for an access key from an external secure memory device having a memory configured to store protected data;

determining whether a condition defined in a security policy is fulfilled; and

providing the access key to the secure memory device in response to the result of the determining.

28. The method according to claim 27, wherein said determining whether a condition defined in the security policy is fulfilled further comprises:

determining whether one or more requirements are met, the requirements including at least one of:

a correct entry of a PIN code;

a determined location of the secure element;

a determined location of the secure memory device; and

a determined current time.

29. The method according to claim 27, wherein said request for said access key from said secure memory device is received over a first physical communication interface.

30. The method according to claim 27, wherein said request for said access key from said secure memory device is received over a second wireless interface.

31. The method according to claim 29, wherein said providing said access key to said secure memory device in response to said result of said determining is performed using said first physical communication interface.

32. The method according to claim 30, wherein said providing said access key to said secure memory device in response to said result of said determining is performed using said second wireless device.

33. The method according to claim 27, wherein said access key is a decryption key enabling decryption of said data.

34. The method according to claim 28, wherein said security policy is updateable by a policy server.

35. The method according to claim 28, wherein said security policy is updateable via a user interface.

36. The method according to claim 27, wherein said secure memory device communicates with the secure element using an IP address.

37. The method according to claim 27, wherein said secure memory device communicates with the secure element indirectly by sending said request to the secure element by way of a remote server, said request including a unique identification of said secure element.

38. The method according to claim 37, wherein said unique identification is chosen from the group consisting of: ICC identification and Mobile Station ISDN number.

39. The method according to claim 27, wherein said secure memory device is uniquely associated with said secure element.

40. The method according to claim 27, wherein data stored in said secure memory device is uniquely associated with said secure element.

41. A secure element operable in a mobile device, comprising:

a memory storing an access key;

a reception unit configured to receive a request for the access key from an external secure memory device having a memory configured to store protected data;

a determination unit configured to determine whether a condition defined in a security policy is fulfilled; and

a key providing unit configured to provide the access key to the secure memory device in response to the result of the determining by the determination unit.

42. A computer readable medium having stored thereon a program that when executed by a secure element performs a method of providing an access key from the secure element, the method comprising:

receiving a request for an access key from an external secure memory device having a memory configured to store protected data;

determining whether a condition defined in a security policy is fulfilled; and

providing the access key to the secure memory device in response to the result of the determining.

43. A mobile device, comprising:

a secure element having an access key;

a first communication interface configured to receive a request for the access key from an external secure memory device having a memory configured to store protected data;

a determination unit configured to determine whether a condition defined in a security policy is fulfilled; and

a providing unit configured to provide the access key to the secure memory device via the first communication interface in response to the result of the determining by the determination unit.

44. A policy server, comprising:

a computer readable memory configured to store a security policy;

a central processing unit; and

a transmission unit configured to provide an external secure element with an authentication requirement corresponding to the security policy requiring that a condition be satisfied before an access key is provided to a secure memory device from the external secure element.

45. A policy server, comprising:

a computer readable memory configured to store a security policy;

a central processing unit;

a policy transmission unit configured to provide an external secure element with the security policy requiring that a condition be satisfied in order that an access key can be provided to a secure memory device from the external secure element; and

a condition approval unit configured to receive a request for approval from the external secure element generated based on the security policy and including condition information, to determine whether the condition is satisfied based on the

condition information, and to transmit an approval response based on the determination.

46. A policy server, comprising:

a computer readable memory;

a central processing unit;

a credential request reception unit configured to receive an access key request from a secure device having a memory configured to store protected data, the credential request including a unique identification of a secure element;

a condition information reception unit configured to send a request to the secure element identified based on the unique identification for condition information and to receive the condition information from the secure element in response to the request;

a determination unit configured to determine whether a condition is satisfied based on the condition information; and

a credential providing unit configured to provide the secure device having the memory with the access key in response to a result of the determination unit.

47. The policy server according to claim 41, wherein

the secure element has the access key and the condition information reception unit is further configured to receive the access key from the secure element in response to the request.

48. A secure memory system comprising:

a secure memory device, including:

a first memory;

a secure memory configured to store protected data,

an access key request unit configured to request an access key from a secure element external to the secure memory device using configuration information stored in the first memory, the configuration information configuring the request for the access key,

an access key reception unit configured to receive an access key from the secure element in response to a condition defined in a security policy being fulfilled and to temporarily store the received access key in a temporary memory, and

an access controller configured to provide the requested access to the secure memory based on the received access key;

the secure element including:

a memory storing the access key,

a reception interface configured to receive a request for the access key from the secure memory device,

a determination unit configured to determine whether the condition defined in the security policy is fulfilled, and

a providing unit configured to provide the access key to the secure memory device in response to the result of the determining by the determination unit.

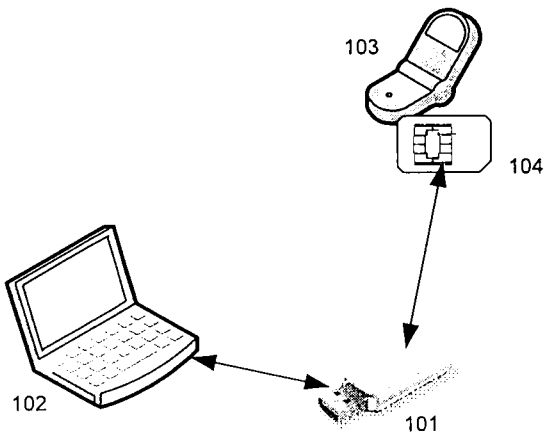

FIG. 1

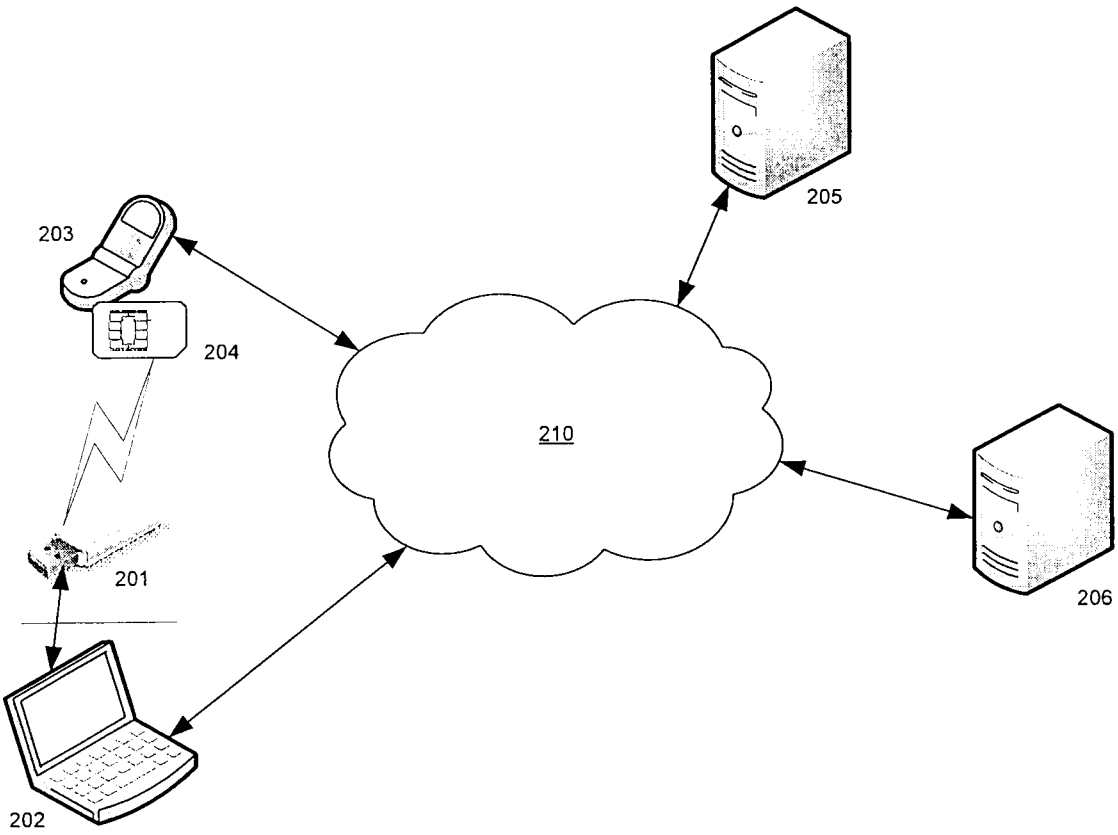

FIG. 2

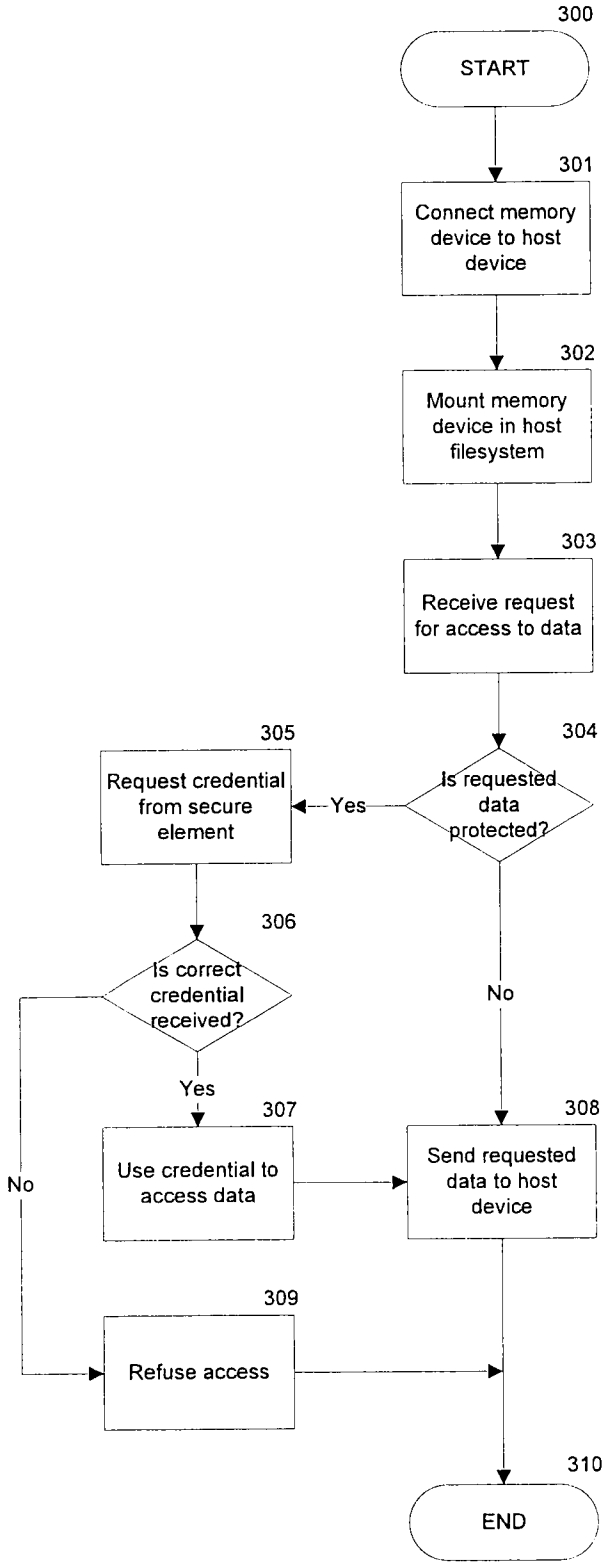
300
START
301
Connect memory device to host device
302
Mount memory device in host filesystem
303
Receive request for access to data
304
Is requested data protected?
Yes
305
Request credential from secure element
306
Is correct credential received?
Yes
No
307
Use credential to access data
No
308
Send requested data to host device
309
Refuse access
310
END

FIG. 3

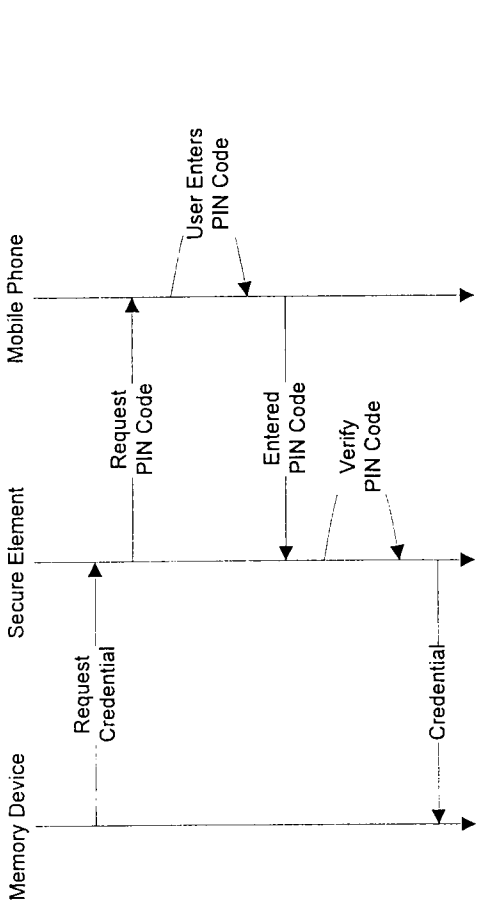
Mobile Phone
Secure Element
Memory Device
User Enters PIN Code
Request PIN Code
Entered PIN Code
Verify PIN Code
Request Credential
Credential

FIG. 4A

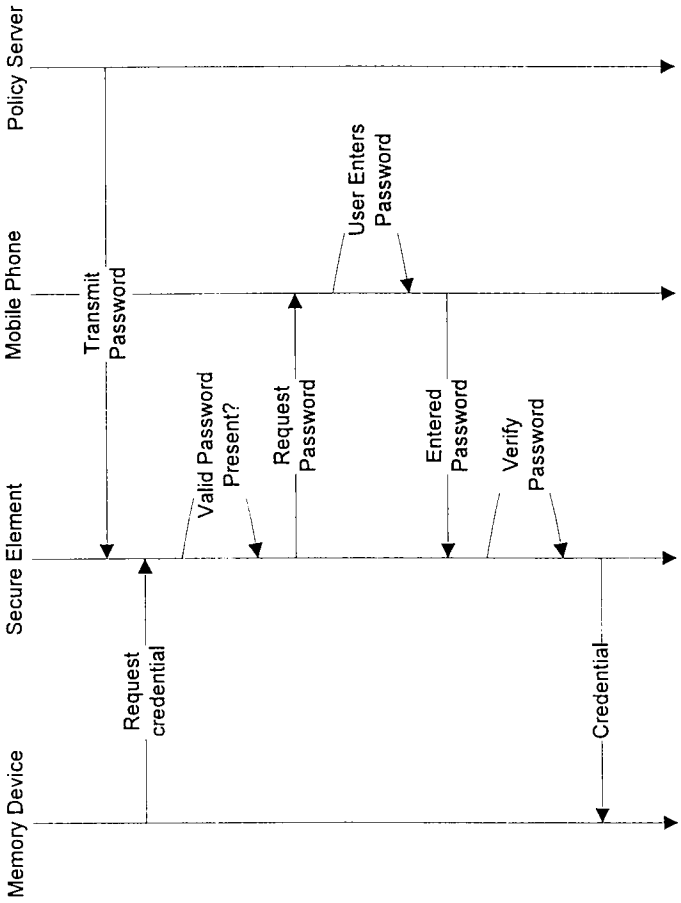
Policy Server
Mobile Phone
Secure Element
Memory Device
Transmit Password
User Enters Password
Valid Password Present?
Request Password
Entered Password
Verify Password
Request credential
Credential

FIG. 4B

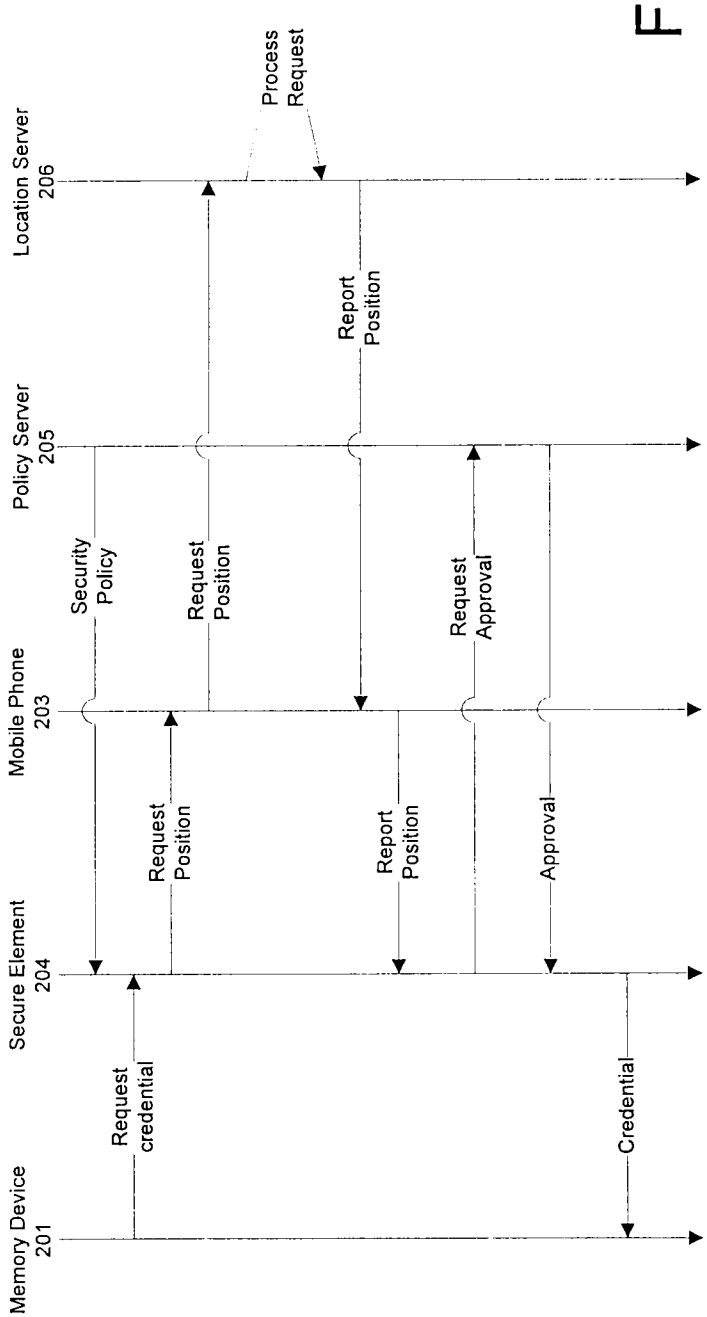
Memory Device
201
Secure Element
204
Mobile Phone
203
Policy Server
205
Location Server
206
Request credential
Request Position
Security Policy
Request Position
Process Request
Report Position
Request Approval
Report Position
Approval
Credential

FIG. 4C

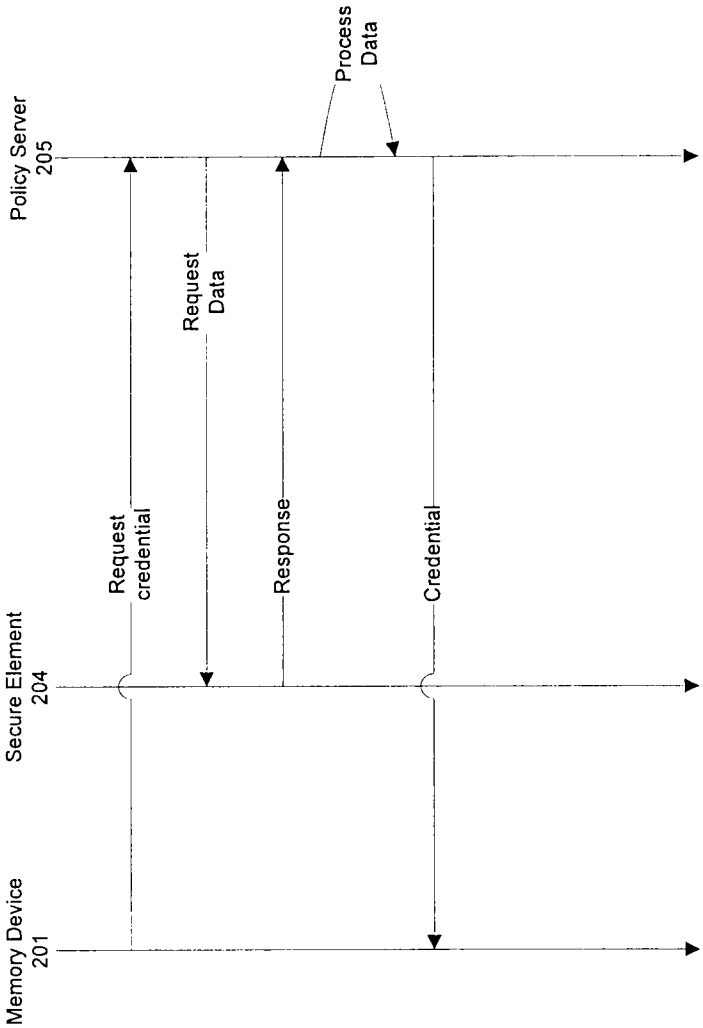
Process Data
Policy Server 205
Request Data
Request credential
Response
Credential
Secure Element 204
Memory Device 201

FIG. 4D

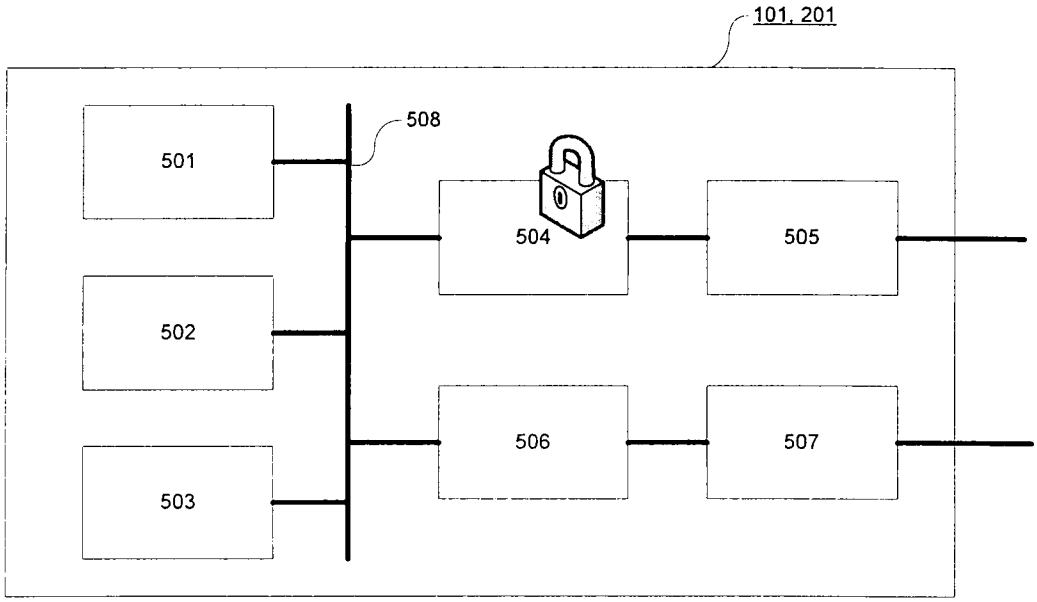
101, 201
508
501
502
503
504
505
506
507

FIG. 5

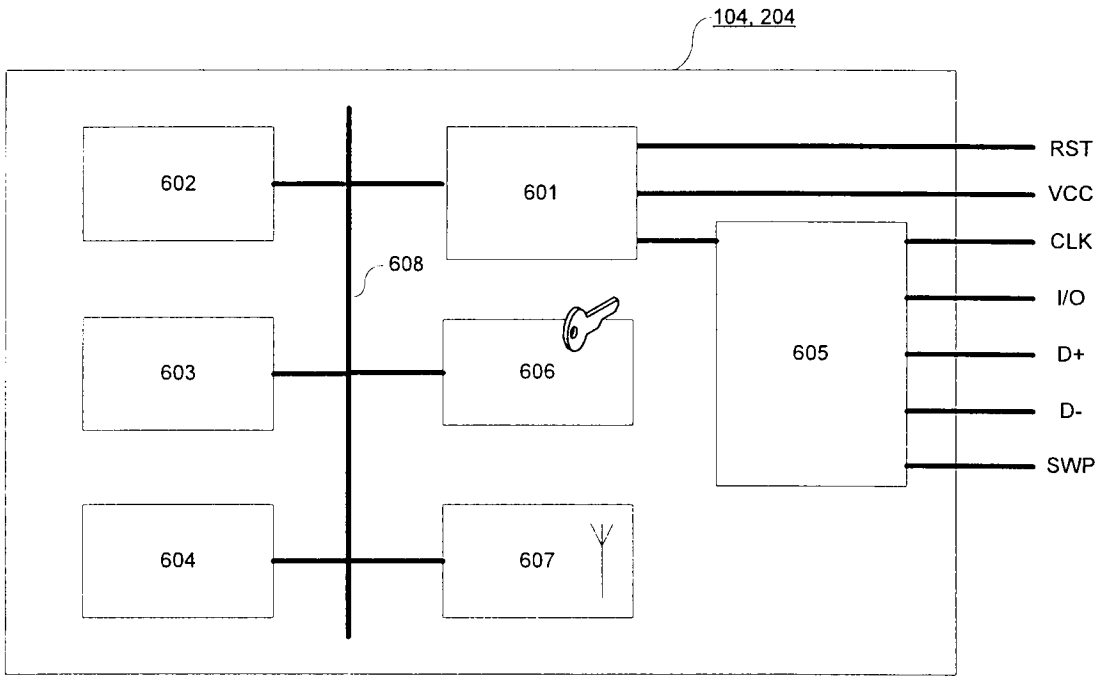
104, 204
602
603
604
608
601
606
607
605
RST
VCC
CLK
I/O
D+
D-
SWP

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2009/006827

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00 G06F21/24
ADD.

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)
G06F

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 107 627 A1 (SIEMENS AG [DE]) 13 June 2001 (2001-06-13)	1-9,11, 12, 15-17, 19,20, 22-36, 39-43,48
Y	the whole document	10,13, 14,18, 21,37, 38,47
Y	WO 2009/083478 A1 (GEMALTO SA [FR]; FAHER MOURAD [FR]) 9 July 2009 (2009-07-09) the whole document	10,18,21
X	US 2007/053306 A1 (STEVENS GILMAN R [US]) 8 March 2007 (2007-03-08)	46
Y	the whole document	13,14, 37,38,47

☐ 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 document 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	Date of mailing of the international search report
9 August 2010	26/08/2010

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Fax: (+31–70) 340–3016	Mäenpää, Jari

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2009/006827

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.

3. ☒ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

1-43, 46-48

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☒ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-12, 15-26, 48

A method, secure memory device and a computer readable medium wherein messages to the secure element are routed through a host device. The connectivity via a host device of claims 10, 18, 21 is considered as a special technical feature. The corresponding technical problem to be solved is a more flexible connectivity between a secure memory device and a secure element.

---

2. claims: 13, 14, 27-43, 46, 47

A method, secure element, computer readable medium, a mobile device and a policy server wherein the requests to the secure element are routed indirectly via the policy/remote server. The server mediated connectivity between the secure memory device and the secure element of claims 37 and 46 (and figure 4d) is considered as a special technical feature. The corresponding technical problem solved is to implement centrally manageable policies for accessing a secure memory device.

---

3. claims: 44, 45

A policy server transmitting policies/authentication requirements and responding to condition approval requests from a secure element. The server performed condition approval of claim 45 (and figure 4c) is considered as a special technical feature. The corresponding technical problem solved is to implement centrally manageable policies for accessing a secure memory device.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2009/006827

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1107627 A1	13-06-2001	NONE	
WO 2009083478 A1	09-07-2009	EP 2077517 A1	08-07-2009
US 2007053306 A1	08-03-2007	NONE	