



US 20080046739A1

(19) **United States**

(12) **Patent Application Publication**

Adams et al.

(10) **Pub. No.: US 2008/0046739 A1**

(43) **Pub. Date: Feb. 21, 2008**

(54) **HASH OF A CERTIFICATE IMPORTED FROM A SMART CARD**

(22) Filed: **Aug. 16, 2006**

(75) Inventors: **Neil Adams, Waterloo (CA); Herbert Little, Waterloo (CA); Michael K. Brown, Kitchener (CA)**

Publication Classification
(51) **Int. Cl. H04L 9/00** (2006.01)

(52) **U.S. Cl. 713/176**

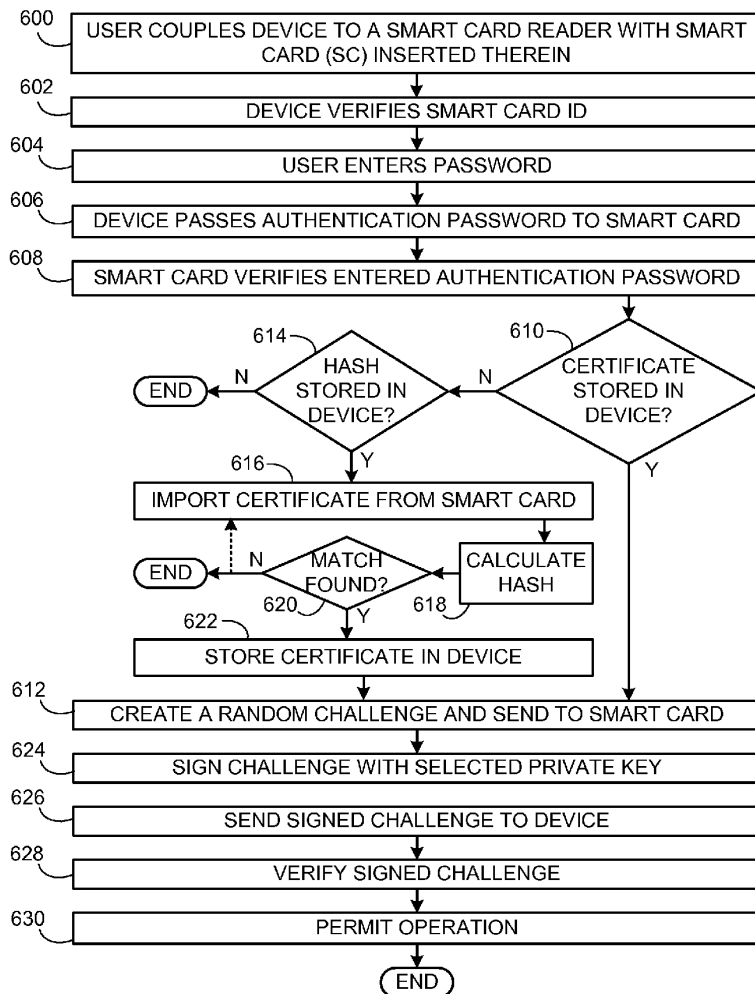
Correspondence Address:
**INTEGRAL INTELLECTUAL PROPERTY INC.
1370 DON MILLS ROAD, SUITE 300
TORONTO, ON M3B 3N7**

(57) **ABSTRACT**

A certificate from a smart card is imported into a computerized device via a smart card reader. The computerized device calculates a hash of the imported certificate and stores the hash in memory. The hash may be stored in a region of the memory that is unaffected by upgrades to the device.

(73) Assignee: **RESEARCH IN MOTION LIMITED, Waterloo (CA)**

(21) Appl. No.: **11/464,900**



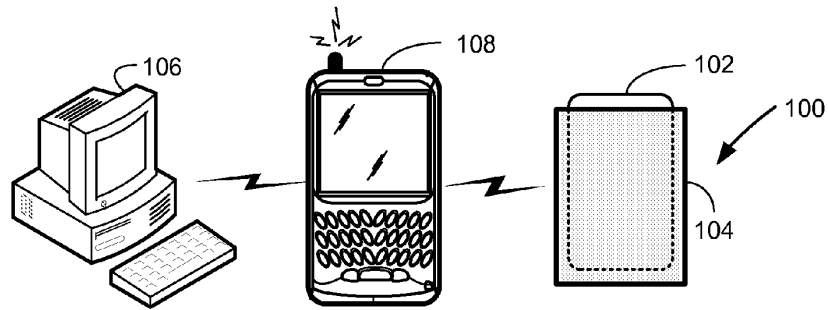


FIG. 1

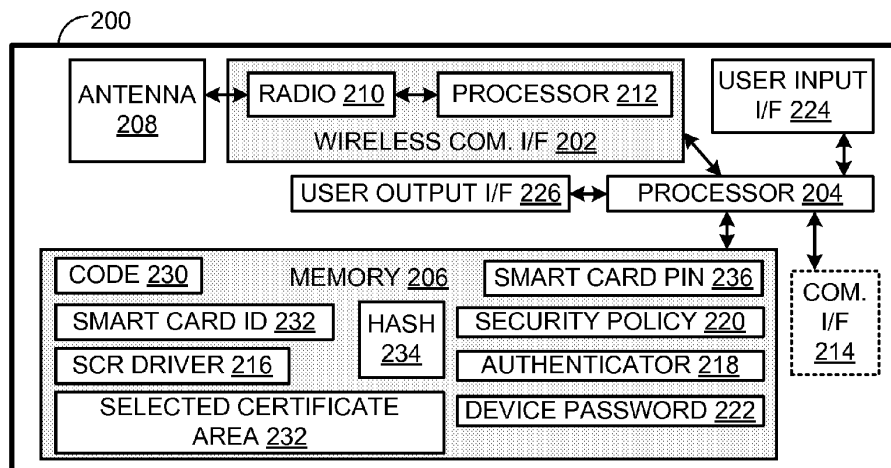


FIG. 2

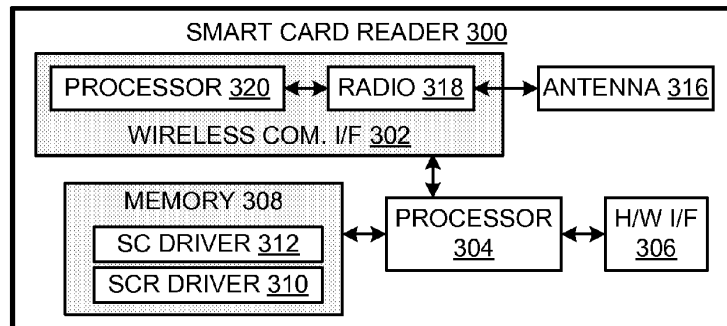


FIG. 3

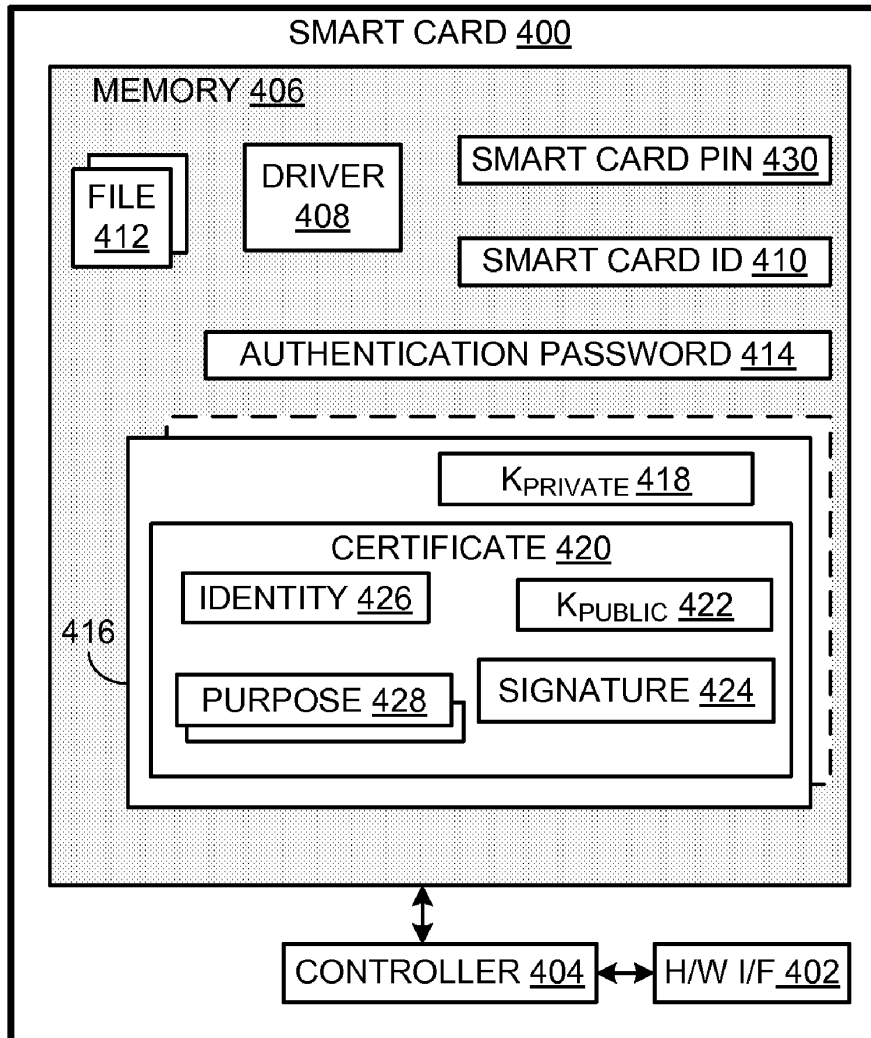


FIG. 4

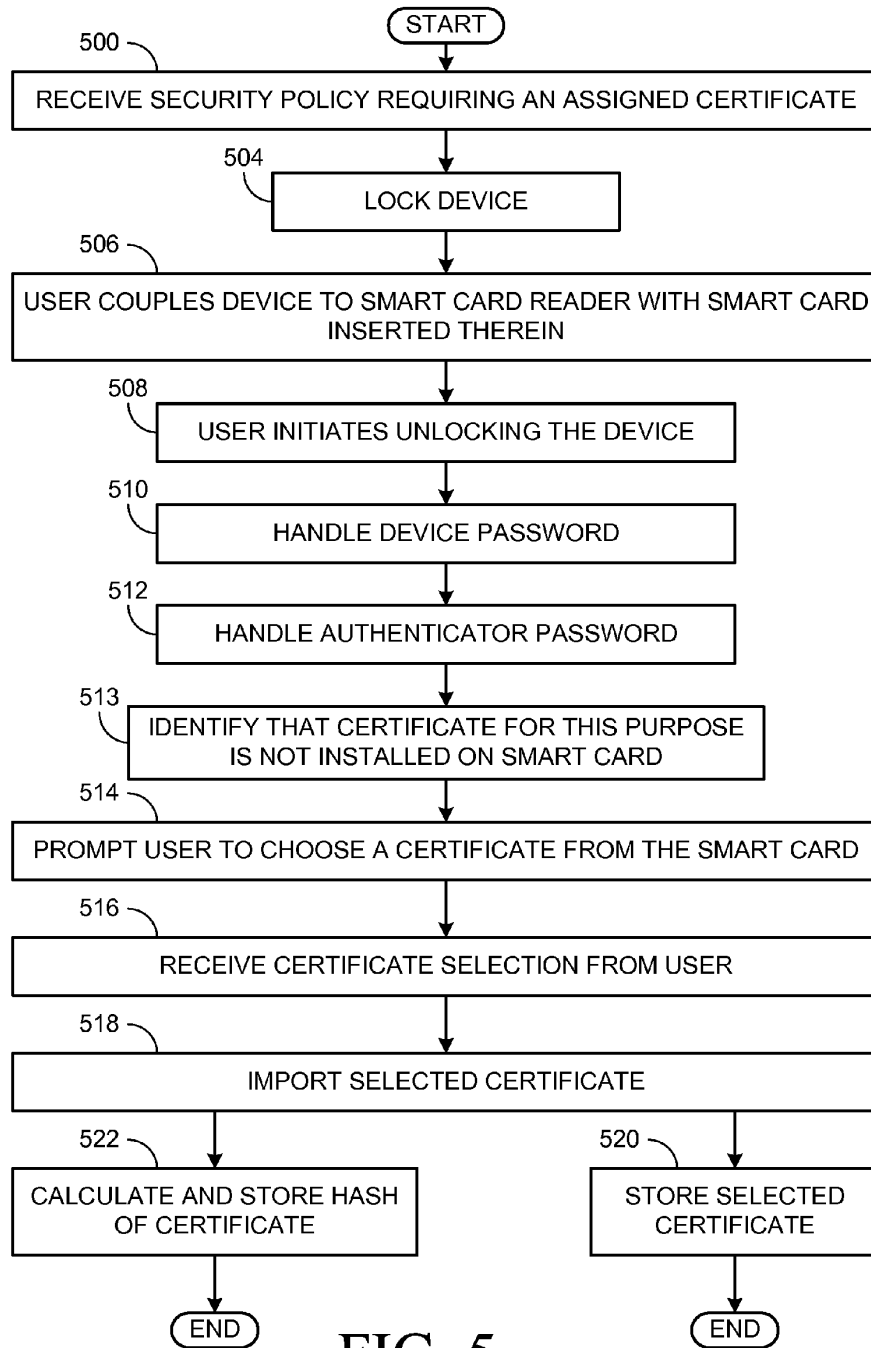


FIG. 5

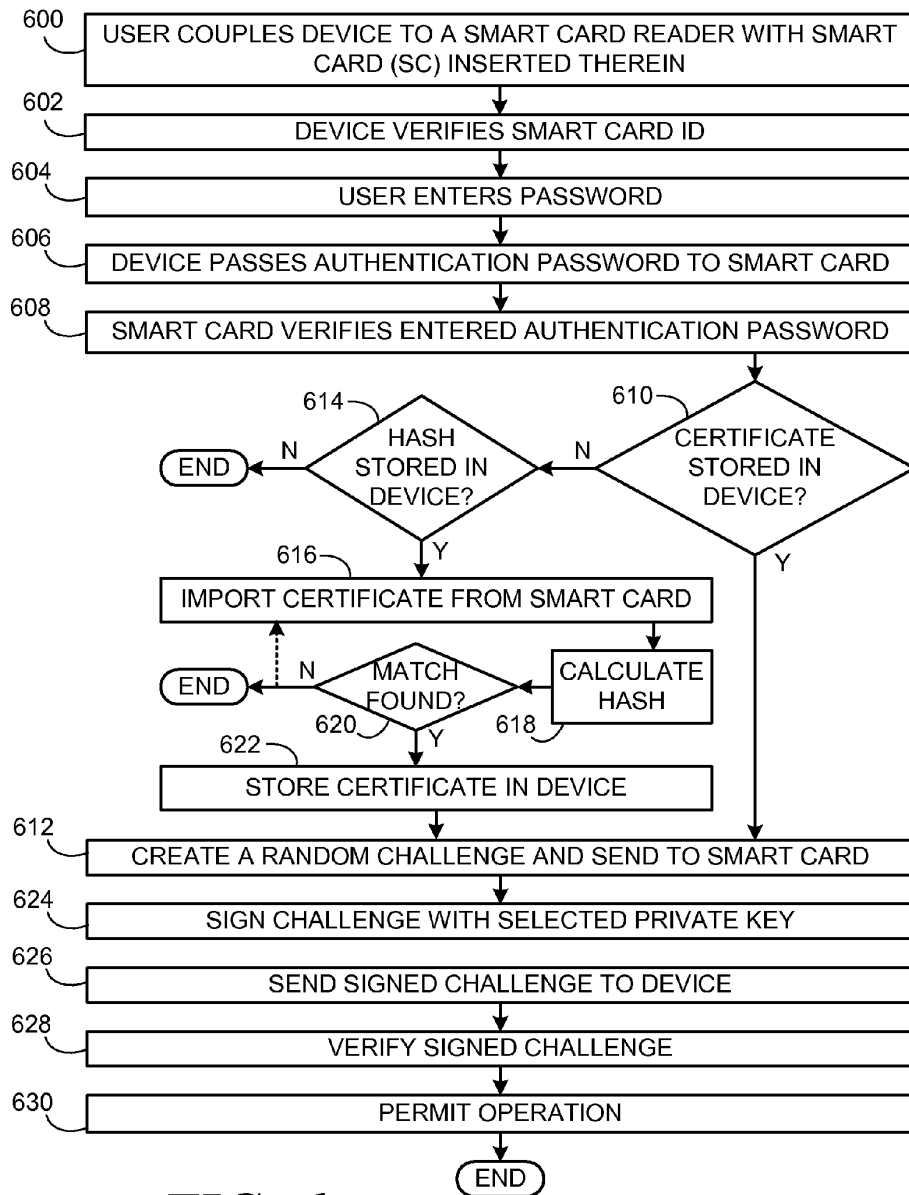


FIG. 6

HASH OF A CERTIFICATE IMPORTED FROM A SMART CARD

BACKGROUND

[0001] Smart Cards (SC) are widely used in conjunction with security measures such as authentication and encryption. For example, in order to access a computerized device and to access information using the computerized device, one may have to couple a smart card to the computerized device. Access to the computerized device and to information may be granted following a successful interaction between the computerized device and the smart card. The interaction may involve user input.

[0002] A smart card may be programmed or otherwise set to have security related information. An example is identification information of the smart card itself, for example, a serial number. Another example is an authentication password, where access to functionality of the smart card may require knowledge of the authentication password. A further example is one or more files that include specific items of information, such as personal identification information of one or more authorized users of the smart card.

[0003] Yet another example is a certificate/private key pair. A certificate may include a public key that is associated with the private key of the pair, and may also include a signature, identity information and a field defining one or more purposes assigned to the certificate. Private keys are stored in a secure area on the smart card and are not accessible from the outside. Certificates, on the other hand, may be exported from the smart card to other devices.

[0004] A certificate may be assigned, for example, for authentication of a user, for encryption of information, for signing information, for securing web browsing, for login into a WEB service and/or for providing an access to a network or a device. A smart card may include one or more certificate/private key pairs.

[0005] A certificate that is assigned to a particular purpose may include information specific to the purpose. For example, a certificate assigned for login into a network may include information about the network. The purpose defined in a certificate is not mandatory, and a certificate may be used for any other purpose.

[0006] Information is usually initialized into a smart card using dedicated equipment and usually by dedicated personnel, such as members of an IT (Information Technology) department of an organization. A smart card may be initialized for specific purposes with a particular number of certificate/private key pairs that are assigned for these specific purposes. At a later time, however, there may be a need to use the smart card for a purpose that is not defined in any of the certificates. Intervention of the dedicated personnel may then be required in order to initialize an additional certificate/private key pair in the smart card.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] Embodiments are illustrated by way of example and not limitation in the figures of the accompanying drawings, in which like reference numerals indicate corresponding, analogous or similar elements, and in which:

[0008] FIG. 1 is a schematic diagram of an exemplary system comprising a smart card, a smart card reader and computerized devices;

[0009] FIG. 2 is a block diagram of an exemplary computerized device;

[0010] FIG. 3 is a block diagram of an exemplary smart card reader;

[0011] FIG. 4 is a block diagram of an exemplary smart card;

[0012] FIG. 5 is a flowchart of an exemplary method to enable the use of a certificate stored in a smart card; and

[0013] FIG. 6 is a flowchart of another exemplary method to enable the use of a certificate stored in a smart card.

[0014] It will be appreciated that for simplicity and clarity of illustration, elements shown in the figures have not necessarily been drawn to scale. For example, the dimensions of some of the elements may be exaggerated relative to other elements for clarity.

DETAILED DESCRIPTION

[0015] In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of embodiments. However it will be understood by those of ordinary skill in the art that the embodiments may be practiced without these specific details. In other instances, well-known methods, procedures, components and circuits have not been described in detail so as not to obscure the embodiments.

[0016] A smart card is traditionally initialized with content using dedicated equipment and dedicated personnel, such as members of an IT department of an organization. A smart card may be initialized with one or more pairs of a certificate and a private key and any one of the certificates may be assigned with particular one or two purposes. The purposes may be included in the certificate.

[0017] If a smart card is to be used for a particular purpose and there is no certificate initialized on the smart card for this purpose, a fairly complex operation is traditionally needed in order to initialize such a certificate on the smart card.

[0018] According to some embodiments of the invention, a computerized device may enable a user to select one of the certificates already installed in the smart card for the particular purpose. The user may need to identify himself or herself by entering one or more correct passwords and will then be prompted to select a certificate. The device may import the selected certificate from the smart card.

[0019] According to some embodiments of the invention, the device may store a copy of the imported certificate in a memory of the device. To enable the user to use the device for the particular purpose, the device may verify that the user has coupled an appropriate smart card to the device and that the user has a permission to use the smart card. The device may send a challenge to the smart card and an identification of the selected certificate. The smart card may sign the challenge using the private key corresponding to the previously selected certificate. The device may verify the signature using the copy of the certificate and may permit the user to perform the desired operation.

[0020] According to other embodiments of the invention, the device may calculate a hash of the imported certificate and may store the calculated hash in a memory of the device. The hash may be stored in a region of the memory that is unaffected by upgrades to the device. To enable the user to use the device for the particular purpose, the device may verify that the user has coupled an appropriate smart card to the device and that the user has a permission to use the smart

card. The device can import certificates from the smart card; all of them or one by one. The device may calculate the hash of the certificates in order to find a match with the previously stored hash. A matching hash, if found by the device, identify the selected certificate. The smart card may sign the challenge using the private key corresponding to previously selected certificate. The device may verify the signature using the imported certificate and may permit the user to perform the desired operation.

[0021] According to some other embodiments of the invention, the device may calculate a hash of the imported certificate and may store both the calculated hash and a copy of the certificate in a memory of the device. To enable the user to use the device for the particular purpose, the device may verify that the user has coupled an appropriate smart card to the device and that the user has a permission to use the smart card. The device may check whether it stores a copy of the required certificate for that particular purpose and if so, may enable the user to use the device to perform a desired operation as described above with a challenge-response. If the device does not store a copy of the required certificate, for example, because it was previously erased from the device, it may use the hash as described above to identify the appropriate certificate.

[0022] FIG. 1 is a schematic diagram of an exemplary system 100 comprising a SC 102, a smart card reader (SCR) 104 and computerized devices 106 and 108.

[0023] Smart cards are personalized security devices, defined by the ISO7816 standard and its derivatives, as published by the International Organization for Standardization. A smart card may have a form factor of a credit card and may include a semiconductor device. The semiconductor device may include a memory that can be programmed with security information (e.g. a private decryption key, a private signing key, biometrics, an authentication certificate, etc.), and may include a decryption engine, e.g., a processor and/or dedicated logic, for example dedicated decryption logic and/or dedicated signing logic. A smart card may include a connector for powering the semiconductor device and performing serial communication with an external device. A smart card may be used for visual identification, time cards, door access, and the like.

[0024] A SCR is a device that can communicate with both the SC and a computerized device and can therefore be used to couple them. The SCR may include one or more driver applications to communicate with the SC and with the computerized device.

[0025] Some smart card readers are able to be mechanically and electrically coupled to the computerized device. For example, some smart card readers are designed to be permanently installed inside a computerized device such as a desktop computer. Other smart card readers, for example, those in the form factor of a PCMCIA (Personal Computer Memory Card International Association) card, are designed to be easily installable and removable at an appropriate bay in a mobile computerized device such as a laptop computer. Other smart card readers are designed to connect to a computerized device via an electrical cable.

[0026] However, smart card readers that are mechanically disconnected from the computerized device and can communicate with the computerized device using wireless communication are known. Since a wireless smart card reader does not require mechanical coupling to the computerized

device, it can in principle maintain parallel communication sessions with two or more computerized devices via the wireless communication.

[0027] Although FIG. 1 shows smart card 102 inserted into with SCR 104, embodiments of this invention are equally applicable to contactless smart cards that communicate with their smart card readers via other means, for example, using radio frequency identification (RFID) technology.

[0028] Embodiments of the invention are applicable to any computerized device, whether stationary or mobile, that is able to communicate with a SCR. For example, the communication may be possible via a wired, wireless or optical communication means.

[0029] A non-exhaustive list of examples for devices 106 and 108 includes any of the following computerized devices, for example, server computers, notebook computers, laptop computers, mobile computers, mobile terminals, pocket computers, desktop personal computers, personal digital assistants (PDAs), handheld computers, cellular telephones, MP3 players, and the like.

[0030] In exemplary system 100, computerized device 108 is able to communicate with SCR 104 and via SCR 104, with SC 102. In addition computerized device 108 is able to communicate with computerized device 106.

[0031] FIG. 2 is a block diagram of an exemplary computerized device 200, according to some embodiments of the invention. Device 200 is an example of device 108.

[0032] Device 200 comprises a communication interface 202, a processor 204 coupled to communication interface 202 and a memory 206 coupled to processor 204. Memory 206 may be fixed in or removable from device 200. Processor 204 and memory 206 may be part of the same integrated circuit or in separate integrated circuits.

[0033] In the example shown in FIG. 2, communication interface 202 is a wireless communication interface 202 and device 200 also comprises an antenna 208. Wireless communication interface 202 comprises a radio 210 coupled to antenna 208, and a processor 212 coupled to radio 210. Wireless communication interface 202 and processor 204 may be part of the same integrated circuit or in separate integrated circuits.

[0034] Device 108 may be able to communicate with SCR 104 via communication interface 202 and may be able to communicate with device 106 via communication interface 202. Alternatively, or in addition, device 108 may include a communication interface 214 and may be able to communicate with device 106 via communication interface 214.

[0035] Memory 206 stores a SCR driver 216, an authenticator 218, a security policy 220 and a device password 222. Device 200 includes a human input interface 224, such as a keyboard, and a human output interface 226, such as a display. As part of an authentication process, user output interface 226 may prompt the user to enter a device password using user input interface 224, and authenticator 218 may compare the entered password to device password 222.

[0036] Security policy 220 may be predefined and/or downloadable to device 108 from device 106, and may define security related parameters and behaviors for device 108. For example, security policy 220 may define if and for what purpose an authentication password that is stored on a smart card, and device password 222, are to be used and may define qualities of these passwords. In other examples, security policy 220 may define whether a two-factor chal-

challenge-response authentication is to be used or not, whether or not weak certificates are permitted, and how to treat revoked, invalid or untrusted certificates.

[0037] Memory 206 also stores executable code 230 which, when executed by processor 204, causes device 200 to perform its part in the methods described hereinbelow.

[0038] FIG. 3 is a block diagram of an exemplary SCR 300, according to some embodiments of the invention. SCR 300 is an example of SCR 104.

[0039] SCR 300 includes a communication interface 302, a processor 304 coupled to wireless communication interface 302, a hardware interface 306, and a memory 308 coupled to processor 304. For example, hardware interface 306 is a connector that mates to a corresponding connector with contact pins on a smart card. Memory 308 may be fixed in or removable from smart card reader 300. Memory 308 may be embedded or partially embedded in processor 304. Memory 308 stores a smart card reader driver 310 and a smart card driver 312.

[0040] Processor 304 and memory 308 may be part of the same integrated circuit or in separate integrated circuits.

[0041] In the example shown in FIG. 3, communication interface 302 is a wireless communication interface 302 and SCR 300 also comprises an antenna 316. Wireless communication interface 302 comprises a radio 318 coupled to antenna 316, and a processor 320 coupled to radio 318. Wireless communication interface 302 and processor 304 may be part of the same integrated circuit or in separate integrated circuits.

[0042] FIG. 4 is a block diagram of an exemplary SC 400, according to some embodiments of the invention. SC 400 is an example of SC 102. SC 400 includes a hardware interface 402, a controller 404 coupled to hardware interface 402, and a memory 406 coupled to controller 404.

[0043] Memory 406 stores a driver 408 to handle functionality of SC 400, a smart card identification 410, for example a serial number, and one or more files 412 with information about the smart card's owner and/or any other information. Memory 406 may store an authentication password 414 to be used in conjunction with authenticator 218 of SCR 300. As part of an authentication process, user output interface 226 may prompt the user to enter an authenticator password using user input interface 224 and authenticator 218 may compare the entered password to authentication password 414.

[0044] Memory 406 may store one or more pairs 416 each comprising a private key 418 ($K_{PRIVATE}$) and a certificate 420. Any of certificates 420 may comprise a public key (K_{PUBLIC}) 422 associated with private key 418, a signature 424, identification information 426 and one or more definitions 428 of purposes assigned to the certificate.

[0045] Memory 406 may store in addition a smart card PIN (Personal Identification Number) 430.

[0046] A non-exhaustive list of examples for antennae 208 and 316 includes dipole antennae, monopole antennae, multilayer ceramic antennae, planar inverted-F antennae, loop antennae, shot antennae, dual antennae, omnidirectional antennae and any other suitable antennae.

[0047] A non-exhaustive list of examples of communication protocols with which communication interfaces 202 and 302 may be compatible includes Bluetooth®, ZigBee™, radio frequency identification (RFID), ultra wideband (UWB), IEEE 802.11, and proprietary communication protocols.

[0048] A non-exhaustive list of examples for processors 204, 212, 304 and 320 and controller 404 includes a central processing unit (CPU), a digital signal processor (DSP), a reduced instruction set computer (RISC), a complex instruction set computer (CISC) and the like. Furthermore, processors 206, 218, 306 and 318 may be part of application specific integrated circuits (ASICs) or may be a part of application specific standard products (ASSPs).

[0049] A non-exhaustive list of examples for memories 206, 308 and 406 includes any combination of the following:

[0050] a) semiconductor devices such as registers, latches, read only memory (ROM), mask ROM, electrically erasable programmable read only memory devices (EEPROM), flash memory devices, non-volatile random access memory devices (NVRAM), synchronous dynamic random access memory (SDRAM) devices, RAMBUS dynamic random access memory (RDRAM) devices, double data rate (DDR) memory devices, static random access memory (SRAM), universal serial bus (USB) removable memory, and the like;

[0051] b) optical devices, such as compact disk read only memory (CD ROM), and the like; and

[0052] c) magnetic devices, such as a hard disk, a floppy disk, a magnetic tape, and the like.

[0053] Device 200, SCR 300 and SC 400 include additional components which are not shown in FIGS. 2, 3 and 4 and which, for clarity, are not described herein.

[0054] FIG. 5 is a flowchart of an exemplary method to enable use of a certificate stored in smart card 400.

[0055] At 500, device 200 stores in memory 206 security policy 220 that requires a certificate installed in SC 400 for a particular purpose. For example, security policy 220 may require a certificate for the purpose of authentication of a user, two-factor authentication challenge/response, encryption of information, signing information, securing web browsing, login into a WEB service and/or providing access to a network or a device.

[0056] If device 200 is not already locked, at 504, device 200 may become locked. At 506, a user that wants to perform an operation involving device 200 couples SC 400 to SCR 300 and SCR 300 to device 200. At 508, the user initializes a process of authenticating himself or herself to device 200, for example, by turning on device 200 or by activating user input interface 224 in a pre-defined manner.

[0057] At 510, device 200 may prompt the user to set a new device password and may store the received device password as device password 222. Otherwise, if device password 222 is already defined, device 200 may prompt the user to enter a device password and may compare the entered password to a value stored in device password 222.

[0058] At 512, device 200 may prompt the user to set a new authentication password and may store the received authentication password as authentication password 414 in memory 406 of SC 400. Otherwise, if authentication password 414 is already defined, device 200 may prompt the user to enter an authentication password and may compare the entered password to a value stored in authentication password 414.

[0059] At 513, device 200 identifies that SC 400 does not store a certificate that is assigned with the particular purpose required by security policy 220.

[0060] At 514, device 200 may prompt the user to select one of certificates 420 for the particular purpose defined in security policy 220. At 516, device 200 receives from the

user a selection of one of certificates **420**. At **518**, device **200** imports the selected certificate from SC **400**.

[**0061**] At **520**, device **200** may store a copy of the selected certificate into a selected certificate store area **232** in memory **206**. At **522**, device **200** may calculate a hash **234** of the selected certificate and may store hash **234** in memory **206**.

[**0062**] Device **200** may perform only one of boxes **520** and **522**, or may perform both.

[**0063**] Many modifications to this method are contemplated. For example, the requirement that a certificate installed in SC **400** be used for a particular purpose may be enabled by the user of device **200**, rather than from a security policy **220**. In another example, if device **200** has already imported the certificates from SC **400** (for other purposes), then device **200** may determine already after **500** that a certificate for this particular purpose is not installed on SC **400**.

[**0064**] FIG. **6** is a flowchart of another exemplary method to enable the use of a certificate stored in a smart card to perform an operation that requires a particular certificate. Device **200** may have been upgraded and information about the particular certificate, or even a copy of the particular certificate stored in device **200**, may have been deleted from device **200** during the upgrade. At **600**, a user couples SC **400** to SCR **300** and SCR **300** to device **200**. At **602**, device **200** verifies whether it recognizes smart card **400**. For example, device **200** may read smart card identifier **410** from SC **400** and may compare it to a smart card identifier **232** previously stored in memory **206**.

[**0065**] At **604**, device **200** prompts the user to enter an authentication password and at **606**, device **200** passes the password entered by the user to SC **400** for verification. At **608**, SC **400** verifies whether the entered password is identical to authentication password **414**.

[**0066**] If, as shown at **610**, a copy of the particular certificate is stored in area **232**, the method may continue to **612**. If a copy of the certificate is not stored in area **232** and a hash of the particular certificate is not stored in hash **234**, the method may terminate, as shown at **614**. If, however, a hash of the particular certificate is stored in hash **234**, the method may continue to **616**.

[**0067**] At **616**, device imports one of the certificates stored in SC **400** and at **618**, device **200** calculates a hash of the imported certificate. At **620**, device **200** compares the calculated hash to hash **234**. If the calculated hash is not identical to hash **234**, the method may continue to **616** to check other certificates stored on SC **400**, or may terminate, if all certificates on SC **400** were checked and no match was found. Although the flowchart of FIG. **6** shows the device importing the certificates one at a time, the device may import all of the certificates and then check them one at a time.

[**0068**] If, however, device **200** imports a certificate and finds that the hash of the certificate is identical to hash **234**, at **622**, device **200** may store the imported certificate in area **232**. The method may continue to **612**.

[**0069**] At **612**, device **200** generates a random challenge and sends the challenge and an identification of the certificate stored in area **232** to SC **400**. Using the private key paired with the selected certificate, SC **400** signs the challenge at **624**, and at **626**, SC **400** sends the signed challenge to device **200**.

[**0070**] Using the certificate stored in area **232**, device **200** verifies at **628** that the challenge is signed with the private key paired with that certificate. If the challenge is signed with the private key paired with the certificate stored in area **232**, device **200** permits a desired operation, for example, unlocking device **200** for the user to use.

[**0071**] Computer-executable instructions for performing any portions of the above-described method may be stored on a form of computer readable media. Computer readable media includes volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules or other data. Computer readable media includes, but is not limited to, random access memory (RAM), read-only memory (ROM), electrically erasable programmable ROM (EEPROM), flash memory or other memory technology, compact disk ROM (CD-ROM), digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store the desired instructions and which can be accessed by device **108** and/or SCR **104**, including by internet or other computer network forms of access.

[**0072**] Although the subject matter has been described in language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the specific features or acts described above. Rather, the specific features and acts described above are disclosed as example forms of implementing the claims.

What is claimed is:

1. A method in a computerized device, the method comprising:
 - calculating a hash of a certificate imported from a smart card; and
 - storing said hash in said device.
2. The method of claim **1**, further comprising:
 - importing another certificate;
 - calculating a hash of said other certificate; and
 - comparing said hash of said other certificate to said stored hash.
3. The method of claim **2**, further comprising:
 - if said hash of said other certificate and said stored hash are identical, using said other certificate for a particular purpose in said device.
4. The method of claim **3**, wherein said particular purpose is authentication of a user.
5. The method of claim **3**, wherein said particular purpose is encryption of information.
6. The method of claim **3**, wherein said particular purpose is signing of information.
7. The method of claim **3**, wherein said particular purpose is securing web browsing.
8. The method of claim **2**, wherein said device has been upgraded after storing said hash in said device and prior to importing said other certificate.
9. The method of claim **1**, wherein storing said hash in said device comprises:
 - storing said hash in a region of a memory of said device that is unaffected by upgrades to said device.

10. A computer-readable medium having computer-executable instructions thereon which, when executed by a computerized device that is coupled to a smart card reader, result in:

calculating a hash of a certificate imported from a smart card via said smart card reader; and storing said hash in said device.

11. The computer-readable medium of claim 10, wherein said instructions, when executed by said computerized device, further result in:

importing another certificate; calculating a hash of said other certificate; and comparing said hash of said other certificate to said stored hash.

12. The computer-readable medium of claim 11, wherein said instructions, when executed by said computerized device, further result in:

if said hash of said other certificate and said stored hash are identical, using said other certificate for a particular purpose in said device.

13. The computer-readable medium of claim 12, wherein said particular purpose is authentication of a user.

14. The computer-readable medium of claim 12, wherein said particular purpose is encryption of information.

15. The computer-readable medium of claim 12, wherein said particular purpose is signing of information.

16. The computer-readable medium of claim 12, wherein said particular purpose is securing web browsing.

17. A computerized device comprising:

a communication interface through which said device is able to couple to a smart card reader;

a processor coupled to said communication interface; and a memory coupled to said processor, said memory to store code which, when executed by said processor, imports a certificate from a smart card via said smart card reader, calculates a hash of said certificate, and stores said hash in said memory.

* * * * *