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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 April 2010 (29.04.2010)

PCT

(10) International Publication Number
WO 2010/048350 A1

(51) International Patent Classification:
G07F 7/10 (2006.01) *G06F 21/00* (2006.01)

(21) International Application Number:
PCT/US2009/061567

(22) International Filing Date:
21 October 2009 (21.10.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12/255,438 21 October 2008 (21.10.2008) US
61/107,232 21 October 2008 (21.10.2008) US

(72) Inventor; and
(71) Applicant : **HABRAKEN, G., Wouter** [NL/US]; 602 E. 42nd Street, Austin, TX 78751 (US).

(74) Agent: **BHARUCHA, Cyrus, F.**; Campbell Stephenson LLP, 11401 Century Oaks Terrace, Building H, Suite 250, Austin, TX 78758 (US).

(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))*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) **Title**: CARD CREDENTIAL METHOD AND SYSTEM

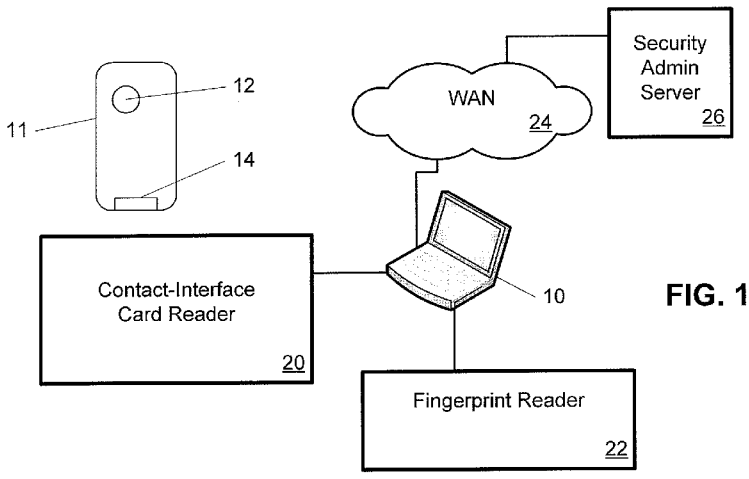

FIG. 1

(57) **Abstract**: In one implementation, a method for providing access to a secure facility includes authenticating the user; generating a card credential, transmitting the card credential to an access card carried by of the user, and transmitting the card key to the access card in a form that is usable by the access card. The generating the card credential includes encrypting the card key using a server encryption key. The card key is usable for a challenge-response interaction during subsequent access requests by the user. In one embodiment, a device includes a first interface, a second interface, a memory, and a processor coupled to the first and second interfaces and to the memory. The processor is configured to receive key-management information via the second interface, and to store the key-management information in a protected portion of the memory as stored key- management information. The processor is also configured to perform a challenge-response authentication interaction via the first interface. The challenge-response authentication interaction is based at least in part on the stored key-management information. The device is configured to prevent data in the protected portion of the memory from being modified in response to information received via the first interface.

WO 2010/048350 A1

Card Credential Method and System

BACKGROUND OF THE INVENTION

Related Applications

[0001] This application claims the benefit under 35 U.S.C. § 119(e) of U.S. Provisional Patent Application No. 61/107,232, titled "Dual-Interface Key Management," filed on October 21, 2008, and naming G. Wouter Habraken as inventor. This application is also related to U.S. Patent Application No. 12/255,438, titled "Card Credential Method and System," filed on October 21, 2008, and naming G. Wouter Habraken as inventor. The aforementioned applications are hereby incorporated by reference herein, in their entirety and for all purposes.

Field of the Invention

[0002] The present invention relates to secure access techniques, and more particularly to authentication using physical devices such as access cards with two or more communication interfaces.

Description of the Related Art

[0003] There are currently several widely used contactless communications technologies, including those defined by the International Organization for Standardization (ISO) in ISO 14443 "Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards," as well as several technologies used with radio-frequency identification (RFID) tags. These technologies allow devices such as access cards, credit cards, passports and product tags to communicate with specialized readers to provide information about the people or products they are associated with.

[0004] For example, some access card technologies assist users with authenticating themselves to a door for the purpose of opening the door. Examples include the Mifare® products produced by NXP Semiconductors. Another technology, the MasterCard® Paypass™ system, assists users with paying for purchases using a contactless interaction. And many different types of RFID allow the tagging of products and pallets for the purpose of tracking their process through supply chains. More and more devices are now integrating these contactless communication technologies. Because of their physical limitations, however, contactless interfaces have thus far found only limited use in secure authentication techniques. For example,

the communication capacity ("bandwidth") and power required to perform a public-key cryptographic operation is generally not available in unpowered contactless smart cards.

SUMMARY

[0005] Described herein are tools and techniques for managing and using access cards that have two or more communications interfaces. In one embodiment, a method includes receiving key-management information onto an access card that has a first interface, a second interface, and a memory. The key-management information includes a key to be used in making access requests such as requests by a user to enter a secure area, or to log in to a secure computation server. The key-management information is received through the second interface. The access card is configured so that the memory cannot store data that is based on information received through the first interface. The method further includes storing the key-management information in the memory, generating an access request based at least in part on the key-management information as stored in the memory, and transmitting the access request from the access card through the first interface.

[0006] In various implementations, the first interface is a contactless interface, while the second interface is a contact interface. The method can additionally include receiving authentication requests from a provider of the key-management information. The authentication requests comprises data strings that are formatted to serve as challenges in a challenge-response authentication system. In various implementations of the method, the challenge-response data strings can serve as vehicles for carrying the key-management information.

[0007] In one embodiment, a device includes a first interface, a second interface, a memory, and a processor coupled to the first and second interfaces and to the memory. The processor is configured to receive key-management information through the second interface, and to store the key-management information in a protected portion of the memory. The processor is also configured to perform a challenge-response authentication interaction through the first interface. The challenge-response authentication interaction is based at least in part on the key-management information as stored in the protected portion of the memory. The device is configured to prevent data based on information received through the first interface from being stored in the protected portion of the memory. In various implementations, the processor includes hardware configured to prevent access from the first interface to the protected portion of the memory.

[0008] The device can be deployed as a physical-access card or other system, such as a mobile communications device that has two interfaces. In one example, the first interface is a near field communication (NFC) interface and the second interface is a mobile telephony interface on the mobile communications device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] A more complete understanding of the present invention and advantages thereof can be acquired by referring to the following description and the accompanying drawings, in which like reference numbers indicate like features.

[0010] FIG. 1 illustrates an example of an environment in which an access card obtains an access key through a contact interface.

[0011] FIG. 2 illustrates an example of an environment in which the access card from FIG. 1 uses the access key for a transaction through a contactless interface.

[0012] FIG. 3 is a flowchart of a process for managing and using keys with a dual-interface access card.

[0013] FIG. 4 illustrates an example of an environment in which a device with two communications interfaces manages and uses key-management information

[0014] FIG. 5 illustrates an example of an environment in which a user enrolls an access card.

[0015] FIG. 6 illustrates an example of an environment in which the access card is used with a card reader to gain access to a secure area.

[0016] FIG. 7 illustrates an example of information flow during the enrollment operations from FIG. 5.

[0017] FIG. 8 illustrates an example of information flow during a first phase of the access request from FIG. 6.

[0018] FIG. 9 illustrates an example of information flow during a second phase of the access request from FIG. 6.

[0019] FIG. 10 illustrates an example of information flow during a third phase of the access request from FIG. 6.

[0020] FIG. 11 illustrates an example of a process used in an access control environment.

[0021] FIG. 12 illustrates an example of details of some of the operations illustrated in FIG. 11.

DETAILED DESCRIPTION

[0022] One challenge for designers of contactless devices, and the systems that use them, is to protect the devices from unauthorized duplication. Another challenge is ensuring the privacy of the information that is stored in the contactless devices. One issue is that the contactless nature of the device can severely limit the interaction time and processing cycles available for executing protective security processes. The security of contactless systems would be significantly enhanced if the lifetime of the keys or other sensitive information on the card were systematically limited to a time span that is much shorter than the usable lifetime of the contactless device. The cryptographic keys on the devices (and related readers) could then be changed for each project and renewed regularly and frequently over the lifetime of the devices.

[0023] For a variety of technical and business reasons, previous systems rarely enforce such discipline. Setting or changing the keys on contactless devices generally requires a dedicated card "writer." Because the ability to change the keys can be used for malicious purposes (a bad actor could use the writer to duplicate a valid card), vendors make it very difficult to obtain the required writer. As a result, contactless devices like cards typically use only a single key that must secure the card contents throughout the expected lifecycle of the contactless device. Because the keys on contactless devices are hard to change, they are often shared across multiple buildings or even multiple campuses. This means that when a device is hacked, or a key is exposed, the results are often a systemic failure of the project's security.

[0024] A method and system are presented for managing the keys on a dual- (or multi-) interface device. One example of such a device is a smart card that has both an ISO 14443 contactless interface and a contact interface such as a standard interface conforming to ISO 7816 "Identification Cards - Integrated Circuit Cards with Contacts."

[0025] Key management involves the functions relating to the key lifecycle(s) of the device keys, as well as the management of the security properties related to the keys that are managed. Key management includes, for example, loading, refreshing, and generating keys, setting usage and access rules for a particular key (e.g., allowing that key to be used by one application, but not another), setting and changing personal identification numbers (PINs), user passwords, or userids, or similar information that is required to use the keys, setting the number

of uses of a key before a particular event (such as key blocking) occurs, as well as unblocking PINs and keys.

[0026] A dual-interface device is a device that has two (or possibly more) logical interfaces for communicating with a reader. For example, the two interfaces can be physically distinct components, and/or can use different physical communications protocols. The two interfaces can, for example, have significantly different properties of available bandwidth, length of sessions, stability of the connection, and/or predictability of the connection. In one example implementation, a dual-interface device is a smart card (or other device) with both an ISO 14443 contactless interface and an ISO 7816 electronic-contact interface. Another example implementation is a device with both an ISO 7816 interface and a USB interface (both using electronic contacts). Yet another example implementation is a card with that has a single hardware interface, but uses two distinct data protocols. For example, such a dual-interface device could be achieved using a SmartMX® card that uses a single 14443 contactless interface to communicate both (a) with a Mifare reader (e.g., for opening doors, using a relatively fast, somewhat unpredictable transaction with low bandwidth) and (b) to a desktop station. The device can communicate with the desktop station through, for example, a PC desktop card reader in which the card can sit for relatively long periods of time, and with which the card can take advantage of smart card ISO 7816 application protocol data unit (APDU) communications, high bandwidth, and long predictable sessions.

[0027] FIG. 1 illustrates an example of an environment in which a dual-interface access card 11 obtains an access key through a contact interface 14. A user of the access card can then utilize the card, loaded with the access key, to gain access to secure services, such as a secure physical area protected by an access-card lock on a door. As discussed below, the access key is typically a temporary access key, with a limited lifetime. The contact interface enables an embedded processor within the access card to communicate with other devices such as a portable computer 10. This communication is carried through a portable contact-interface card reader 20 into which the access card can be inserted. Card reader 20 can be connected to portable computer 10 through an interface such as universal serial bus (USB) interface. Alternatively, a card reader can be directly installed in portable computer 10. In addition to contact interface 14, access card 11 also has a contactless interface 12, discussed below.

[0028] In this environment, access card 11 can obtain the access key from a remotely located security administration server 26. Administration server 26 communicates with portable computer 10 though a network 24 such as the Internet or other wide-area network (WAN). Portable computer 10 then loads the access key onto the access card through the card reader.

Before transmitting the access key, the administration server can require the user of the portable computer to verify that he or she is an appropriate user, for example, by entering a userid and password. Alternatively, or in addition, the administration server can require the entry of some biometric data, such as a through a portable fingerprint reader 22 connected to portable computer 10.

[0029] The administration server can also require the access card to verify that the access card is an appropriate access card. This verification can be performed, for example, using an authentication procedure based on a public key infrastructure (PKI). In one implementation, the access card is embedded with a public-private key pair. (This embedded key pair can in general be unrelated to the access key that access card 11 is attempting to obtain from the administration server 26.) The key pair can be generated and stored by the embedded processor within access card 11 when the access card is initially activated and registered by a card manufacturer, or by a card administration service. At that time, the public-key portion of the key pair can be read out from the access card and provided to relevant organizations, such as the owner of administration server 26. The private-key portion of the key pair remains securely locked within access card 11. Typically, this key pair is used throughout the lifetime of access card 11.

[0030] In the scenario illustrated in FIG. 1, administration server 26 can use the public key for access card 11 to pose a challenge to the access card. For example, administration server 26 can generate and encrypt the random message with the public key of access card 11. Administration server 26 then transmits the encrypted random message as a challenge to access card 11. The access card receives this message through contact interface 14.

[0031] Contact interface 14 provides a relatively large communication capacity for access card 11. Additionally, contact interface 14 supplies power to the embedded processor in access card 11. Using this power supply and the available communication capacity, access card 11 decrypts the challenge to recover the original random message that was generated by administration server 26. By transmitting the original random message (or a hash thereof) back to administration server 26, access card 11 demonstrates that it is in possession of the private-key counterpart of the public key used by the administration server. To the extent that administration server 26 has confidence in the PKI distribution and protection of the public-private key pairs, the administration server can then have confidence that it is in communication with an appropriate access card 11.

[0032] After the user has been verified through the appropriate user-authentication procedure, and after the access card has been verified through the appropriate card-authentication

procedure, administration server 26 can transmit the access key to access card 11. In this example, the access key is communicated from administration server 26 via network 24, portable computer 10, and card reader 20 to access card 11.

[0033] FIG. 2 illustrates an example of an environment in which access card 11 from FIG. 1 uses an access key for a transaction through contactless interface 12. In this example, an access key has already been loaded into access card 11 (e.g., using the techniques described above with regard to FIG. 1). The access key allows a user of the access card to enter a secure area behind a door 29. To open the door, the user presents access card 11 to a contactless card reader 28. Card reader 28 interacts with contactless interface 12 using non-contact communication. For example, card reader 28 and contactless interface 12 can be configured to use a 13.56 MHz wireless link with the ISO/IEC 14443 standard. During this interaction, access card 11 uses the access key stored therein to respond to a challenge posed by card reader 28. By responding to this challenge, access card 28 authenticates itself to card reader 28, which then opens a door lock 27. The user is thus permitted to enter the secure area protected by door 29.

[0034] The interactions discussed above illustrate various features of the dual interfaces on access card 11. Contactless interface 12 enables quick easy access by a user, who may merely wave the access card in front of a card reader to open a door. However, contactless interface 12 can suffer from low-bandwidth and low-power issues, especially if access card 11 does not have an on-board battery. Thus, contactless interface 12 is generally not able to support high-security transactions, such as PKI authentication.

[0035] Moreover, contactless interfaces can be relatively vulnerable to eavesdropping attacks when they are in use. In addition, contactless interfaces can be vulnerable to spoofing attacks, in which a malicious user surreptitiously attempts to interrogate the contactless interface. Similarly, a malicious user may attempt to disable an access card by submitting a false access key through the contactless interface. In anticipation of such attacks, some wireless cards are configure a to disable themselves if they detect malicious activity (such as repeated failed attempts to communicate through the contactless interface). Unfortunately, this defense leads to another type of attack: a malicious user can use this defense mechanism to potentially disable the access card by presenting the access card with attack-like communication attempts.

[0036] To protect against such attacks, access card 11 can be configured to merely ignore any communications that are deemed to be attack attempts. In addition, access card 11 can be configured so that the embedded key pair and other high-security information is not readable or otherwise accessible through the contactless interface. Thus, this sensitive information is

protected from attacks through the contactless interface. At most, the access key that is used for opening door 29 is vulnerable to attack through contactless interface 12. This possible vulnerability can be ameliorated by configuring the access key with a relatively short life time, such as a few hours or a few days. Devices that respond to the access key, such as card reader 28, can be configured to ignore the access key if it has not been recently updated (e.g., replaced with a more current access key).

[0037] The updating can occur when the access card is inserted into contact-interface card reader 20. Access card 11 can then be updated with a new key after undergoing the higher-security measures discussed above with regard to FIG. 1.

[0038] These higher-security measures are enabled by card reader 20, which supplies power and comparatively high-bandwidth communications to access card 11. As discussed above, these interactions can utilize higher-security features of access card 11, such as an embedded PKI key pair, which is assigned a comparatively long life time. In various implementations, access card 11 can be configured so that these higher security features are available only through contact interface 14, thereby protecting these long-lifetime features from attacks through contactless interface 12. (Conversely, in certain implementations, access card 11 can be configured such that interactions that use the access key are available only through contactless interface 12.)

[0039] FIG. 3 is a flowchart of a process 30 for managing and using access keys with a dual-interface access card. In this example, process 30 includes two sets of operations. An access card is loaded with a temporary access key through a contact-interface card reader in block 31 (e.g., card reader 20). Block 31 includes acts 32 and 33, which can be used, for example, for the operations discussed above with relation to FIG. 1. The access card is then used with a different card reader (e.g., card reader 28) to gain access to a secure facility in block 35. Block 35 includes acts 36, 37, 38, and 39, which can be used, for example, for the operations discussed above with relation to FIG. 2.

[0040] After being loaded with a temporary access key in block 31, the access card can be used to access a secure area or other secure facility. This access can be repeated during the built-in life span of the access key, as indicated by a looping arrow for block 35. From time to time (e.g., occasionally or on a set schedule), the access keys can be updated, either voluntarily or as required by a security protocol. This updating is indicated by a looping arrow in FIG. 3 that returns from block 35 to block 31.

[0041] Block 31 begins with act 32, in which the access card is authenticated. The authentication can use, for example, a challenge-response PKI protocol such as described above. In conjunction with the authentication of the access card, a user of the access card may also be authenticated, for example by a password or biometric measurement. In act 33 a temporary access key, having a relatively short life time, is stored on the access card through the contact interface. Additional key-management information can also be stored on the access card in conjunction with the keys.

[0042] The access card can then be used in block 35 to gain access to a secure facility using a contactless card reader. (In various implementations, access can also be granted to other facilities by using a contact-interface card reader). The card reader used in block 35 is generally deployed at a different location from the card reader used in block 31. In various implementations, the card reader used in block 35 is mounted next to a door or at a security checkpoint.

[0043] Block 35 begins with act 36, in which a user holds the access card near a card reader, or otherwise presents the access card to the card reader. In one implementation, the card reader continuously broadcasts an RF signal. The access card detects the signal when it is within close range (a few inches to a few feet) of the card reader, and transmits an RF response to inform the card reader of the presence of the access card. In act 37, the card reader transmits a challenge to the access card. In act 38, the access card returns a response to the card reader. The response is based on the challenge and on the access key that was stored on the access card in act 33. In act 39, the communications between the card reader and access card are evaluated to decide if access should be granted to the secure facility.

[0044] The techniques described above can also be used in implementations with two interfaces that are both contact interfaces, or that are both contactless interfaces. In general, a dual-interface device can use a first interface (e.g., an ISO 14443 contactless interface) for interactions such as authentication or other interactions that make use of keys or other sensitive information stored on the device. A second interface (e.g. an ISO 7816 electronic-contact interface) can be used for the management of the keys that are used by the first interface, or management of applications that use the first interface. It is contemplated that the second interface can be used (e.g., for key updates or other management) to support applications that use the first interface on a dual-interface device.

[0045] Once the keys are put in place using the second interface of an access card, the first interface on the same card can be used for interactions that employ those keys. For example,

a Mifare application can authenticate the card by using the keys loaded into the card. In some implementations, key management can employ tools that do work through the first interface (e.g., a contactless interface) on a device to set or change the keys for that device. Such implementations typically provide another "administration" key. However, it is also contemplated that dual-interface management can also be used with classes of devices that do not assist with, or do not allow, key management through the first (contactless) interface.

[0046] In various implementations, the second interface of a dual-interface device provides functionality that is different from the first interface, or is used with different applications. For example, a dual-interface smart card's contact interface can be used to gain logical access to a computer. Communication through the second interface can be used to execute a cryptographic function (such as a 2048 bit RSA authentication) for remote authentication by an access server. The access server then allows the user to log on to a computer. Such an authentication typically requires the user to provide a PIN (or other pass code) or a fingerprint (or other biometric authentication) and is therefore more secure than the presentation of a card to a reader.

[0047] It is contemplated that a function or application used by the second interface can be used to trigger a key-management event for the keys used by the first interface. For example, the card may be used for a successful authentication of the card (e.g., using relatively higher-security measures and keys, such as embedded PKI keys) when the second interface makes a logical connection to an organization's remote server. After the successful authentication, the remote server can automatically update or otherwise change the short-term keys or security policies that are stored on the card for use by the first interface. This update may then enable future physical access for the user through the organization's security doors, with challenge-response interactions between the card's first interface and card readers mounted next to the security doors. Alternatively, or in addition, this update may refresh the user's credentials for subsequent data access through the second (or first) interface. Similarly, this automatic update may revoke or limit future rights of physical access or data access.

[0048] One result of this feature may be the secure binding of one type of authentication (such as certificate-based authentication for logical access through a contact interface) with another (such as key-based authentication for physical access through a contactless interface). Another result may be that security-relevant communications through the second interface can be used to affect the policies for applications that use the first interface. In addition, another result may be that secure communication channels which use the second interface can supply information to be used by applications on the device that employ the first interface.

[0049] A variety of uses and implementations are contemplated for such dual-interface management, as will be appreciated from the following examples of application scenarios.

[0050] In a first illustrative scenario, dual-interface access card 11 from FIGs. 1 and 2 is used by an employee of an organization. When the employee is at is at her desk in her office, she can logs in to her computer (e.g., portable computer 10) and a security system in the organization confirms her location (e.g., through the use of IP address / Device MAC and/or 802.1X authentication chaining). Then, using contact interface 14, the security system updates a set of temporary access keys the on the employee's access card 11. The temporary access keys are available to applications that use contactless interface 12, including a physical-access authentication system for the organization. In this example, the updated keys have a life time of only 48 hours. When the user returns to her office building the next day, she presents access card 11 to a card reader (e.g., card reader 28) next to a door at the building entrance of the organization. The physical-access authentication system interacts with the card reader through contactless interface 12, and uses the updated keys to confirm the user's identity as a person who was recently within the building. If the user should lose her card, the updated keys expire within 48 hours; that is, the physical-access authentication system will not honor them after that period.

[0051] In various implementations, the physical-access authentication system can update the first interface keys (which in this use case are used to provide physical access), and can also apply new security policies, for example by increasing a "remaining number of uses" counter (which forces the user to undergo some form of re-authentication when the counter reaches 0).

[0052] An extensible authentication protocol (EAP) authentication method, as defined in RFC 3748, can also be used with a dual-interface device. For example, such a protocol can be used to integrate user authentication for logical access through the second interface of the dual-interface device with the provisioning of keys and policies for the first interface of the dual-interface device. One benefit of such an implementation can be that it enables the access system to remotely refresh keys or policies, and obviates the need for users to update their cards at a particular physical location. Another possible benefit is that such a process flushes out cards that are lost, stolen, or otherwise not used for a period of time.

[0053] In a second illustrative scenario, the same user visits a branch office of her organization—where she has not been before. She tries to enter the building by presenting access card 11 to a contactless reader next to the entrance. This fails because the user is not yet approved with keys for this branch office. The user then uses her card to log in at a kiosk (which uses contactless interface 14) in the entrance hall, and provides her fingerprint. The security

system determines that the user is valid, based on the fingerprint. The user is then is approved for entry (for example, by credentials encoded in a digital certificate on her card, or through a back channel operation). The system loads appropriate temporary keys (and/or credentials), specific to this branch office, onto access card 11 through the contact interface in the kiosk. The user once again presents her card to the contactless door reader. This time access card 11 is recognized and the door is opened, allowing the user to enter the branch office building.

[0054] In a third illustrative scenario, the same user is now at a location at the branch office where she is not authorized to be (for example a computer server room). The user plugs her laptop computer (e.g., portable computer 10) into the server room's local area network and attempts to log in to the network using access card 11. Access card 11 is plugged into her laptop computer through a portable contact-interface card reader (e.g., card reader 20). The network access system rejects the login attempt, and at the same time voids access card 11 by revising key-management information stored on access card 11. For example, the network access system may change the security policies for contactless interface 12, which is used for the user's physical access in the organization. When the user returns tries to enter another locked room with her card, entry is refused, and a security guard for branch office is alerted.

[0055] FIG. 4 illustrates an example of an environment in which a device 41 with two communications interfaces manages and uses key-management information. In this example, the device is a cell phone that has one radio transceiver in a cellular telephone interface, and also has another radio transceiver in a near field communication (NFC) interface. The cellular telephone interface is used to obtain keys and other key-management information from a security administration server 56 through a cellular link 42. The NFC interface communicates with a wireless card reader 48 through a short-range radio link 44. Card reader 48 uses the obtained keys to open a door lock 47 through wireless card reader 48.

[0056] A fourth illustrative scenario uses the communication links shown in FIG. 4. There is a fire at an office building in the middle of the night. A first responder arrives at the building. He uses his mobile telephone (e.g., device 41 from FIG. 4) to call the emergency-access number displayed at the entrance of the building. A security department at the mobile-phone service provider responds to the call and uses the service provider's caller authentication procedures to confirm that the caller is indeed a first responder. The security department then sends access keys from the security department's server, e.g., by short message service (SMS) over cellular link 42, to the first responder's mobile telephone. The access keys are received by an application on the first responder's mobile telephone through SMS software. The first responder then presents his telephone's NFC interface to a physical access reader at the building

entrance's door. The NFC interface communicates the received access keys through, and the door opens.

[0057] In other implementations, other communications protocols can be used for communicating between the mobile telephone and the physical access reader. For example, a Bluetooth or 802.11 communications link can be used between these two devices.

[0058] In the above example, the first responder's mobile telephone enables a binding of two domains: the authentication between the mobile telephone and the physical access reader is bound with the authentication between the mobile telephone and the security department. That is, the physical access reader effectively understands the first responder to have been authenticated by the procedures used by the security department, despite a lack of direct back-channel communication between the physical access reader and the security department.

[0059] In various implementations, contact interfaces can generally provide communication through mechanical contacts between portable devices and device readers. Similarly, contactless interfaces can generally provide communications through wireless communication elements (e.g., antennas, capacitive coupling elements, inductive coils, other inductive coupling elements, or combinations thereof) in portable devices and device readers. In various scenarios, contact interfaces are interfaces that primarily use current signals (electrons) for inter-device communications while contactless are interfaces that primarily use electromagnetic wave signals (photons) for inter-device communications.

[0060] In some implementations, a contact interface can connect a portable device to an off-card power source, while a contactless interface can not. In other implementations, a contact interface can more readily connect a portable device to an off-card power source than can a contactless device. These considerations are usable for designers of dual-interface devices. For example, a designer may elect to use a contact interface for interactions that require relative lengthy interaction and/or power-intensive calculations by the portable device, such as key management or public-key cryptography. Conversely, a designer may elect to use a contactless interface for interactions that need only brief interactions and/or low-power calculations by the portable device, such as symmetric-key authentication.

Combined Secure-Session Initiation and Key Transmission

[0061] Various security protocols include the transmission of a key over a network to a card. For example, the above discussion of FIG. 1 included a transmission of a key from administration server 26 to access card 11 via a network and a card reader 20. (Similarly, FIG. 5,

discussed below, shows an example in which a card credential is communicated from trusted server 130, through a data network and card reader 120, to access card 110.) A computing device, such as portable computer 10, is configured to (1) communicate with the remote server and receive a transmission that includes the key, (2) parse the transmission to obtain the key, and (3) initiate a communication with access card 11 and pass the key on to access card 11. Appropriate software for these operations can be installed on portable computer 10.

[0062] Operations (1) and (3) can be performed through various forms of standard communications software running on portable computer 10. For example, network interface drivers and web browsers on portable computer 10 can be used to support communication with administration server 26. Similarly, a card-reader driver and interface software can enable portable computer 10 to communicate with card reader 20. However, operation (2) can require customized software to decrypt and parse the data received from administration server 26. In one implementation, a specialized application is installed on portable computer 10. The specialized application reaches administration server 26 through the network interface driver on portable computer 10. Similarly, the specialized application reaches card reader 20 through the card-reader driver. The specialized application is configured to communicate with corresponding modules on administration server 26, obtain the key from those communications, and pass the key to access card 11.

[0063] Generating such a specialized application poses a challenge to system designers. This challenge can be exacerbated in environments where the application needs to be deployed in a number of versions, e.g., for different operating systems that can be used by portable computers and other computing devices. The challenge of generating the specialized application for operation (2) is accompanied by a second challenge: how to deploy the specialized application. A large number of users may need to install the specialized application on their respective portable computers. The installation and maintenance of the application can impose an ongoing overhead for support staff. And yet a third challenge arises: to protect the specialized application and its communications from eavesdropping by malicious programs that may surreptitiously be running on portable computer 10.

[0064] It has been found that these three challenges can be addressed by the following design approach. Instead of terminating the communication from administration server 26 only on portable computer 10, at least some of the communication from administration server 26 is terminated on access card 11. That is, portable computer 10 does not receive and parse all of the payload communications from administration server 26. Instead, portable computer 10 creates and supports a conduit for communications between administration server 26 and access card 11.

This conduit passes through WAN 24, portable computer 10, and card reader 20. Such a conduit can be established without specialized software.

[0065] In various implementations, this conduit can be established using relatively standard web-browser software and a card-reader driver running on the portable computer. For example, the web-browser software on portable computer 10 can receive an applet from administration server 26. This applet is executed by the web browser to receive a data stream from administration server 26 and pass it to access card 11 through the card-reader driver. The applet also sends a return data stream, received from access card 11 through the card-reader driver, back to administration server 26.

[0066] Such configurations simplify the first challenge, of generating specialized software for supporting the communication between access card 11 and administration server 26. The applet is written and made available on a web site on administration server 26 for execution by client web browsers; no specialized applications need to be installed on portable computer 10. This configuration also simplifies the second challenge, of deploying and supporting the specialized software. The applet can be configured such that it is readily deployed by standardized web browsers such as Internet Explorer®, for example.

[0067] Contact interface 14 of access card 11 is inserted into card reader 20 during the communication between administration server 26 and access card 11. Thus, access card 11 can draw power from the card reader during this communication. The power received from the contact-interface card reader allows access card 11 to perform relatively more intensive computations during the communication. With this supply of power, access card 11 establishes a secure channel over with administration server 26. For example, access card 11 and administration server 26 can use a key-negotiation protocol to establish a session key for the secure channel. This secure channel protects the channel from eavesdropping, including eavesdropping by malicious applications that may be running on portable computer 10. The secure channel therefore also addresses the third challenge, of securing the information transmitted to and from access card 11.

[0068] Beyond these three possible benefits, it has also been found that a secure channel between access card 11 and administration server 26 can simplify the transmission of key-management information to the access card. To start, the payload information—keys and other key-management information—does not need to be parsed and recognized by any intermediate devices (such as portable computer 10 or card reader 20). Moreover, the secure channel is generally initiated with a transmission of some random data, such as a string of challenge data,

from the administration server to the access card. The challenge data can be part of a challenge-response PKI protocol, for example as part of establishing a secure socket layer (SSL) link. The access card would reply by using an internal private key to generate a response to the challenge, and then return the response to confirm that the access card is bona fide. This challenge-response operation can be repeated multiple times during operation of the secure channel, each with a different version of the challenge string.

[0069] Instead of using purely random data to generate the challenge string, administration server 26 can include an encrypted version of the short-term access keys, or other key-management information, in a second or subsequent version of challenge string. Thus, the key-management information can be somewhat hidden within one or more of the challenge strings after the access card has been authenticated. In addition, by placing the relevant payload data—the access keys and other key-management information—within the challenge string, the administration server simplifies the operations that need to be performed by the access card (and possibly by the applet running on the portable computer). This simplification arises because no routines are needed to parse any data that is separate from the challenge string; once the payload-laden challenge string (or strings) is received by access card 11, the secure channel can be terminated.

Dual-Interface Card Credential Authentication

[0070] As described above, a dual-interface access card can be used in a variety of environments. The following discussion introduces a credential and associated procedures that can be used with a dual-interface card. In various embodiments, this credential and associated procedures can provide secure authentication for via a contact interface, while enabling convenience for users with a contactless interface. The credential and associated procedures can also be used with dual-contactless interface cards, dual-contact interface cards, and single-interface cards as well.

[0071] Physical-access cards are often used as a security measure for preventing access by unauthorized personnel to a secure area such as an office suite. A simple form of a physical-access card is an access card with a magnetic stripe that stores a digital password. When a user approaches a locked door and presents the access card to a card reader, the card reader reads the password from the magnetic stripe. The card reader may communicate with a central server to confirm the password, and/or to check if the user is listed in an approved access control list. The central server can then unlock a door for the user.

[0072] One weakness of this simple system is that if the password from the magnetic-stripe can be read and reproduced by a malicious party, then the malicious party may be able to use the password to gain unauthorized access. One approach for strengthening the security measures is to use access cards that are "smart" cards, with a built-in processor and memory. A password, or key, is stored into the memory in such a manner that it can be read by the built-in processor, but cannot be read by a malicious party.

[0073] When a smart card is used to gain access to a secure area, the smart card can respond in real time to a challenge received from a card reader. The card reader typically uses random numbers to generate challenges that are unique: the challenges include data that are different from one access attempt to another. The smart card performs a calculation using its internally stored key and the data received from the card reader, and transmits a response, based on that calculation, back to the card reader. The card reader examines the response to confirm that the smart card possesses the correct key. Access is granted only if the smart card returns an acceptable response to the challenge sent by the card reader. This challenge-response interaction protects the key on the smart card: the key itself is not transmitted as part of the communications between the smart card and the card reader.

[0074] Such smart cards are generally more difficult to reproduce or simulate than a magnetic-stripe card. One of the concerns in such smart card authorization systems is that a malicious party may be able to deduce the internal key or otherwise "break" the cryptographic features in the calculations performed by the smart-card, and thereby provide acceptable responses to challenges from card readers. One approach to avoiding such attacks is to increase the sophistication of the challenge-response calculations performed by the smart-card. Such an approach generally imposes some additional cost, such as an increased processing power for the smart card. System designers, therefore, must generally make trade-offs between various costs and cryptographic security.

[0075] Various tools and techniques are presented for authenticating an access card used for access to a secure facility. In various implementations these tools and techniques can be used to control physical access to offices, office suites, buildings, data centers, or other secure areas. Alternatively, or in addition, these tools and techniques can logical access (e.g., login access or data read/write access) to computer systems, databases, or other secure computing equipment or information. Similarly, these tools and techniques can be applied to control financial access to deposit accounts, credit accounts, or other financial resources.

[0076] In some implementations, these tools and techniques can interweave two different cryptographic techniques, such that a computationally less-intensive protocol is performed on an access-card processor, and is linked with a computationally more-intensive protocol that is performed on a secure server. In some implementations, the less-intensive protocol can be used on access cards during a contactless interaction with a card reader. In some implementations, the less-intensive protocol is a symmetric encryption protocol, and the more-intensive protocol is a public-key protocol, which can be better utilized in interactions with contact-interface readers.

[0077] It is contemplated that in some implementations these tools and techniques can use two linked cryptographic protocols; one cryptographic protocol is executed on an access card using keys with relatively short life cycles, and the other cryptographic protocol is executed on a secure server using keys with relatively longer life cycles.

[0078] In some implementations, these tools and techniques provide a stateless security system that enables secure access without needing to consult a centralized access control list at the time that access needs to be granted.

[0079] In some implementations, these tools and techniques enable administrators to upgrade the security of some users, without necessitating a wholesale replacement of access cards for all users. In some implementations, these tools and techniques enable administrators to upgrade the security of some secure areas, without necessitating a wholesale replacement of card readers for all the secure areas in an organization.

[0080] In one implementation, a method for enabling a user to access a secure facility includes authenticating that the user is indeed an acceptable person (or entity) to have the access, generating a card credential, transmitting the card credential to an access card in the possession of the user, and transmitting the card key to the access card in a form that is usable by the access card. The generating the card credential includes encrypting the card key using a server encryption key. The card key is usable for a challenge-response interaction during subsequent access requests by the user.

[0081] The card credential can be used to authenticate the access card by checking the validity of a challenge-response interaction. Thus, in some implementations, the method can further include receiving a request for authentication that includes the card credential and a candidate response, and obtaining the card key from the card credential using a server decryption key. The candidate response can be a response that was provided by the access card during a challenge-response interaction as part of an access request by the user. The method can additionally include generating a response data based on at least the card key, a challenge data,

and a card authentication protocol; comparing the candidate response to the response data; and generating an authentication output based at least on the comparing.

[0082] In various implementations, the generating the card credential is performed by a first server computer as part of an enrollment procedure following the authentication of the user, and the receiving the request for authentication is performed by a second server computer (which can be different from the first server computer, and possibly disconnected from the first server computer) following the access request by the user.

[0083] In yet another implementation, a method includes receiving a request for authentication, including a card credential and a candidate response; decrypting at least a portion of the card credential using a server decryption key to recover a card key; generating a response data based on at least the card key, a challenge data that was provided to an access card during a challenge-response interaction, and a card authentication protocol; comparing the candidate response to the response data; and generating an authentication output based at least on the comparing.

[0084] FIG. 5 shows an example of an environment in which a user 115 enrolls an access card 110. An "out-of-band" authentication process is employed to establish that user 115 is a legitimate user, authorized to gain access to an organization's secure area. This out-of-band authentication is some technique by which a gate-keeping administrator 125 of the secure area confirms that user 115 is a person to be trusted with the access to the secure area. In various implementations, the access card enrollment is not completed unless user 115 passes the out-of-band authentication.

[0085] In the depicted example, administrator 125 is a security guard at an organization's front security desk. The security guard recognizes user 115 by sight as a trusted member of the organization. Other measures can be used instead of, or in addition to, this simple recognition. User 115 may need to provide a photo identification or a biometric identification (fingerprint, voice recognition, retinal scan); speak, write, or type a password or personal identification number (PIN) code; or respond to interview questions, or other measures, or some combination thereof. Similarly, the security guard or other administrator can consult a database to confirm that the user's information matches the organization's records, and that the user is indeed approved for access to the secure area.

[0086] After the out-of-band authentication has been successfully completed, the user's access card 110 is provided with a digital credential. The credential, discussed below, is generated by a trusted server 130, and is communicated over a data network or other

communications link to a card reader 120 that is located within convenient range of the user. Card reader 120 loads the credential onto access card 110 through a contact-interface link 170, which uses radio waves to transmit the credential to access card 110. For example, contact-interface link 170 can use the ISO/IEC 14443 standard and a 13.56 MHz frequency. In other implementations, an access card can receive the credential and otherwise communicate through a contact interface. For example, the card reader and access card can be equipped with contact interfaces that use the ISO 7816 smart card standard. User 115 then carries the access card, loaded with the credential, as a proof that user 115 has undergone the out-of-band authentication.

[0087] FIG. 6 shows an example of an environment in which access card 110 is used with a card reader 220 to gain access to a secure area. A door 250 provides entry to the secure area, and remains locked unless opened by a signal from a door controller system 240 to a door lock 245. Door 250 is typically located at a different location than the card enrollment of FIG. 5. For example, enrollment can be performed at the front security desk of an organization's building. Door 250 can be located in a different section or on a different floor of the building, or even in a different location altogether, such as a different building or a different city.

[0088] In this example, user 115 uses access card 110 to request that door 250 be unlocked. User 115 holds access card 110 in close proximity to card reader 220, which is typically mounted near door 250. Card reader 220 communicates with access card 110 through a wireless link 270 or a contact interface. Card reader 220 performs a challenge-response interaction with access card 110, and receives the credential from access card 110. Card reader 220 communicates the credential and information about the challenge-response interaction to a trusted server 230. Trusted server 230 can be the same as or different from trusted server 130 from FIG. 5. Trusted server 230 analyzes the credential and the information about the challenge-response interaction. Based on this analysis, trusted server 230 determines whether access card 110 has indeed undergone the enrollment process from FIG. 5.

[0089] If trusted server 230 determines that access should be granted, an appropriate signal is sent from trusted server 230 to door controller system 240, which then signals door lock 245. Door lock 245 then unlocks door 250 for user 115. Trusted server 230 can also communicate an appropriate signal back to card reader 220, which flashes a green light and/or emits a tone or otherwise indicates that access has been approved. If trusted server 230 determines that access should not be granted, trusted server 230 can communicate a different signal back to card reader 220, which can then flash a red light and/or emit a tone or otherwise indicate that access has been denied. Trusted server 230 can also log the failed access attempt by

user 115, and can alert security personnel after an excessive number (one or more) of failed access attempts.

[0090] The above introduction includes two acts of "authentication." The out-of-band authentication (FIG. 5) is an authentication of the user. This first authentication verifies that the user is indeed a person who can access a secure facility. This first authentication must be successfully completed by a user in order to enroll the user's access card. After enrollment, the user can request access to the secure facility (FIG. 6) using the enrolled access card. The decision whether to grant or deny access involves electronic authentication of the access card. This second authentication verifies that the request comes from an access card that has indeed been enrolled.

[0091] FIG. 7 shows an example of information flow during the enrollment operations from FIG. 5. This figure shows trusted server 130, card reader 120, and access card 110 from FIG. 5. Access card 110 includes circuitry for a contact interface 350, a processor 360, and a memory 370. Contact interface 350 enables communication with card reader 120 through contact-interface link 170.

[0092] Processor 360 is coupled to contact interface 350 and to memory 370. Processor 360 obtains power from an off-card supply through contact interface 350.

[0093] After administrator 125 from FIG. 5 has completed the out-of-band authentication for user 115, administrator 125 uses trusted server 130 and card reader 120 to load information onto the user's access card 110. Trusted server 130 generates a card key 310 for access card 110. Card key 310 is a set of data that can be generated, for example, using a cryptographic key generation processes. In alternate implementations, trusted server 130 receives card key 310 from a key source (not shown) using appropriate key distribution procedures. In the illustrated example, card key 310 is unique to the particular key card 110, and/or to the particular user 115. In alternate implementations, each card key is shared among several key cards and/or among several users.

[0094] Trusted server 130 encrypts card key 310 using a trusted server encryption key (TSEK) 320. In various implementations, TSEK 320 is a relatively strong encryption key having a substantially large number of bits and is protected by relatively strong security practices. TSEK 320 is generally not the same as card key 310. For example, TSEK 320 can be accessible only to a limited number of trusted personnel within an organization. In various implementations, TSEK 320 can be a 1024-bit, 2048-bit, 4096-bit, or other-size public key from a public-private key pair. The encryption of card key 310 can correspondingly be performed

using a public-key encryption (e.g., using Digital Signature Standard (DSS), elliptic curve, or RSA algorithms, or others). In various alternate implementations, TSEK 320 can be an 80-bit, 112-bit, 168-bit, or 256-bit, or other-size symmetric key. The encryption of card key 310 can correspondingly be performed using a symmetric-key encryption (e.g., using Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES), Blowfish, Twofish, or Elliptic Curve Cryptography (ECC) procedures, or others).

[0095] Trusted server 130 generates a card credential 330 that includes the encrypted card key. Other information can also be included in the card credential, such as the life cycle of card key 310 (e.g., a lifetime, or expiration time and date, that causes the card key to be obsolete and unusable after a particular duration or point in time), card configuration data 312, and card data 314. In various implementations, these data 312 and 314 include information that is obtained from access card 110, or entered by administrator 125, or received from an access control list, or generated by trusted server 130, or combinations thereof.

[0096] Card configuration data 312 includes a description of access card 110. For example, different types of access cards are capable of performing different types of "on-card authentication protocols" to carry out the challenge-response calculations. The on-card authentication protocols are calculations that generate card responses based on the card key and the received challenge data. In various implementations, card configuration data 312 identifies which type of card is access card 110, and/or identifies which type of authentication protocol(s) can be performed by access card 110.

[0097] Card data 314 can include other types of information regarding access card, such as a name of user 115, an identifier of user 115, names or identifiers for the organizations of which user 115 is a member, a card identifier that is unique to access card 110, information regarding access control lists on which the card identifier is listed, information regarding a security clearance of user 115, information regarding which secure facility (or facilities) user 115 is permitted to access, or restrictions that apply to user 115 regarding time, duration, or escort requirements, or other information, or combinations thereof.

[0098] Depending on the implementation, some or all of these data 312 and 314 can also be encrypted using TSEK 320. It is also contemplated that additional encryption functions can also be used to generate card credential 330, and that various salt, hash, message authentication codes (MAC), and signature data can be included in card credential 330. In the illustrated example, card credential 330 is generated by using TSEK 320 to encrypt a combination of: card

key 310, an expiration date for card key 310, card configuration data 312, and card data 314. As illustrated, these data are locked into card credential 330, protected by TSEK 320.

[0099] After generating card credential 330 in this manner, trusted server 130 transmits card credential 330 to card reader 120 over a data network or other communications link. Card reader 120 in turn transmits card credential 330 via contact-interface link 170 to access card 110. Card key 310 is also transmitted, securely, to access card 110. (It is contemplated that in alternate implementations, a trusted server can initially obtain the card key and/or card data from an access card. In such implementations, it may not be necessary to transmit the card key back to the access card.) Card credential 330 and card key 310 are then stored in memory 370 on access card. Card key 110 is stored in on access card 110 in such a way that it is protected from being readable by a malicious unauthorized user. In this example, enrollment is then complete for access card 110.

[00100] FIG. 8 shows an example of information flow during a first phase of the access request from FIG. 6. This figure shows trusted server 230, card reader 220, and access card 110 from FIG. 6. In this example, access card 110 has completed the enrollment described above with regard to FIG. 5, and is being used to request access to a secure area. A wireless interface 351 enables access card 110 to communicate with card reader 220 through wireless link 270. This communication is used for the challenge-response interaction between card reader 220 and access card 110. In some implementations, wireless interface 351 is a radio-frequency (RF) interface, and communicates with corresponding circuitry (not shown) in card reader 120 using electromagnetic waves. In various implementations, processor 360 and other circuitry in access card 110 are powered by electromagnetic waves received from card readers such as card reader 220. The power circuitry (not shown) can be included within or separate from wireless interface 351. In some implementations, the power circuitry uses inductive coupling and rectification to receive a particular frequency or frequencies of electromagnetic energy from card reader 220.

[00101] In this example, the challenge-response interaction begins after communication has been established between card reader 220 and access card 110. Card reader 220 recognizes that access card 110 has been presented to card reader 110. Card reader 220 then generates a challenge data 410. Alternatively, challenge data 410 can be generated on trusted server 230 and received by card reader 110. Challenge data 410 can consist of or include, for example, a large random number such as a 20-bit, 40-bit, 64-bit, 80-bit, or longer random number. Card reader 110 then transmits challenge data 410 to access card 110 through wireless link 270.

[00102] Access card 110 stores challenge data 410 into memory 370. Processor 360 then retrieves card key 310 and challenge data 410 from memory and executes an on-card authentication protocol using both of these data to generate a card response 415. In various implementations, the on-card authentication protocol is a calculation that includes a one-way hashing function. This calculation generates a hash of card key 310 and challenge data 410. The resulting hash is, or is used to generate, card response 415. In other implementations, the on-card authentication protocol involves a calculation that uses challenge data 410, followed by an encryption, signature, or MAC operation with card key 310.

[00103] The authentication protocol performed by processor 360 is designed to demonstrate that the access card has possession of the card key. To the extent that possession of the card key indicates that the user of the access card has undergone the enrollment process from FIG. 5, the on-card authentication protocol establishes that the user of the card key has previously undergone the out-of-band authentication process from FIG. 5.

[00104] The on-card authentication protocol is designed to execute without compromising the security of the card key. Thus, the on-card authentication protocol preferably generates the card response in such a way that a malicious party cannot easily determine card keys by analyzing card responses. Various examples of hashing functions are contemplated for use in these calculations, such as Message-Digest Algorithm 5 (MD5), or a Secure Hash Algorithm (SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512), or others. Alternatively, or in addition, various encryption functions are also contemplated for use in these calculations, such as DES, 3DES, AES, Blowfish, Twofish, or ECC.

[00105] When selecting an authentication protocol (or protocols) for processor 360, a designer can elect to balance various considerations. For example, high cryptographic security can increase processing overhead for processor 360. At some point, the processing overhead can be unacceptable, especially in implementations where processor 360 is powered by electromagnetic waves received from card reader 220. Such implementations provide convenience to a user: the user can "swipe" the access card by briefly holding or waving (for less than approximately 0.2, 0.5, 1.0, 2.0, or 5.0 seconds, for example) the access card close to (e.g., within a few inches or a few feet) of the card reader. However, these implementations require processor 360 to perform the on-card authentication protocol, and the accompanying communication with the card reader, in a relatively short time, and with relatively little power available. In implementations where an access card is powered by a small on-board battery, the power constraints can be less important, but the short time constraints can still apply. In these and other implementations, power and time constraints can limit the complexity of the on-card

authentication protocol. Similarly, these constraints can limit the length of the card key, the length of the challenge data, and/or the length of the card response to the challenge data. In various implementations, designers can avoid using high-overhead algorithms, such as some public-key protocols, in the authentication protocol that is performed by processor 360. Moreover, designers can refrain from processing the card credential 330 in the on-card authentication protocol.

[00106] After processor 360 generates card response 415, access card 110 transmits card response 415, along with card credential 330, to card reader 220. Card reader 220 receives these data from access card 110 via wireless link 270. In the illustrated example, card reader 220 does not itself analyze the results of the authentication protocol. Instead, card reader 220 requests assistance from trusted server 230. Card reader 220 transmits a request for authentication 450 to trusted server 230 through a secure link. This request includes card credential 330, challenge data 410, and card response 415. (In some implementations, a card reader can initially obtain challenge data from a trusted server. In these implementations, it is may not be necessary to transmit the challenge data back to the trusted server.) As discussed below, trusted server 230 then uses a trusted server decryption key 420 to examine the data received in request for authentication 450.

[00107] FIG. 9 shows an example of information flow within trusted server 230 during a second phase of the access request from FIG. 6. After receiving request for authentication 450 from card reader 220, trusted server 230 decrypts card credential 330 and determines whether card response 415 is an acceptable response to challenge data 410. The decryption is performed using trusted server decryption key (TSDK) 420. TSDK 420 is a securely protected key that is available to trusted server 230. TSDK 420 is related to TSEK 320, which was discussed above with regard to trusted server 130 in the enrollment environment of FIG. 5. In some implementations, TSDK 420 is a private key from a public-private key pair, and TSEK 320 is the corresponding public key from the public-private key pair. In some implementations, TSDK 420 is a symmetric key, and is the same as TSEK 320. These symmetric-key implementations may offer a streamlined key management in situations where card enrollment is overseen by the same server as card authentication, e.g., where trusted server 230 is the same as trusted server 130.

[00108] This decryption with TSDK 420 unlocks the contents that are protected by TSEK 320, and provides trusted server 230 with card key 310, card configuration data 312, and card data 314. In this example, therefore, trusted server 230 does not require advance knowledge of card key 310. Instead, card key 310 is obtained from the unlocking of the card credential that was received in request for authentication 450. This is an example of a "stateless"

implementation, where a trusted server can operate without requiring a priori knowledge such as a log of out-of-band authentications and/or information recorded in an access control list. Such implementations may provide various advantages. In this example, a card-authenticating server (e.g., trusted server 230) functions without needing direct communication with an enrolling server (e.g., trusted server 130). Instead, these two servers effectively communicate through information stored on a physical token (e.g., access card 110). In other implementations, the security of the overall system can be augmented by such inter-server communication and/or by the use of access control lists.

[00109] The illustrated example applies an encryption and decryption technique that is different from the on-card authentication protocol. In particular, the relevant key (TSDK 420) and decryption calculations for unlocking card credential 330 are different from and independent of the key (card key 310) and challenge-response calculations that were used by the processor on the access card. Thus, obtaining the card key from the card credential uses an encryption protocol that is independent of the on-card authentication protocol.

[00110] FIG. 10 shows an example of information flow during a third phase of the access request from FIG. 6. After obtaining card key 310 from card credential 330, trusted server 230 locally generates a response 615 using card key 310 and challenge data 410. This server-generated response 615 is therefore based on the same data (card key 310 and challenge data 410) that were used by access card 110 for the on-card authentication protocol. In the context of FIG. 10, the card response 415 received from access card 110 is under scrutiny by trusted server 230. Card response 415 is treated as a "candidate response"—it is evaluated to determine whether it is an appropriate response to challenge data 410.

[00111] In one implementation, this evaluation is done by comparing card response 415 to server-generated response 615. If these data do not match, then card response 415 is understood to have been generated by a device that either did have possession of card key 310, and/or was not responding to challenge data 410. Trusted server 230 then generates a negative authentication output 611. Negative authentication output 611 can be provided as an alert to an administrator or an automated security monitoring system, noting that an invalid access request was made. Negative authentication output 611 can be also be provided as feedback to card reader 220 from FIG. 6, which can then flash a red light or emit a tone indicating that access has been denied. Door 250 from FIG. 6 is not unlocked in response to negative authentication output 611. If instead card response 415 and server-generated response 615 do match, then card response 415 is understood to have been generated by a device that did have possession of card key 310, and which was responding to challenge data 410. Trusted server 230 then generates a

positive authentication output 610. Positive authentication output 610 is provided to door controller system 240 from FIG. 6, which then unlocks door 250. User 115 can then gain access to the secure area behind door 250.

[00112] In addition to, or instead of, communicating with door controller system 240, trusted server 230 can communicate directly with an electronic lock on the door (e.g., door lock 245), a door controller, a magnetic lock, or other system that directly or indirectly controls access. The communication can be based on positive authentication output 610 or on other analyses of received card credentials and information about challenge-response interactions.

[00113] In other embodiments, positive authentication output 610 prompts trusted server 230 to initiate additional security checks before opening door 250. For example, trusted server 230 can first verify that an expiration date obtained from card credential 330 has not been exceeded. As another example, trusted server 230 can use a user identification from card data 314 to consult an access control list (not shown), and confirm that according to the access control list, user 115 is approved for access to door 250.

[00114] FIG. 11 shows an example 700 of a process used in an access control environment. In this example, process 700 includes two sets of operations. An access card is enrolled with a card reader (such as, for example, card reader 120) in act 710, which includes acts 712 and 714. Act 710 can be used, for example, for the operations discussed above with relation to FIG. 5. The access card is then used with a different card reader (such as, for example, contactless card reader 220, or a contact-interface reader) to gain access to a secure facility in act 720, which includes acts 722, 724, 726, and 728. Act 720 can be used, for example, for the operations discussed above with relation to FIG. 6.

[00115] After an enrollment in act 710, the access card can be used to access a secure facility more than once (e.g., when a user exits the secure facility and later needs to return, or when the user needs to log in again to the same protected computing facilities). The access card can also be used to access additional secure facilities. These repeated access attempts are indicated by a looping arrow in FIG. 11, which causes act 720 to repeat. From time to time (e.g., occasionally or on a set schedule), the access card can be re-enrolled either voluntarily or as required by a security protocol. This re-enrollment is indicated by a looping arrow in FIG. 11 that returns from act 720 to act 710.

[00116] It is contemplated that the access card can be a physical-access card, and that the secure facility can be a secure area such as one or more offices, office suites, buildings, residences, data centers, or other secure areas, or combinations thereof. It is also contemplated

that the access card can be a data access card, such as a login token card, and the secure facility may include secure computing equipment or information, such as secure computer systems or databases. Combinations of physical access and data access are also contemplated, as well as particular applications to financial accounts, secure government facilities, military facilities, corporate facilities, and organizational facilities. In one example, process 700 is used to protect a military research and development laboratory from improper physical access by unauthorized personnel. In another example, process 700 is used with appropriate card=reader hardware to protect data on laptops used by humanitarian aid workers from improper access by unauthorized personnel. In yet another example, process 700 is used for access to monetary funds (e.g., on-line purchases or transfers, or withdrawals from automated teller machines) by an account holder at a financial institution.

[00117] In various implementations, the interactions between the card reader and the access card in act 710 are contactless interactions. For example, these interactions can use contact-interface link 170 from FIG. 5. Alternatively, or in conjunction, these interactions can use a contact interface for communication between the card reader and the access card.

[00118] Act 710 begins with act 712, in which a user undergoes an out-of-band authentication process. Act 712 is an operation that establishes that a user of the access card is a legitimate user, authorized to gain access to one or more of an organization's secure facilities. In various implementations, act 712 can include a face-to-face interaction between a user and a human gatekeeper of a secure facility (e.g., a facial comparison with a photo identification or other biometric identification of the user, a security interview, and the like), and/or an electronic interaction with an automated gate-keeping circuit or software (e.g., entry of a personal identification number on a keypad at a front security desk, entry of a userid and password or other computer login through a remote login procedure, authentication of a digital certificate or other user credential, and the like). The out-of-band authentication can also include additional checks to review access rights of the user. For example, databases can be used to check an approved set of locations for the user, a security level of the user, a security alert status of the secure area or the organization (high alert, low alert, lockdown, and the like), an access history of user, an access history of the access card, suspected security compromises, relevant administrator instructions, a revision of an access control list, or other factors, or combinations thereof.

[00119] In act 714 a card credential and a card key are stored on the access card. In various implementations, the card credential and card key are generated only after the out-of-band authentication process of act 714.

[00120] The card credential is generated by a trusted server (such as, for example, trusted server 130). The trusted server used in act 714 can, for example, be remotely located from the card reader in a secure computing center, and connected to the card reader through a secure communications link. Alternatively, the trusted server used in act 714 can be incorporated within the card reader. In one implementation, the trusted server used in act 714 is implemented in a replaceable smart card that is securely mounted within the card reader. The card key can also be generated by the trusted server. The card key and card credential are stored in one or more memories on the access card.

[00121] After the enrollment in act 710, the access card can then be used in act 720 to gain access to a secure facility using a card reader. In various implementations, the interaction between the card reader and the access card in act 720 are contactless interactions. For example, these interactions can use wireless link 270 from FIG. 6. Alternatively, or in conjunction, these interactions can use a contact interface for communication between the card reader and the access card.

[00122] The card reader used in act 720 is generally deployed at a different location from the card reader used in act 710. In various implementations, the card reader used in act 720 is a contact-interface reader or a contactless interface reader mounted next to a door or at a security checkpoint that protects a secure area, such as an entry door, an elevator door, a pedestrian gate, an access gate for vehicles, or other doors, to regulate physical movement within an organization, for example.

[00123] It is also contemplated that in some implementations, the card reader used in act 720 is the same as the card reader used in act 710. For example, a user may use a card reader for enrollment and then immediately use the same card reader to test the enrollment by requesting access.

[00124] As another example, a card reader may serve a double purpose, enabling authentication for cards that it has previously enrolled. Such a double-purpose card reader can be deployed next to an off-site computer, for example. It is contemplated that such a card reader could be plugged into a USB port of a user's home computer or portable computer, or otherwise connected to or integrated into an off-site computer. In this example, the card reader regulates remote access from the off-site computer to computing equipment or to information. Alternatively, or in addition, the card reader regulates access to data that is stored within the off-site computer itself. This card reader is used for enrollment operations (act 710) by requiring entry of an account password or some other out-of-band authorization (e.g., a simultaneous voice

telephone call, or entry of a time-varying token code, for example) before granting access to the protected data. This same card reader is again used after some time (act 720) to let the user continue to have access to the protected data, but without having to repeat the out-of-band authorization.

[00125] Act 720 begins with act 722, in which a user holds the access card near a card reader, or otherwise presents the access card to the card reader. In one implementation, the card reader continuously broadcasts an RF signal. The access card detects the signal when it is within close range (a few inches to a few feet) of the card reader, and transmits an RF response to inform the card reader of the presence of the access card. In another implementation, the card reader becomes aware of the access card through a change in RF coupling to the surrounding environment, such as an inductive coupling that occurs when the access card is brought within close range. In other implementations, the user presents the card by placing the access card on or in the card reader.

[00126] In act 724, the card reader transmits a challenge to the access card. In act 726, the access card returns a response to the card reader. The response is based on the challenge and on the card key that was stored on the access card in act 714. The access card also transmits the card credential to the card reader.

[00127] In act 728, the communications between the card reader and access card are evaluated to decide if access should be granted to the secure facility. The evaluation is performed by a trusted server (such as, for example, trusted server 230) that can be different from the trusted server discussed above with regard to act 714. The trusted server used in act 728 can be remotely located from the card reader in a secure computing center, and connected to the card reader through a secure communications link. Alternatively, the trusted server used in act 728 can be contained within the card reader. In one implementation, the trusted server used in act 728 is implemented in a replaceable smart card that is securely mounted within the card reader.

[00128] FIG. 12 shows an example 800 of a process with details of some of the operations shown in FIG. 11. In various implementations, acts 810 and 812 can be used in act 714 from FIG. 11 to enroll an access card. Similarly, acts 821, 822, 823, 824, 825, 826, and 827 can be used in acts 724, 726, and 728 from FIG. 11 to authenticate a request for access that was made with the access card. It is noted that various different types of hardware (e.g., access cards, card readers, and servers) and software (e.g., different orderings or combinations of the various acts in

processes 700 and 800) are contemplated in addition to the specific examples discussed with respect to FIGs. 11 and 12.

[00129] In act 810, a trusted server uses an encryption key, for example TSEK 320 from FIG. 7, to encrypt a card key into a card credential. In various implementations the trusted server can also sign the card credential after (or before) the encryption operation. The card key can also be generated by the trusted server. In act 812, the card credential and card key are communicated to the access card, and are stored in one or more memories on the access card. The card key is stored in on the access card in such a way that it is protected from being readable by an unauthorized user. In various implementations, the card key is injected into a section of memory on the access card (e.g., a key slot) such that the card key is accessible only to a processor on the access card, and the processor is configured not to output or otherwise reveal the raw contents of this section of memory. The card key thus cannot be read from the access card.

[00130] In act 821, a challenge is transmitted to the access card. In various implementations, the challenge is (or includes) a unique random number, generated solely for the purpose of challenging the access card on this access attempt. The challenge can be transmitted by a card reader or by a trusted server (via the card reader). In act 822, the access card uses an on-card authentication protocol to generate a candidate response. The candidate response is based on the challenge and on the card key that was stored on the access card in act 812. In act 823, the candidate response is received by a trusted server from the access card. The card credential, from act 812, is also received from the access card.

[00131] In act 824, the trusted server uses a decryption key, for example TSDK 420 from FIG. 8, to decrypt the card credential that was received from the access card in act 823. In various implementations the trusted server can precede (or follow) the decryption by authenticating a signature on the card credential. The decryption recovers a card key, which is expected to be the same as a card key that was generated in acts 810 and 822.

[00132] In act 825, the trusted server locally generates a response to the challenge that was posed in act 821. To generate this response, the trusted server uses the same on-card authentication protocol that was used in act 822 by the access card. The trusted server can use information extracted from the card credential to determine which of several on-card authentication protocols was used by the access card. The server generates its response based on the challenge and on the card key that was recovered in act 824.

[00133] In act 826, the trusted server compares the locally generated response from act 825 to the candidate response that was received in act 823. If and only if these responses

match, then the candidate response is understood to have been generated by a device that had possession of the card key and was responding to the challenge data.

[00134] In act 827, if the locally generated response fails to match the candidate response, the trusted server denies access. If the locally generated response matches the candidate response, the trusted server initiates a process that can lead to granting access. In various implementations, the subsequent process can include additional checks to review access rights of the user based on data extracted from the card credential (e.g. card data 314) and/or data obtained by the trusted server from databases such as access control lists. For example, the extracted data and/or a positive access control list and/or a negative access control list can be used to check other forms of key life cycle (e.g., "valid-until" time limit, a duration-of-use limit, a number-of-uses limit, a predetermined time mark), an approved set of locations for the user, a security level of the user, a security alert status of the secure area of the organization (high alert, low alert, lockdown, and the like), an access history of the user, an access history of the access card, a suspected security compromise, an administrator instruction, a revision of an access control list, or other factors, or combinations thereof.

[00135] FIGs. 1-12 illustrate some of the operational examples of the techniques and tools contemplated for use with access cards. Those having ordinary skill in the art will readily recognize that certain steps or operations described herein can be eliminated or taken in an alternate order, and that various arrangements and alternatives of hardware components can be used.

[00136] For example, it is contemplated that the trusted server keys (e.g., TSEK 320 and TSDK 420) can be managed by a public key infrastructure (PKI), which securely manages the distribution of keys among trusted servers and, when necessary, the revocation of keys. It is also contemplated that the trusted server keys can be symmetric keys that are protected by other security procedures and key-management protocols. The security of the trusted server keys can be managed and protected with different and separate procedures than the card keys. Thus, in various implementations, a compromise of a card key (e.g., card key 110) does not cause a trusted server key (e.g., TSEK 320 or TSDK 420) to be compromised. If a malicious party were somehow to compromise an access card and read a card key from the access card, this compromise would have a limited effect, providing access only during the life cycle of the compromised card key, and not directly leading to a compromise of a trusted server key.

[00137] Moreover, the trusted server keys can have larger key sizes and can use more computationally intensive encryption protocols than the card keys and their on-card

authentication protocols. In various implementations, the trusted server keys can have key life cycles that are substantially longer than the life cycles of the card keys. For example, a key lifetime recorded in TSEK 320 or TSDK 420 (e.g., weeks, months, or years) can be substantially longer than a key lifetime recorded in card credential 330 (e.g., hours, days, or weeks). In various implementations, the lifetime for card keys is selected to be something less than an estimated time to compromise a card key, and the lifetime for trusted server keys is selected to be something less than an estimated time to compromise a trusted server key.

[00138] The system can also be implemented with revocation mechanisms for card keys or for users. Card-key revocation or user revocation can be implemented, for example, using access control lists. Alternatively, revocation of card keys or users can be done with revocation lists that are more concise than access control lists. Various offline or out-of-band checks can also be done to screen for compromised or revoked users, access cards, card keys, or card identifiers. In various implementations, revocations and other responses to the compromise of a card key can be implemented without invoking higher-level responses that would be needed in response to the compromise of a trusted server key.

[00139] It is also contemplated that access control lists can be used to augment the authentication procedures described above. For example, a system can use an access control list to retrieve additional information regarding a user, such as permissions or restrictions previously established for the user. The information retrieved from an access control list can be used in conjunction with information that is retrieved by the decryption of a card credential (such as information in FIG. 9 from card data 314 and/or card configuration data 312, for example). For example, a card identifier can be stored in card data 314, and an access control list can be used to confirm that the user's access card matches a card identifier that was previously stored in an access control list (e.g., during or before an enrollment procedure such as act 710). Alternatively, various implementations can avoid the use of access control lists altogether; these implementations may extract all relevant permissions and restrictions for a user from the card credential. Such implementations enable stateless security systems that can authenticate access cards without needing to consult access control lists.

[00140] By avoiding a reliance on access control lists, designers may facilitate inter-organization authentication. In one example, a user undergoes an out-of-band authentication and enrollment (discussed above with regard to FIG. 5) at a first organization in the morning of a particular day. This authentication provides the user with a credential that expires at the end of that day. The user can then use the access card to enter secure areas (discussed above with regard to FIG. 6) at the first organization throughout the morning. In the afternoon of the same

day the user needs to access secure areas within a second organization. The second organization is different from the first organization, but cooperates with the first organization. In this example, the second organization shares static information such as decryption keys (e.g. TSDK 420) with the first organization, but does not share continually updated information such as access control lists. When the user requests entry to a secure area in the second organization, a trusted server in the second organization can respond to the request (similar to the situation described above with regard to FIG. 6). In this example, the trusted server at the second organization compares a candidate response to a server-generated response (e.g., act 826), but does not need any additional confirmation of the candidate response or the underlying card key from an access control list.

[00141] Such an implementation can be useful, for example, in situations where one organization performs enrollment operations and a second, different, organization relies on those enrollments. The second organization can rely on (a) the integrity of its decryption key and (b) the successful matching of the candidate response to the locally generated response to verify that the access attempt is being made with an access card that has successfully undergone enrollment. The second organization can use additional information in the decrypted card credential, for example to confirm that the successful enrollment was recent.

[00142] Hybrid reliance on access control lists is also contemplated. Continuing the above example, the second organization can consult an internal access control list for purposes other than authenticating the user or the user's access card. For example, the second organization's internal access control list can indicate which of several secure areas within the second organization can be accessed by this user.

[00143] Moreover, it is contemplated that a third organization can cooperate with the first organization, but is not willing to share trusted server keys with the first organization. The third organization can, however, cooperate such that users can employ a single access card for both the first and third organizations. The third organization can be a bank (or other financial institution) that uses a separate set of trusted server keys, which are used to enroll access cards with corresponding card credentials that allow the users to withdraw or otherwise use money on deposit (or on credit) at the bank. The bank can require the user to undergo an out-of-band authentication, in person or on-line, to demonstrate that the user indeed holds an account at the bank. For a limited time thereafter (e.g., hours or days, or perhaps weeks if the user informs the bank that she will be travelling on vacation), the user can use the access card to withdraw funds from a conforming automated teller machine (ATM) or use a portable card reader to direct transfers of funds from the account or authorize purchases with funds from the account.

[00144] In the above example, one access card is configured to store two card credentials and two card keys: one card key and card credential are for the first and second organizations, and the other card key and card credential are for the third organization. In other environments, the access card can be configured to store simultaneously three (or more) different card credentials, for three or four (or more) different organizations.

[00145] It is also contemplated that a single trusted server can be used with a variety of types of access cards. For example, an organization can have deployed three different types of access cards, which perform three different types of on-card authentication protocols. The card credential stored on an access card can indicate which type of on-card authentication protocol is performed by that access card. This information can be recorded, for example, in card configuration data 312. When the trusted server decrypts the card credential, it uses this information to decide which on-card authentication protocol should be used to locally generate the server response (e.g. response 615).

[00146] This flexibility with regard to different types of access cards can be useful to system designers when performing an incremental (user-by-user, or area-by-area) upgrade of a security system. Depending on the implementation, the different types of access cards may or may not require different types of card readers.

[00147] It is also contemplated that the tools and techniques described above can be added incrementally, on an area-by-area basis, to an organization that has an existing legacy access control system. The legacy system may use legacy card readers and a large number of existing legacy access cards issued to existing users. One or more of the areas can then be upgraded to use the techniques described above. In one example, a limited number of personnel who need to access the upgraded areas can be given access cards (such as access card 110, for example) that require an out-of-band authentication and can carry a card credential such as described above. Other users can continue to use the legacy access cards. The card readers for the upgraded area can then be connected to a trusted server (such as trusted server 230) that can decrypt the card credentials. This trusted server can then transmit authentication outputs to the legacy access control system, which is connected with a legacy door controller system. Depending on the implementation, the card readers for the higher-security areas may need to be upgraded (or replaced), but this upgrade can be carried out on an area-by area basis, without disrupting the entire security operations at one time.

[00148] In one example, the legacy card readers transmit card identifiers as the output to authentication requests. The card identifiers are unique identifiers that conform to a format for

the legacy system. The legacy card readers transmit this output to the legacy access control system. The legacy access control system checks a received card identifier against an access control list to determine whether or not to open a door. This type of legacy system can be upgraded, one secure area at a time, by deploying a trusted server (such as trusted server 230) between the upgraded secure areas and the legacy access control system. When a user requests access to a non-upgraded area, the legacy system operates normally. When a user requests access to an upgraded area, the trusted server performs operations (such as acts 823-826) to determine whether the user's access card is responding appropriately to challenge data with a card key. If the internal comparison successfully authenticates an access request, the trusted server uses a card identifier (received, for example, from card data 314) as an output that is passed on to the legacy access control system for further comparison to the access control list. However, if the internal comparison fails to authenticates an access request, the trusted server does not generate an authentication output, and the legacy access control system is not prompted to consider the access request.

[00149] It is also contemplated that various implementations can provide convenience to a user by occasionally re-enrolling the user's access card during an access request. For example, in one example a user completes an enrollment by undergoing an out-of-band authentication in the morning of a working day (e.g., by interacting with a front-desk security guard or by logging in from a home computer). The enrollment stores a card credential onto the user's access card, with a life time of 8 hours noted in the card credential. Over the next six hours, the user behaves in a manner that is in accordance with standard security procedures (e.g., by attempting to access only permitted areas in a building, or by re-logging every two hours using a card reader at home). No security alerts are posted over the next six hours. In view of these nominal operations, the security system may renew the enrollment of the user by automatically replacing the card credential on the user's access card with a renewal card credential, whenever the user presents the access card to a card reader. This new card credential can include, for example, a life time of an additional 4 hours beyond the originally noted life time.

[00150] Conversely, it is contemplated that an enrollment may be withdrawn in response to an abnormal behavior of a user, or in response to a security policy not being met. Continuing the above example, if the security system is compromised, or if the user does something that is not approved by standard security procedures, then the next time the user presents the access card to a card reader, the card credential on the access card can be deleted, amended with a cancelation notice, or otherwise revoked. The security policy could be deemed as not being met due to, for example, the detection of an intruder, a report of questionable activity, a passage of a

predetermined time interval, a passage of a predetermined time mark, an excessive number of access attempts, a suspected security compromise, a user instruction for alert, a revision of an access control list, the user attempting access to a forbidden area or to forbidden data, or the entering an correct PIN code or password, among others.

[00151] After a user's card credential has been revoked, the user can be required to undergo an in-person re-enrollment. The re-enrollment can provide confirmation of the validity of the user, and possibly a review of the security clearance of the user.

[00152] Similarly, it is contemplated that card credentials can be withdrawn in response to a security alert. The withdrawal can be organization-wide, or can be limited to credentials for a particular area(s) or a particular user(s). The withdrawal would be performed the next time that the access card is presented to a card reader, for example, the next time the user attempts to enter a secure area. Such a withdrawal can involve the consultation of an access control list or a revocation list, and can involve the examination of restrictions included in a card credential.

[00153] Moreover, various operations discussed with respect to FIGs. 1-12 can be implemented as one or more software programs (or modules) for one or more processors. Those having ordinary skill in the art will readily recognize that various operations and calculations, such as cryptographic operations, communications operations, or data processing operations, and various techniques discussed above can be implemented using software in a variety of computer languages, including, for example, traditional computer languages such as assembly language, Pascal, and C; object oriented languages such as C++, C#, and Java; and scripting languages such as Perl and Tcl/Tk. Similarly, various operations can be implemented as hardware modules such as application-specific integrated circuits (ASICs), microcontrollers, or other appropriate circuits.

[00154] The software can be encoded on a computer readable storage medium as instructions executable on one or more processors, for example on various servers, card readers, or smart cards, or combinations thereof. The computer readable storage medium can include a non-volatile or volatile solid-state storage medium (e.g., flash memory, dynamic random access memory, and the like), a magnetic storage medium (e.g., hard disk, a floppy disk, and the like), or an optical storage medium (e.g., CD-ROM, CD-R, CD-RW, DVD-ROM, and the like), or combinations thereof. Alternatively, or in addition, the software programs can also be provided to a system using a communications medium, such as a transmission line or electromagnetic wave, conveying signals encoding the instructions. Separate instances of the programs can be executed on separate computer systems. Thus, although certain steps have been described as being performed by certain devices, software programs, processes, or entities, this need not be

the case and a variety of alternative implementations will be understood by those having ordinary skill in the art. Additionally, those having ordinary skill in the art will readily recognize that the techniques described above can be utilized with a variety of different smart cards and computing systems with variations in, for example, the number and type of smart cards, communications interfaces, servers, and card readers.

[00155] Although the present invention has been described in connection with several embodiments, the invention is not intended to be limited to the specific forms set forth herein. On the contrary, it is intended to cover such alternatives, modifications, and equivalents as can be reasonably included within the scope of the invention as defined by the appended claims.

What is claimed is:

1. A method comprising:

generating a card credential, wherein:

the generating the card credential comprises encrypting a card key using a server encryption key, and

the card key is usable for a challenge-response interaction;

transmitting the card credential to an access card; and

transmitting an unencrypted copy of the card key to the access card.

2. The method of claim 1, further comprising:

receiving a request for authentication, wherein the request for authentication comprises the card credential and a candidate response;

obtaining the card key from the card credential using a server decryption key;

generating a response data based on at least the card key, a challenge data, and a card authentication protocol;

comparing the candidate response to the response data; and

generating an authentication output based at least on the comparing.

3. The method of claim 2, wherein:

the generating the card credential is performed by a server computer as part of an enrollment procedure following an authentication of a user of the access card; and

the receiving the request for authentication is performed by the server computer following an access request by the user.

4. The method of claim 2, wherein the generating the card credential is performed by a first server computer, and the receiving the request for authentication is performed by a second server computer that is different from the first server computer.

5. The method of claim 2, wherein the generating the authentication output comprises:

generating a positive output only if:

the candidate response matches the response data, and

a key lifecycle data decrypted from the card credential indicates that the card key is not obsolete; and

generating a negative output if the candidate response does not match the response data.

6. The method of claim 2, wherein the card authentication protocol is selected from a plurality of card authentication protocols based on information obtained from the card credential.

7. The method of claim 2, wherein:

the obtaining the card key from the card credential comprises using a decryption protocol;

the card authentication protocol is performed by the access card and is substantially less computationally intensive than the decryption protocol; and

the access card is incapable of obtaining the card key from the card credential.

8. The method of claim 7, wherein the decryption protocol is a public key cryptographic protocol that uses the server decryption key, and the card authentication protocol uses a symmetric key.

9. The method of claim 2, further comprising:

transmitting the challenge data to the access card; and

generating the candidate response using at least the card key, the challenge data, and the card authentication protocol, wherein the generating the candidate response is performed by the access card.

10. The method of claim 9, wherein the transmitting the challenge data to the access card is performed by a card reader, the request for authentication is received from the card reader, and the request for authentication further comprises the challenge data.

11. The method of claim 10, further comprising:

transmitting the candidate response from the access card to the card reader through a contactless communications link between the access card and the card reader; and

generating the request for authentication; wherein the generating the request for authentication is performed by the card reader in response to receiving the candidate response from the access card.

12. The method of claim 1, further comprising:

obsoleting the card key based on a first key life cycle; and

obsoleting the server decryption key based on a second key life cycle that is substantially longer than the first key life cycle.

13. The method of claim 1, further comprising:

authenticating a user of the access card, wherein the transmitting the card credential to the access card is performed in response to the authenticating the user.

14. The method of claim 13, wherein the authenticating the user comprises one or more of:

manually checking a photographic identity card of the user;

the user successfully completing a computer login; or

the user demonstrating authorization to use a financial account.

15. The method of claim 13, further comprising:

replacing the card credential on the access card with a renewal card credential in response to one or more of:

a security policy being met for a period of time,

a successful user login event, or

a re-authentication of the user; and

in response to the security policy not being met, one or more of:

re-authenticating the user, or

revoking the card credential.

16. The method of claim 2, further comprising:

incorporating a card identifier into the card credential, wherein the card identifier is usable with a legacy access system, and the generating the authentication output comprises:

retrieving the card identifier from the card credential; and

transmitting the card identifier to the legacy access system.

17. The method of claim 1, further comprising:

generating a second card credential, wherein the generating the second card credential comprises:

encrypting a second card key using a second server encryption key that is different from the server encryption key; and

transmitting the second card credential to the access card.

18. A method comprising:

receiving a request for authentication, wherein the request for authentication comprises a card credential and a candidate response;

decrypting at least a portion of the card credential using a server decryption key to recover a card key;

generating a response data based on at least the card key, a challenge data that was provided to an access card during a challenge-response interaction, and a card authentication protocol;

comparing the candidate response to the response data; and

generating an authentication output based at least on the comparing.

19. The method of claim 18, wherein the generating the authentication output comprises:

generating a positive output only if:

the candidate response matches the response data, and

a key lifecycle data decrypted from the card credential indicates that the card key is not obsolete; and

generating a negative output if the candidate response does not match the response data.

20. A system comprising:

a data interface;

a memory; and

a processor coupled to the data interface and the memory, and configured to:

transmit an unencrypted copy of a card key to an access card through the data interface;

generate a card credential into which the card key has been locked using an encryption key stored in the memory; and

transmit the card credential to the access card through the data interface.

21. The system of claim 20, wherein the processor is further configured to:

receive a request for authentication through the data interface, wherein the request for authentication comprises the card credential and a candidate response;

obtain the card key from the card credential using a decryption key stored in the memory;

generate a response data based on at least the card key, a challenge data, and a card authentication protocol;

generate a positive authentication output only if:

the candidate response matches the response data, and

a key lifecycle data decrypted from the card credential indicates that the card key is not obsolete; and

generate a negative authentication output if the candidate response does not match the response data.

22. The system of claim 21, wherein the processor is further configured to select the card authentication protocol from a plurality of card authentication protocols based on information obtained from the card credential.

23. The system of claim 21, wherein:

the processor is configured to use a decryption protocol to obtain the card key from the card credential;

the card authentication protocol is performed by the access card and is substantially less computationally intensive than the decryption protocol;

the access card is incapable of obtaining the card key from the card credential;

the card key is a symmetric key;

the encryption key and the decryption key are a public-private key pair;

the processor is configured to obsolete the card key based on a first key life cycle; and

the processor is configured to obsolete the decryption key based on a second key life cycle that is substantially longer than the first key life cycle.

24. A system comprising:

a data interface;

a memory; and

a processor coupled to the data interface and the memory, and configured to:

receive a request for authentication through the data interface, wherein the request for authentication comprises a card credential and a candidate response;

decrypt at least a portion of the card credential using a decryption key to recover a card key;

generate a response data based on at least the card key, a challenge data that was provided to an access card during a challenge-response interaction, and a card authentication protocol; and

generate an authentication output based at least on a comparison of the candidate response and the response data.

25. The system of claim 24, wherein the processor is further configured to select the card authentication protocol from a plurality of card authentication protocols based on information obtained from the card credential.

26. The system of claim 24, wherein:

the processor is configured to use a decryption protocol to obtain the card key from the card credential;

the card authentication protocol is performed by the access card and is substantially less computationally intensive than the decryption protocol;

the access card is incapable of obtaining the card key from the card credential;

the card key is a symmetric key;

the decryption key is an asymmetric key;

the processor is configured to obsolete the card key based on a first key life cycle; and

the processor is configured to obsolete the decryption key based on a second key life cycle that is substantially longer than the first key life cycle.

27. A system comprising:

means for generating a card credential, wherein:

the means for generating the card credential comprises means for encrypting a card key using a server encryption key, and

the card key is usable for a challenge-response interaction;

means for transmitting the card credential to an access card; and

means for transmitting an unencrypted copy of the card key to the access card.

28. A system comprising:

means for receiving a request for authentication, wherein the request for authentication comprises a card credential and a candidate response;

means for decrypting at least a portion of the card credential using a server decryption key to recover a card key;

means for generating a response data based on at least the card key, a challenge data that was provided to an access card during a challenge-response interaction, and a card authentication protocol; and

means for generating an authentication output based at least on a comparison of the candidate response and the response data.

29. A computer-readable storage medium having encoded thereon instruction executable by one or more processors to perform acts comprising:

generating a card credential, wherein:

the generating the card credential comprises encrypting a card key using a server encryption key, and

the card key is usable for a challenge-response interaction;

transmitting the card credential to an access card; and

transmitting an unencrypted copy of the card key to the access card.

30. A computer-readable storage medium having encoded thereon instruction executable by one or more processors to perform acts comprising:

receiving a request for authentication, wherein the request for authentication comprises a card credential and a candidate response;

decrypting at least a portion of the card credential using a server decryption key to recover a card key;

generating a response data based on at least the card key, a challenge data that was provided to an access card during a challenge-response interaction, and a card authentication protocol;

comparing the candidate response to the response data; and

generating an authentication output based at least on the comparing.

31. A method comprising:

receiving key-management information into an access card, wherein

the access card comprises

a first interface,

a second interface, distinct from the first interface, and

a memory, and

the key-management information is received via the second interface;

storing the key-management information in the memory as stored key-management information, wherein

the access card is configured such that the stored key-management information cannot be modified in response to information received via the first interface;

generating an access request based at least in part on the stored key-management information; and

transmitting the access request from the access card via the first interface.

32. A device comprising:

a first interface;

a second interface, distinct from the first interface;

a memory; and

a processor coupled to the first and second interfaces and to the memory, wherein

the processor is configured to receive key-management information via the second interface,

the processor is configured to store the key-management information in a protected portion of the memory as stored key-management information,

the processor is configured to perform a challenge-response authentication interaction via the first interface,

the challenge-response authentication interaction is based at least in part on the stored key-management information, and

the device is configured to prevent data in the protected portion of the memory from being modified in response to information received via the first interface.

33. A system comprising:

an interface;

a memory; and

a processor coupled to the interface and to the memory, wherein the processor is configured to

receive challenge data according to an authentication protocol via the interface,

process the challenge data to obtain key-management information from the challenge data, and

store the key-management information in the memory.

34. The system of claim 33, wherein

the challenge data is comprised in a public key infrastructure (PKI) authentication request; and

the processor is configured to request a PKI authentication of a provider of the key-management information.

35. The system of claim 34, wherein the processor is configured to:

generate a response to the key-management information; and

transmit the response in the form of a second challenge data to the provider of the key-management information.

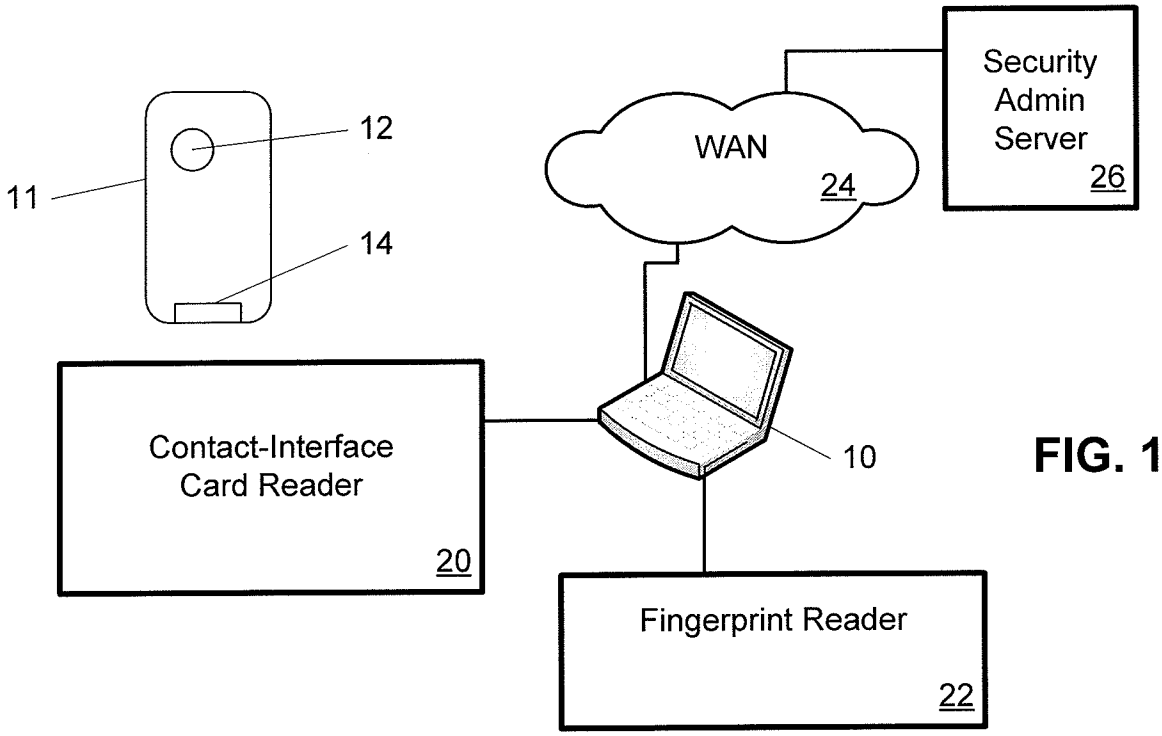
Security
Admin
Server
26
WAN
24
12
11
14
Contact-Interface
Card Reader
20
10
Fingerprint Reader
22

FIG. 1

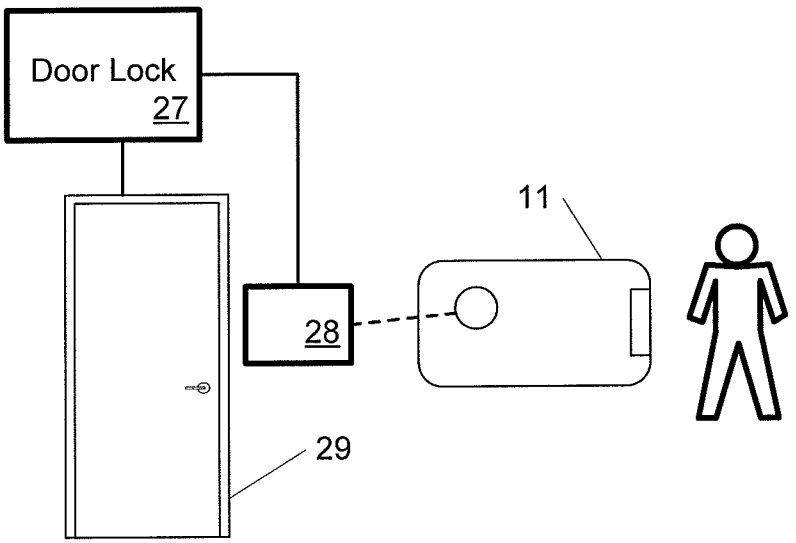
Door Lock
27
11
28
29

FIG. 2

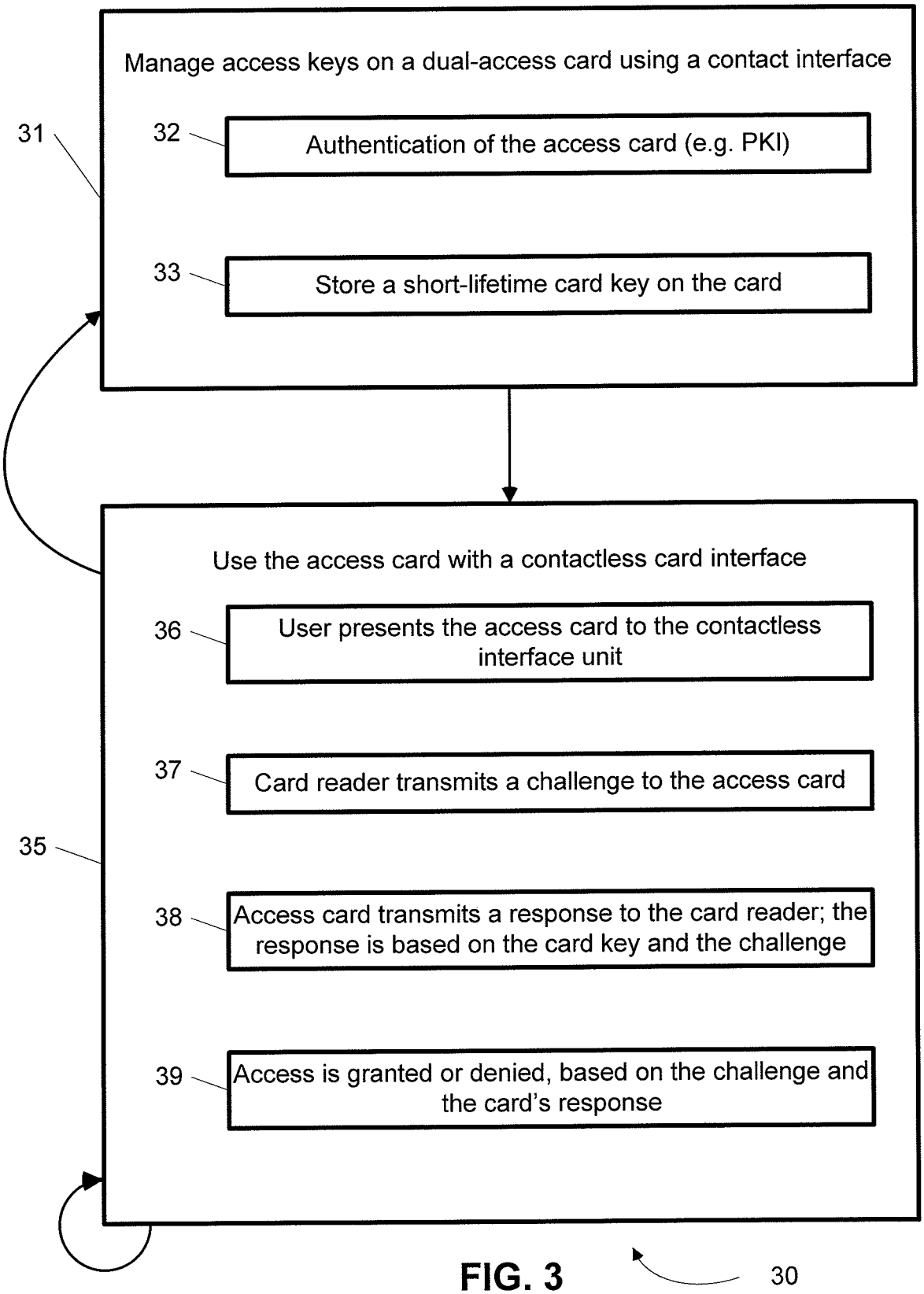
Manage access keys on a dual-access card using a contact interface
31
32
Authentication of the access card (e.g. PKI)
33
Store a short-lifetime card key on the card
Use the access card with a contactless card interface
36
User presents the access card to the contactless interface unit
37
Card reader transmits a challenge to the access card
35
38
Access card transmits a response to the card reader; the response is based on the card key and the challenge
39
Access is granted or denied, based on the challenge and the card's response
30

FIG. 3

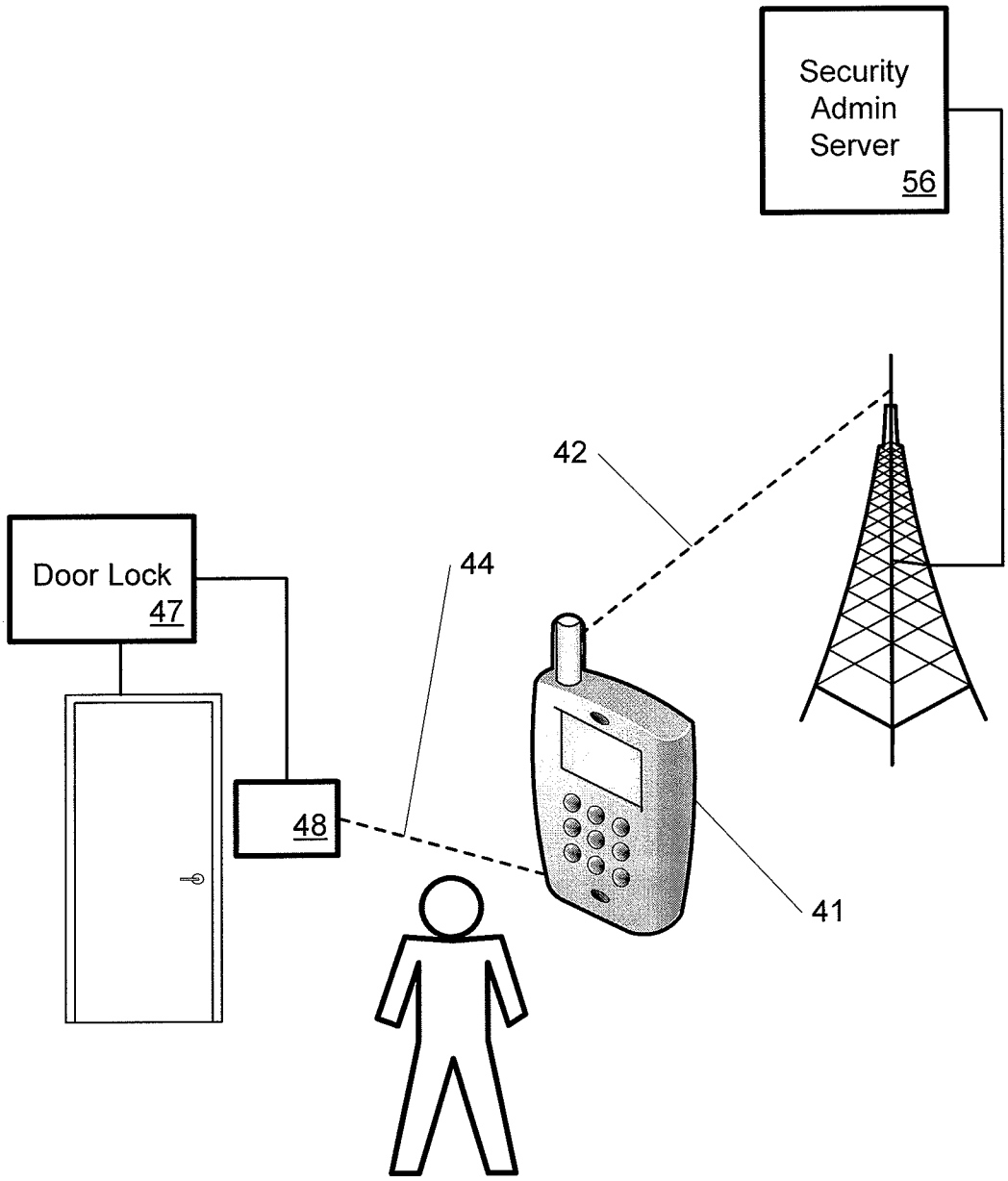

FIG. 4

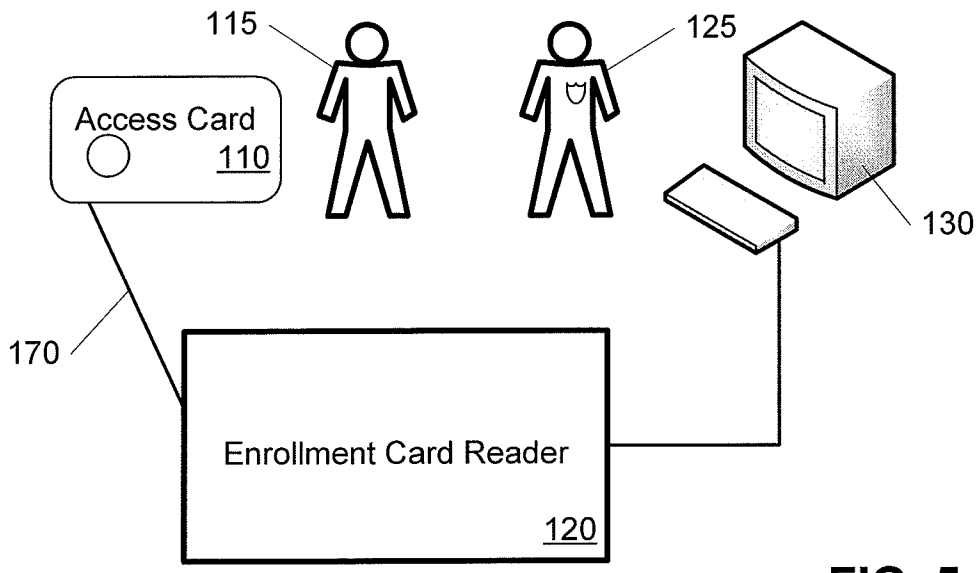
115
125
Access Card
110
130
170
Enrollment Card Reader
120

FIG. 5

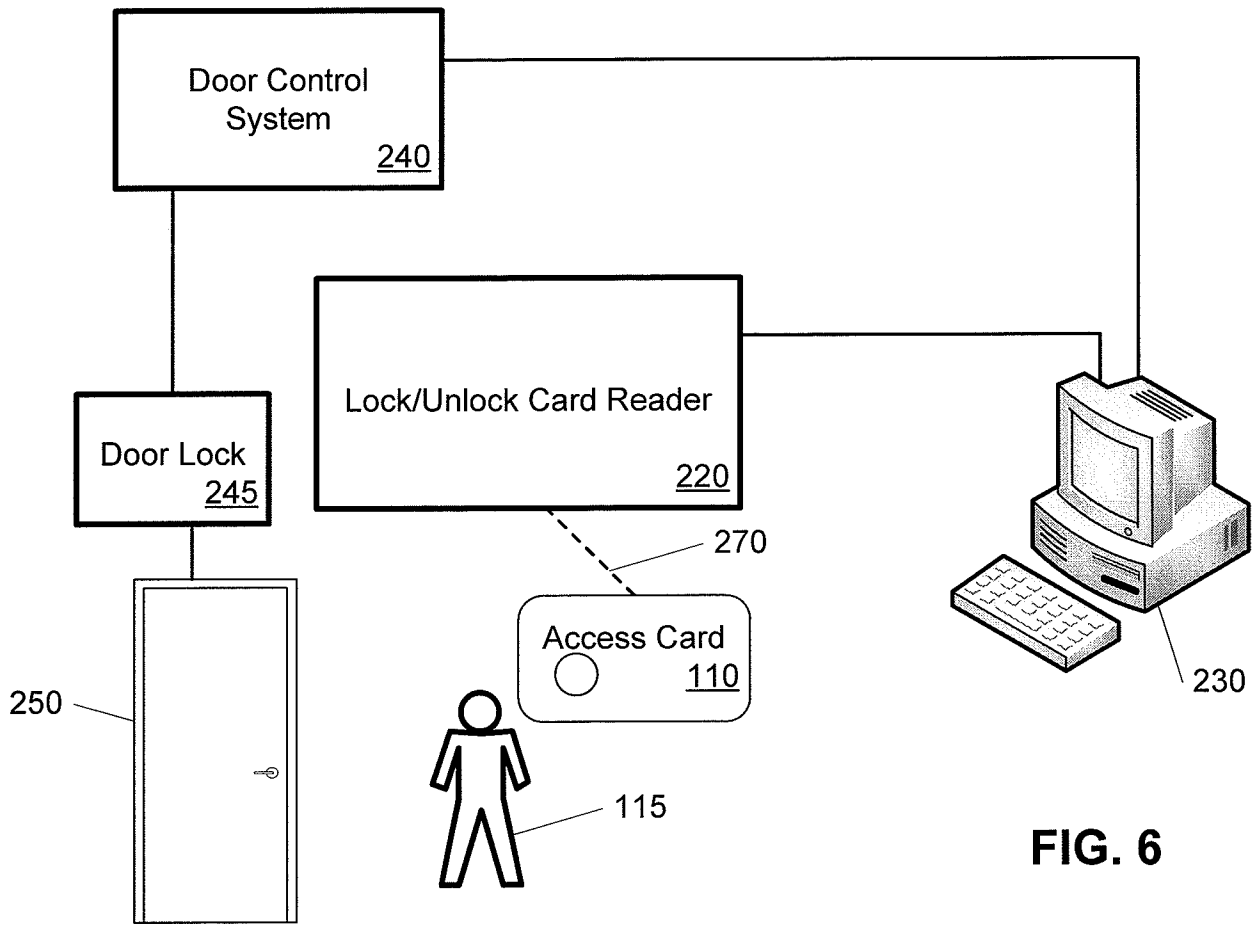
Door Control System
240
Lock/Unlock Card Reader
220
Door Lock
245
270
Access Card
110
230
250
115

FIG. 6

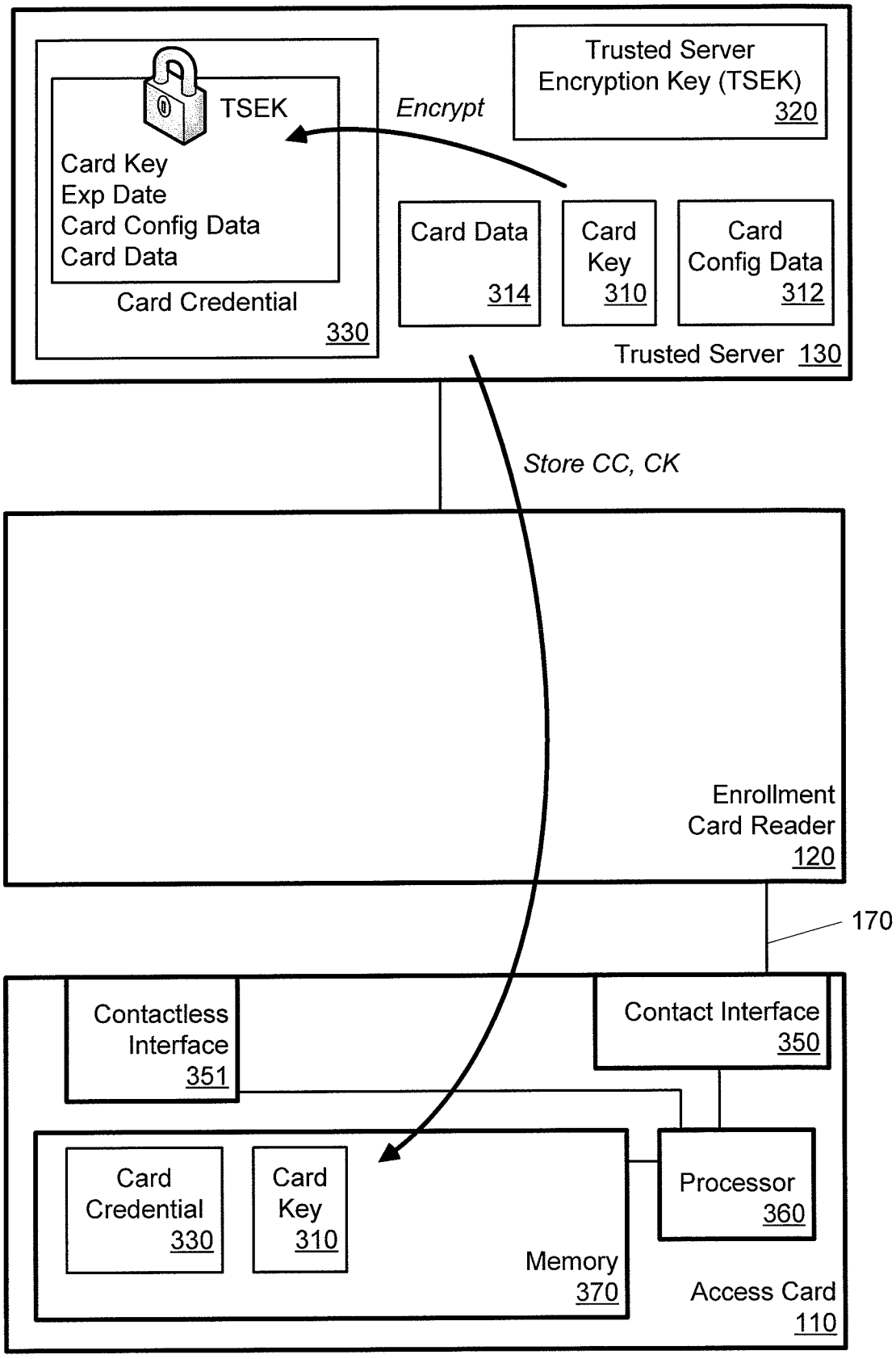
TSEK
Card Key
Exp Date
Card Config Data
Card Data
Card Credential
330
Encrypt
Trusted Server
Encryption Key (TSEK)
320
Card Data
314
Card
Key
310
Card
Config Data
312
Trusted Server 130
Store CC, CK
Enrollment
Card Reader
120
170
Contactless
Interface
351
Contact Interface
350
Card
Credential
330
Card
Key
310
Memory
370
Processor
360
Access Card
110

FIG. 7

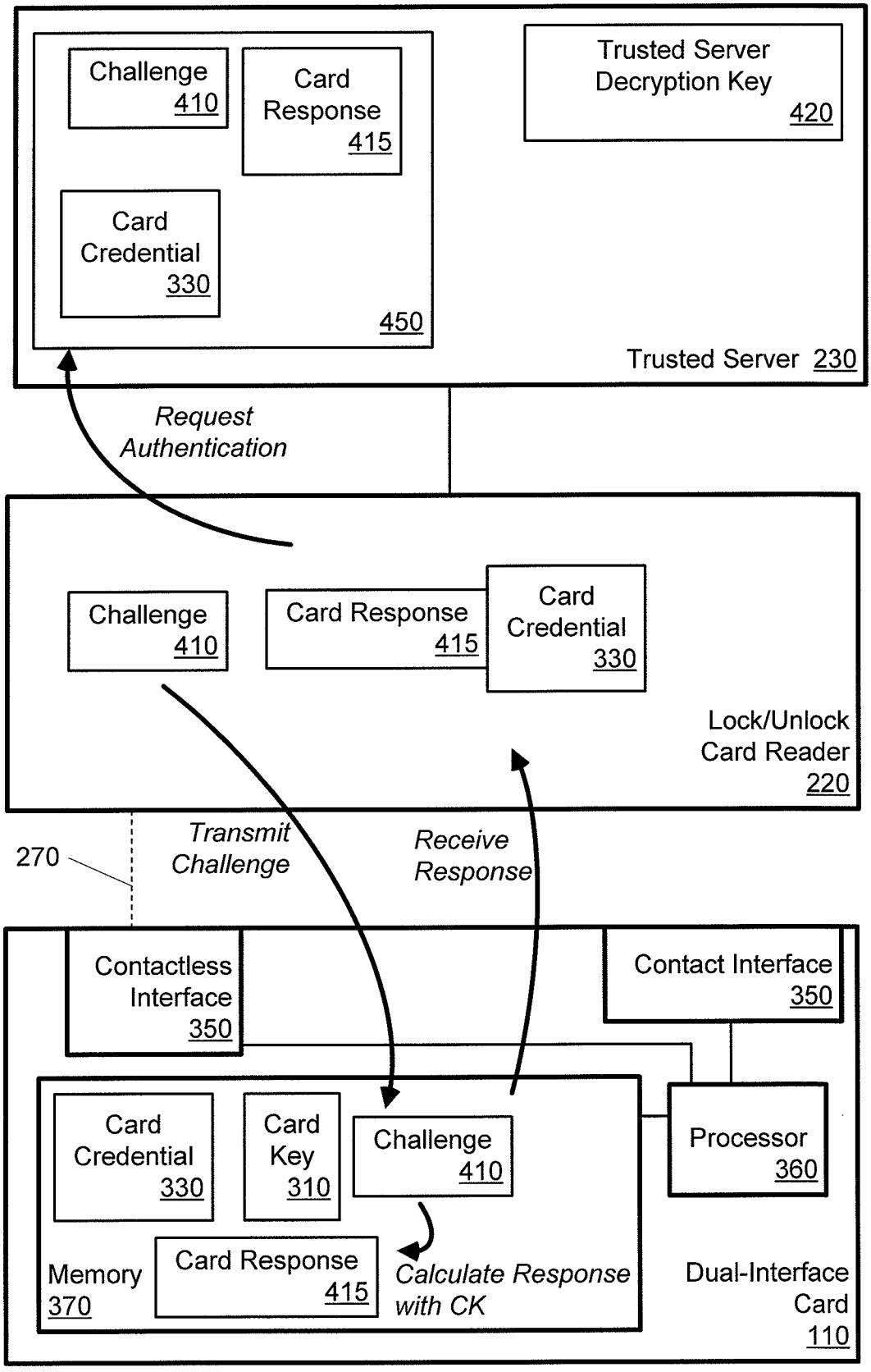
Challenge 410
Card Response 415
Card Credential 330
450
Trusted Server Decryption Key 420
Trusted Server 230
Request Authentication
Challenge 410
Card Response 415
Card Credential 330
Lock/Unlock Card Reader 220
270
Transmit Challenge
Receive Response
Contactless Interface 350
Contact Interface 350
Card Credential 330
Card Key 310
Challenge 410
Processor 360
Memory 370
Card Response 415
Calculate Response with CK
Dual-Interface Card 110

FIG. 8

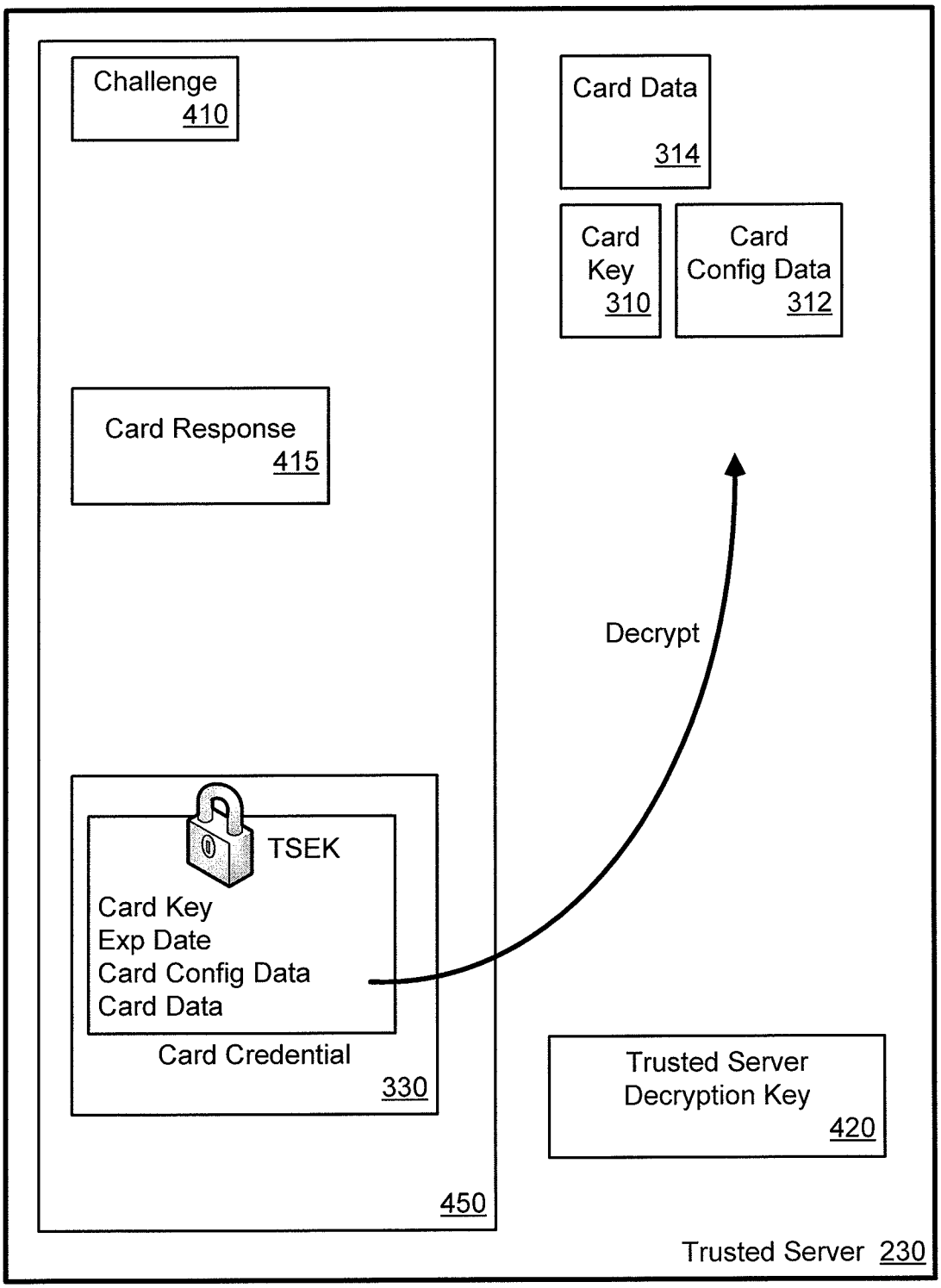
Challenge
410
Card Data
314
Card
Key
310
Card
Config Data
312
Card Response
415
Decrypt
TSEK
Card Key
Exp Date
Card Config Data
Card Data
Card Credential
330
Trusted Server
Decryption Key
420
450
Trusted Server 230

FIG. 9

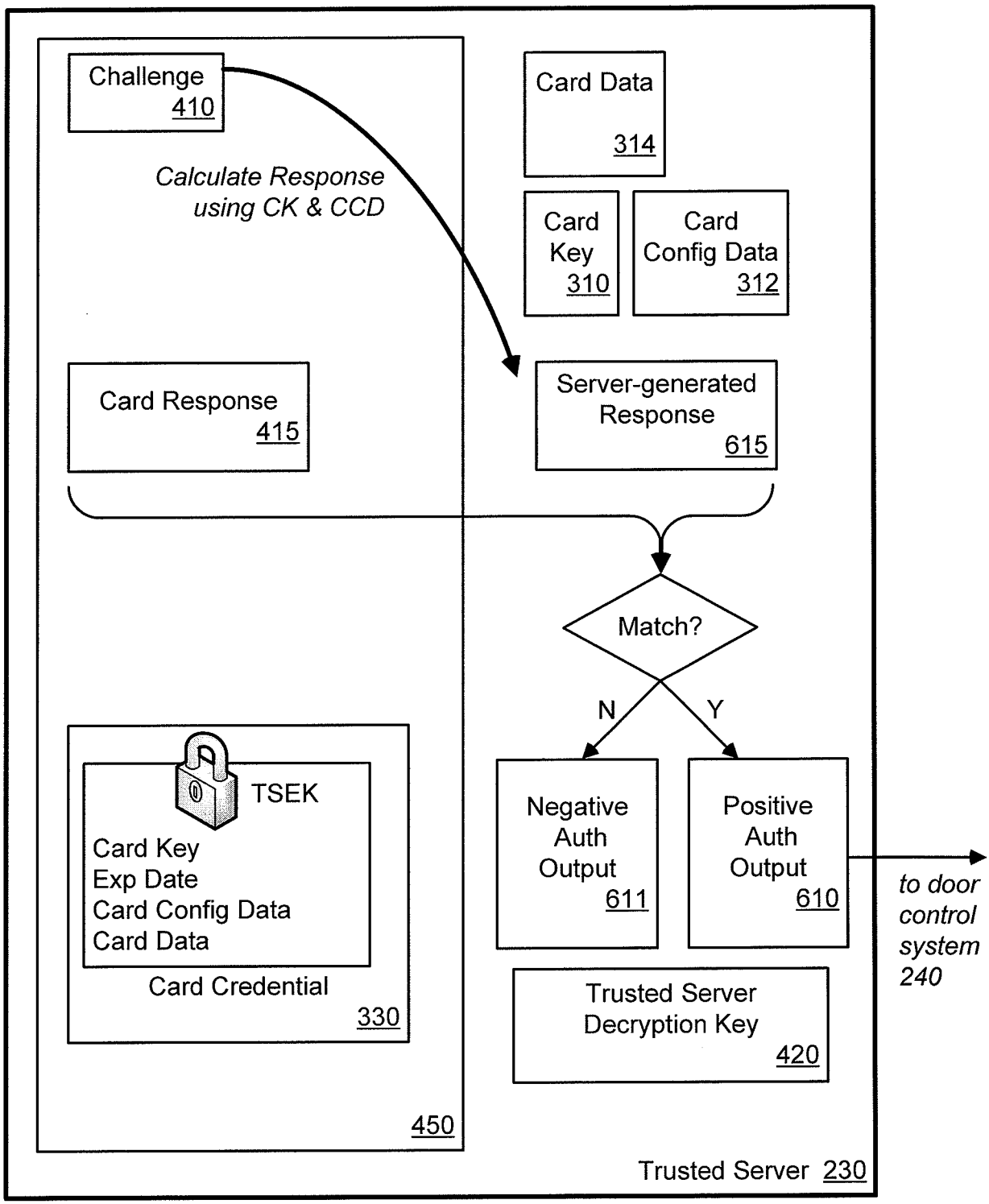
Challenge
410
Calculate Response
using CK & CCD
Card Data
314
Card
Key
310
Card
Config Data
312
Card Response
415
Server-generated
Response
615
Match?
N
Y
TSEK
Card Key
Exp Date
Card Config Data
Card Data
Card Credential
330
Negative
Auth
Output
611
Positive
Auth
Output
610
to door
control
system
240
Trusted Server
Decryption Key
420
450
Trusted Server 230

FIG. 10

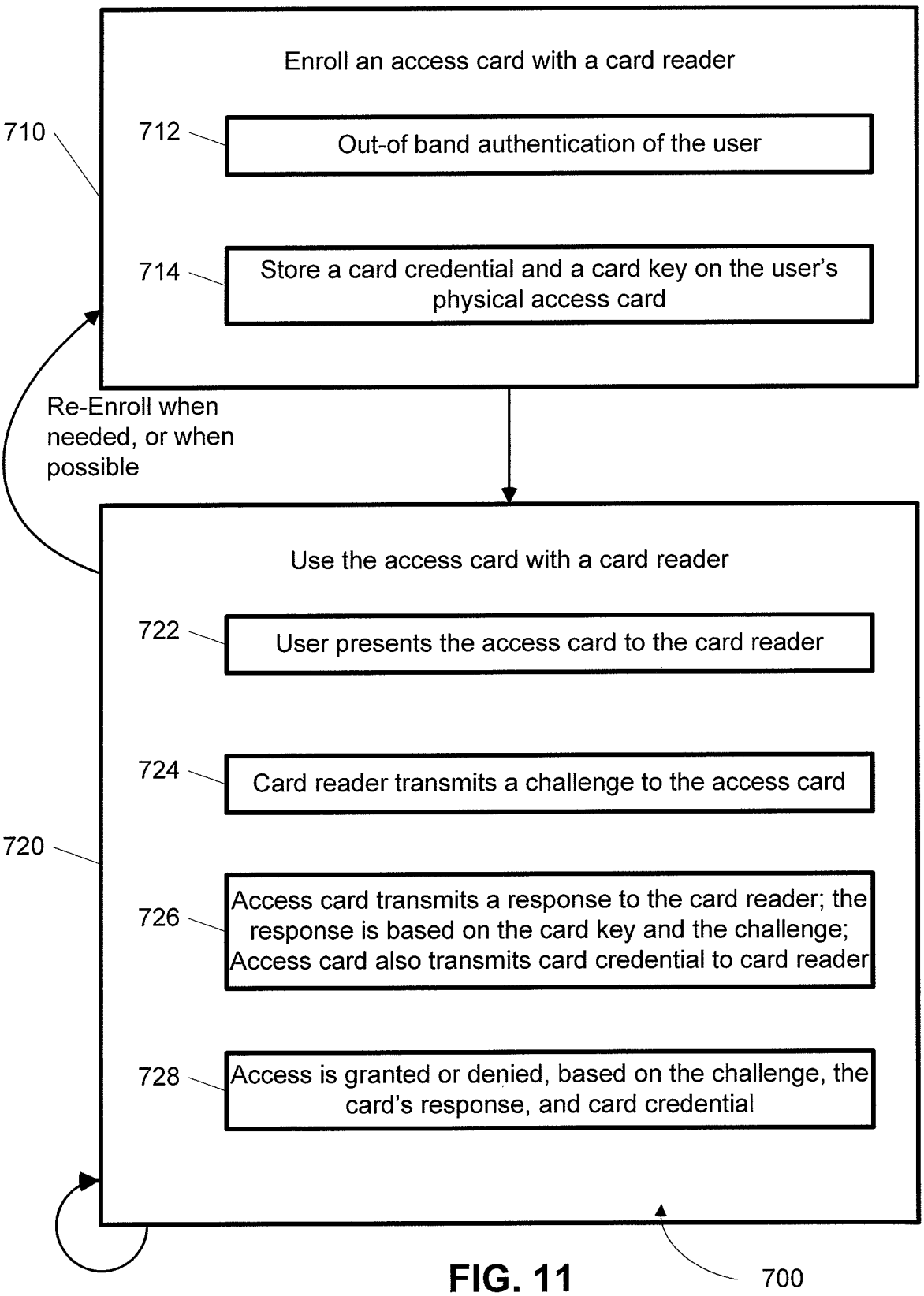
Enroll an access card with a card reader
710
712
Out-of band authentication of the user
714
Store a card credential and a card key on the user's physical access card
Re-Enroll when needed, or when possible
Use the access card with a card reader
722
User presents the access card to the card reader
724
Card reader transmits a challenge to the access card
720
726
Access card transmits a response to the card reader; the response is based on the card key and the challenge; Access card also transmits card credential to card reader
728
Access is granted or denied, based on the challenge, the card's response, and card credential
700

FIG. 11

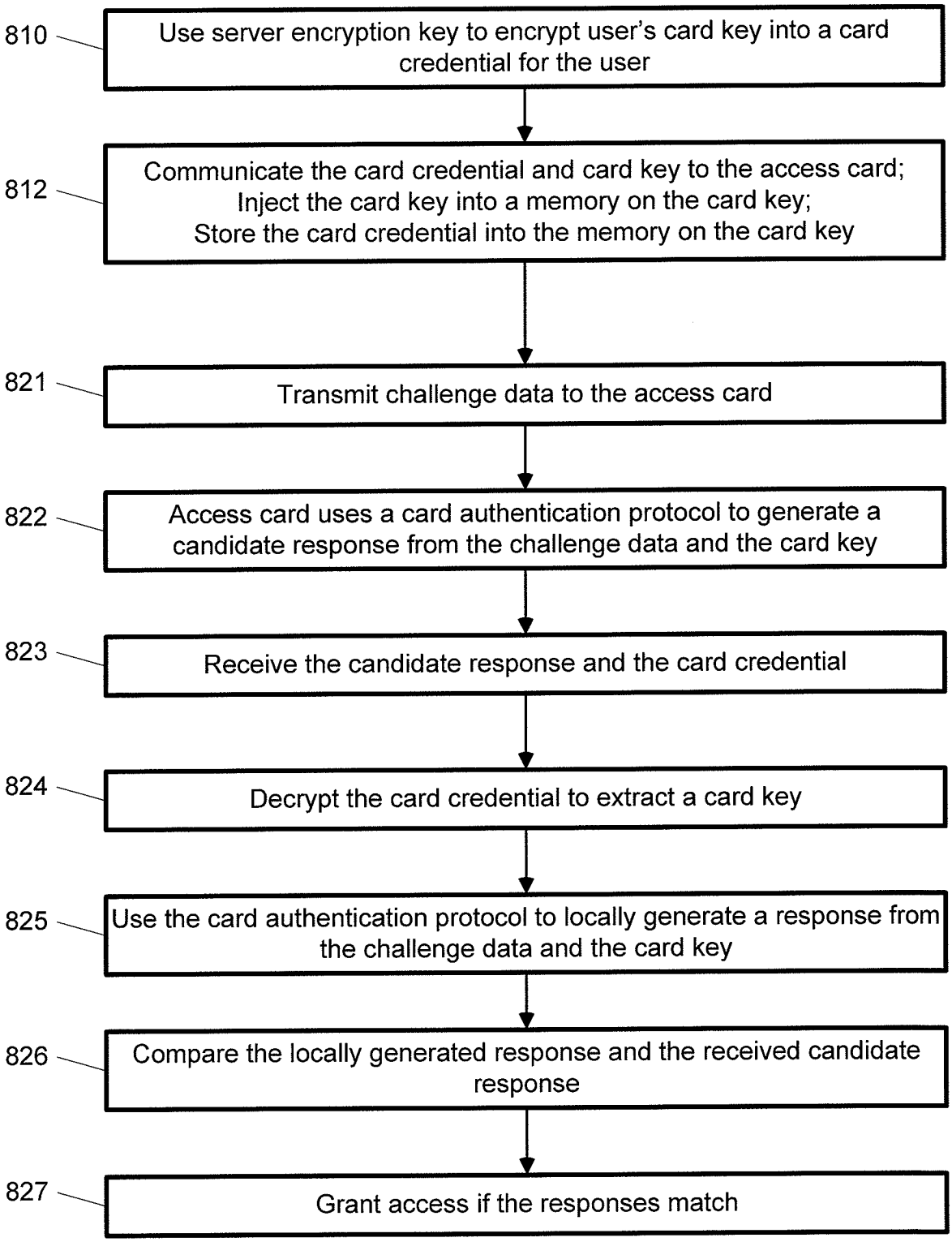
810
Use server encryption key to encrypt user's card key into a card credential for the user
812
Communicate the card credential and card key to the access card;
Inject the card key into a memory on the card key;
Store the card credential into the memory on the card key
821
Transmit challenge data to the access card
822
Access card uses a card authentication protocol to generate a candidate response from the challenge data and the card key
823
Receive the candidate response and the card credential
824
Decrypt the card credential to extract a card key
825
Use the card authentication protocol to locally generate a response from the challenge data and the card key
826
Compare the locally generated response and the received candidate response
827
Grant access if the responses match
800

FIG. 12

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2009/061567

A. CLASSIFICATION OF SUBJECT MATTER
INV. G07F7/10 G06F21/00

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G07F 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.
Y	NEUMAN B C ET AL: "A NOTE ON THE USE OF TIMESTAMPS AS NONCES" OPERATING SYSTEMS REVIEW, ACM, NEW YORK, NY, US, vol. 27, no. 2, 1 April 1993 (1993-04-01), pages 10-14, XP000360298 ISSN: 0163-5980 the whole document	1-30
Y	RANKL W ET AL: "Handbuch der Chipkarten, 4.Auflage, Kap. 10.3, 10.4 Lebenszyklus einer Chipkarte" HANDBUCH DER CHIPKARTEN, XX, XX, 29 August 2002 (2002-08-29), pages 638-656, XP002300685 the whole document	1-30

-/--

[X] 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
26 January 2010	09/04/2010
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Mäenpää, Jari

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FAN C I ET AL: "Robust remote authentication scheme with smart cards" COMPUTERS & SECURITY, ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, NL, vol. 24, no. 8, 1 November 2005 (2005-11-01), pages 619-628, XP025255747 ISSN: 0167-4048 [retrieved on 2005-11-01] page 1	1-30
A	John Clark, Jeremy Jacob: "A Survey of Authentication protocol Literature: Version 1.0"[Online] 17 November 1997 (1997-11-17), pages 1-109, XP002565102 Retrieved from the Internet: URL:http://www-users.cs.york.ac.uk/{jac/papers/drareviewps.ps> [retrieved on 2010-01-22] paragraph [6.5.2]	1-30
A	MENEZES A ET AL: "Handbook of Applied Cryptography KEY ESTABLISHMENT PROTOCOLS" 1 January 1997 (1997-01-01), HANDBOOK OF APPLIED CRYPTOGRAPHY; [CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS], CRC PRESS, BOCA RATON, FL, US, PAGE(S) 489 - 541 , XP002304953 ISBN: 9780849385230 paragraph [12.3] the whole document	1-30

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2009/061567

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.:

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.:

1-30

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: 1-30

Claims 1-30 directed to method, system and a computer-readable storage medium for access card authentication wherein an uncrypted copy of the card key is transmitted to the access card. The technical problem solved is to implement an authentication of low processing power access cards.

---

2. claims: 31-32

Claims 31 and 32 directed to a method and device for receiving key management information over a different interface from what is used for authentication and access requests using said key management information. The problem to be solved is to securely manage keys of access cards/processors.

---

3. claims: 33-35

Claims 33-35 directed to a system for obtaining key-management information from challenge data. The problem to be solved is to efficiently provide key-management information to processors.
