



(22) **Date de dépôt/Filing Date:** 2006/07/27

(41) **Mise à la disp. pub./Open to Public Insp.:** 2007/01/29

(45) **Date de délivrance/Issue Date:** 2014/05/06

(30) **Priorité/Priority:** 2005/07/29 (EP05107065.4)

(51) **Cl.Int./Int.Cl.** **G07C 11/00** (2006.01),  
**G07F 7/10** (2006.01)

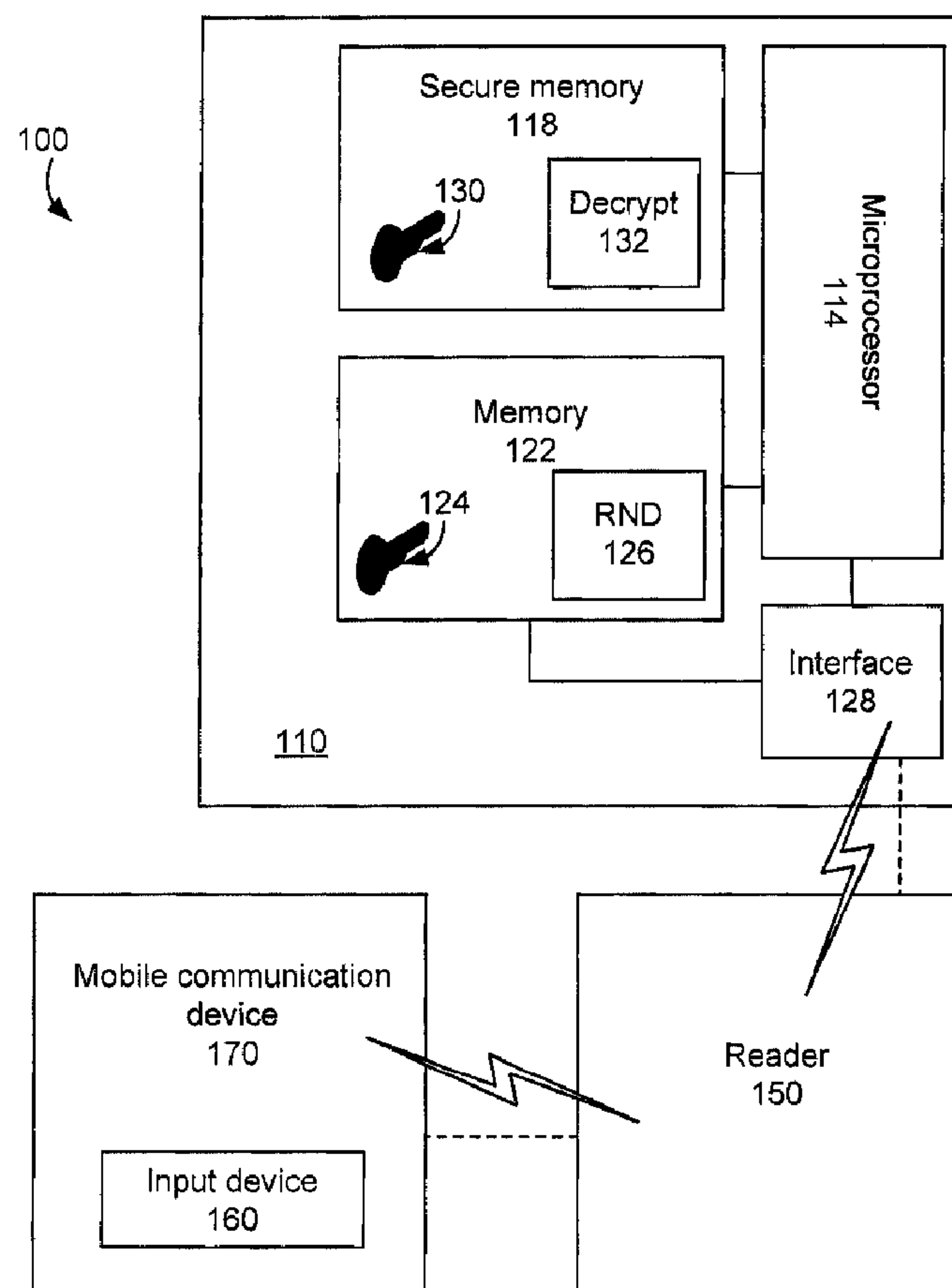
(72) **Inventeurs/Inventors:**  
BROWN, MICHAEL K., CA;  
ADAMS, NEIL P., CA;  
LITTLE, HERBERT A., CA

(73) **Propriétaire/Owner:**  
BLACKBERRY LIMITED, CA

(74) **Agent:** DIMOCK STRATTON LLP

(54) **Titre : SYSTEME ET METHODE POUR ENTRER UN NIP CHIFFRE DE CARTE INTELLIGENTE**

(54) **Title: SYSTEM AND METHOD FOR ENCRYPTED SMART CARD PIN ENTRY**



(57) **Abrégé/Abstract:**

A smart card, system, and method for securely authorizing a user or user device using the smart card is provided. The smart card is configured to provide, upon initialization or a request for authentication, a public key to the user input device such that the PIN or



**(57) Abrégé(suite)/Abstract(continued):**

password entered by the user is encrypted before transmission to the smart card via a smart card reader. The smart card then decrypts the PIN or password to authorize the user. Preferably, the smart card is configured to provide both a public key and a nonce to the user input device, which then encrypts a concatenation or other combination of the nonce and the user-input PIN or password before transmission to the smart card. The smart card reader thus never receives a copy of the PIN or password in the clear, allowing the smart card to be used with untrusted smart card readers.

## ABSTRACT

A smart card, system, and method for securely authorizing a user or user device using the smart card is provided. The smart card is configured to provide, upon initialization or a request for authentication, a public key to the user input device such that the PIN or password entered by the user is encrypted before transmission to the smart card via a smart card reader. The smart card then decrypts the PIN or password to authorize the user. Preferably, the smart card is configured to provide both a public key and a nonce to the user input device, which then encrypts a concatenation or other combination of the nonce and the user-input PIN or password before transmission to the smart card. The smart card reader thus never receives a copy of the PIN or password in the clear, allowing the smart card to be used with untrusted smart card readers.

## SYSTEM AND METHOD FOR ENCRYPTED SMART CARD PIN ENTRY

This invention relates generally to smart cards for authorizing users, and specifically to the encryption of personal identification numbers or passwords utilized  
5 to authenticate a user to a smart card.

Smart cards, also referred to as chip cards or integrated circuit cards, are devices with an embedded integrated circuit (such as a microprocessor and/or memory) for use as storage of sensitive data or user authentication. Smart cards may comprise memory for storing financial or personal data, or private data such as private  
10 keys used in the S/MIME (Secured Multipurpose Internet Mail Extensions) encryption technique. Preferably, some of this data may be secured using a PIN (personal identification number) or a password as an access control measure. In order to access the protected data stored in the card's memory, a user must be validated by providing the correct PIN or password.

15 Typically, the smart card does not include a data entry device for direct entry of a PIN or password for the purpose of user authentication. The smart card is typically used in conjunction with a smart card reader that is in communication with an input device. When the smart card is in communication with the smart card reader, a PIN or password may be provided in the clear by the user via the input device to the  
20 smart card reader. The reader may then pass the user-entered PIN or password on to the smart card for verification, so that the smart card can authenticate the user.

While this prior art smart card solution is satisfactory for hardware systems that are familiar to the user, such as smart card authentication systems used within a workplace environment where the smart card reader is trusted, such a system presents  
25 increased risk outside such environments where the hardware is not trusted. Because the PIN or password is provided by the user to the smart card reader in the clear, the smart card reader has access to this authentication information; the user does not know whether the smart card reader will retain a copy of the PIN or password, or pass the information on to an adversary.

Accordingly, it is desirable to provide a system and method for protecting the user's PIN or password at the time it is entered via the input device to ensure that such sensitive information is not captured or replicated by untrusted hardware.

#### Summary of the Invention

5           In accordance with a preferred embodiment, an enhanced smart card is provided for encrypting user-entered authentication data prior to reception by a smart card reader. The smart card comprises means adapted to store a private key, a public key, and predetermined authentication information, at least the private key being stored in a secure memory; means adapted for communicating with a smart card  
10   reader; means adapted for transmitting a challenge comprising at least the public key to a user device via the smart card reader; means adapted for receiving encrypted authentication information from the user device via the smart card reader, the encrypted authentication information being encrypted by the public key; means adapted for executing a decryption algorithm on the received encrypted authentication  
15   information using the private key to obtain decrypted authentication information; means adapted for comparing the decrypted authentication information with the predetermined authentication information; and means adapted for generating a verification signal if the decrypted authentication information and the predetermined authentication information match.

20           Preferably, the smart card further comprises means adapted for generating and storing a nonce, and the means adapted for transmitting a challenge are further adapted to transmit a challenge comprising at least the public key and the nonce, the means adapted for receiving encrypted authentication information are further adapted to receive encrypted authentication information wherein the information encrypted  
25   comprises the nonce, and the means adapted for comparing the decrypted authentication information are further adapted to compare the decrypted information with both the predetermined authentication information and a stored nonce. The smart card may also comprise means adapted to receive, via a smart card reader, a request for authentication from the user device. The private key may be used by the  
30   user device in digitally signing or decrypting electronic messages, but the smart card

or the user device may further comprise means adapted to store a further private key and a further public key for use in digitally signing or decrypting messages.

In a preferred embodiment, a system for authenticating a user device using a smart card is provided, comprising a smart card comprising a microprocessor and a memory for storing a private key, a public key, and predetermined authentication information, the memory comprising secure memory for storing at least the private key, and the microprocessor being configured to execute a decryption algorithm using the private key and to perform a comparison of the predetermined authentication information against received authentication information; a user device for receiving input from a user, the user device being configured to encrypt input; and a smart card reader for providing communication means between the smart card and the user device; wherein when the smart card is in communication with the user device via the smart card reader, the smart card is configured to transmit to the user device the public key, the user device is configured to encrypt input authentication information from a user using the public key and transmit the encrypted authentication information to the smart card, and the smart card is further configured to decrypt the received encrypted authentication information using the decryption algorithm and the private key such that the microprocessor may perform a comparison of the predetermined authentication information against the received authentication information, and such that the smart card reader never receives or communicates unencrypted authentication information. Preferably the microprocessor is further configured to generate a nonce and store the nonce in memory, such that when the smart card is in communication with the user device via the smart card reader, the smart card is configured to transmit the public key and the nonce, and the user device is configured to encrypt a concatenation of the nonce and input authentication information from a user using the public key and transmit the information thus encrypted to the smart card, and the smart card is further configured to decrypt the received encrypted information using the decryption algorithm and the private key such that the microprocessor may perform a comparison of the predetermined authentication information and the received nonce against the received authentication information and the stored nonce.

Also in a preferred embodiment, a method for authenticating a user device using a smart card is provided, comprising the steps of: providing a smart card comprising a microprocessor and a memory for storing a private key and a public key, the memory comprising secure memory for storing the private key, a decryption  
5 algorithm, and predetermined authentication information; transmitting a challenge to a user device, the challenge comprising the public key; receiving from the user device a response comprising received authentication information encrypted using the challenge; decrypting the received authentication information using the private key; comparing the received authentication information against the predetermined  
10 authentication information; if the received authentication information matches the predetermined authentication information, transmitting a verification signal to the user device. Preferably, the memory of the smart card is further provided with a nonce generation function, and the method further comprises the step of generating and storing a nonce, such that the step of transmitting a challenge to the user device  
15 comprises transmitting a challenge comprising the public key and the nonce, and the step of comparing the received authentication information further comprises a comparison of the stored nonce as well as the predetermined authentication information with the received authentication information.

The method may further comprise the steps of transmitting a request for  
20 authentication to the smart card before the step of transmitting a challenge to a user device; prompting a user of the user device to enter authentication information; encrypting, at the user device, the received authentication information using the challenge; transmitting to the smart card the encrypted received authentication information; and receiving a verification signal from the smart card. The user device  
25 may comprise a mobile communication device, and the method may further comprise the step of decrypting or digitally signing an electronic message upon receipt of the verification signal from the smart card.

#### Brief Description of the Drawings

In drawings which illustrate by way of example only a preferred embodiment  
30 of the invention,

Figure 1 is a block diagram of a smart card and smart card system.

Figure 2 is a flowchart of a method of authenticating a user using a smart card.

#### Detailed Description of the Preferred Embodiment

Referring to Figure 1, a preferred embodiment of a smart card system 100 is shown. The smart card system 100 comprises a smart card 110; a smart card reader 150; and an input device 160. The input device may be comprised in a mobile communication device 170. In the context of a mobile communication device 170, the smart card 110 may be used to authorize certain functions to be carried out by the mobile communication device 170, such as encryption, decryption, and digital signing of messages sent and/or received by the mobile communication device 170. If the input device 160 is comprised in a mobile communication device 170, then the mobile communication device 170 may communicate with the smart card reader 150 either by a direct wired connection, such as via USB (Universal Serial Bus) or by a wireless communication link in accordance with a standard such as the Institute of Electrical and Electronic Engineers (IEEE) 802.11a/b/g standard for wireless local area networks, Bluetooth®, Zigbee®, and the like, or future standards for wireless, preferably short-range, communication.

As will be appreciated by those skilled in the art, the smart card 110 may be a contact smart card or a contactless smart card. A contact smart card is preferably provided with a physical contact portion in accordance with ISO/IEC 7816 published by the International Organization for Standardization, which contact portion provides a interface with the smart card reader 150 for data communication between the card 110 and the reader 150, and further provides any necessary power to the card itself. Preferably, a contactless smart card is provided in accordance with ISO/IEC 10536, 14443, or 15693, which define standards for close-coupled, proximity, and vicinity smart cards, respectively. Contactless smart cards are not required to maintain physical contact with the reader 150 in order to function, but rather communicate with the reader 150 with an antenna and a radiofrequency interface, and are powered by an electromagnetic field generated at the reader 150. In the following description, the interface of the smart card 110 will be understood to comprise the portion of the smart

card, whether a contact or contactless smart card, which carries out the interface functionality of the smart card 110. A typical form factor for the smart card 110 is the “credit card” type form factor, although the smart card 110 may be comprised in another form factor or device that provides the functionality for communication with a smart card reader 150.

In a preferred embodiment, the smart card 110 is provided with a microprocessor 114 in communication with a secure memory 118 and a less secure memory 122. These components may be provided in an ASIC, or in multiple integrated circuits within the smart card 110. The microprocessor 114 is configured to execute any smart card operating system software, and other software applications, and further provides for the execution of various commands, such as memory-related commands to read information from and write information to the secure memory 118 (if the secure memory provided is read/write memory), or the less secure memory 122, which is preferably read/write memory, and security-related commands to perform authentication operations such as password checking. The microprocessor 114 and optionally the less secure memory 122 communicate with an interface 128, which in turn enables the exchange of information between the smart card 110 and the smart card reader 150. The content of the secure memory 122 is not available via the interface to a reader 150 except in accordance with a security-related command executed by the microprocessor 114. The secure memory 122 may be comprised within the microprocessor 114.

The secure memory 118 of the smart card 110 comprises a storage location for a key 130, such as a private key for use in S/MIME decryption or signing. The secure memory 118 further stores a decryption function 132, which is executable by the microprocessor 114, and also authentication information against which user-input authentication information, such as a PIN or password, may be compared in order to authenticate a user to the smart card. Preferably, the PIN or password is not stored in the clear, but rather is stored indirectly (for example, as a hash) in the secure memory 118. The less secure memory 122 stores a public key and/or a certificate containing the public key 124. A nonce generation function 126 may also be stored in the less secure memory 122, for execution by the microprocessor 114.

The smart card 110 is configured such that upon initialization, which takes place when the smart card 110 is activated by a smart card reader 150 and receives sufficient power from the smart card reader 150 to carry out smart card functions, it transmits a challenge comprising the public key 124 to the smart card reader 150. The reader 150 provides the challenge to the input device 160, which in turn is configured to receive from the user authentication information, such as a PIN or a password, for use in authenticating the user to the smart card 110. The input device 160 is further configured to encrypt the authentication information input by the user using the challenge data, i.e., the public key 124. The authentication information thus encrypted is transmitted from the input device 160 to the smart card reader 150, and from the smart card reader 150 to the smart card 110. The encrypted authentication information is passed to the decryption function 132, which accesses the private key 130 to decrypt the encrypted authentication information to obtain the PIN or password input by the user. The smart card 110 then executes a verification command to compare the decrypted authentication information to the previously stored authentication information in the secure memory 118. If the decrypted authentication information matches the previously stored authentication information, then the user is authorized by the smart card 110 and a verification signal is transmitted from the smart card 110 to the input device 160 via the reader 150. As will be appreciated by those skilled in the art, in this embodiment the user may be authenticated by the smart card 110 in communication with any reader 150, whether the reader 150 is trusted or not; the reader 150 at no time is provided with authentication information (i.e., a PIN or password) in the clear.

In a most preferred embodiment, the challenge comprises both the public key 124 and a nonce, which is generated either by the nonce generation function 126 or the microprocessor 114. Thus, the smart card 110 would be configured to generate a challenge upon initialization comprising the public key 124 and the nonce, and further to store the nonce temporarily in memory. The input device 160 would then encrypt the user's entered authentication information using the nonce and the public key 124, for example by concatenating the nonce with the authentication information. The decryption function 132 would then access both the private key 130 and the nonce

temporarily stored in memory by the smart card in order to decrypt the received encrypted authentication information during the verification step and determine the user-entered authentication information and the nonce. The smart card 110 would further be configured to utilize the temporarily stored nonce for a single authentication attempt; if the verification step failed, then the smart card 110, if configured to issue a further challenge to the user, would generate a new nonce and transmit this new nonce as part of the further challenge. By incorporating a nonce, the likelihood of a replay attack is minimized; even if a rogue smart card reader 150 captured the encrypted authentication information and a malicious user attempted to replay this encrypted authentication information at a later time, the verification would not be successful.

Turning to Figure 2, a preferred method for authenticating a user using the smart card described above is provided. The smart card 110 is detected by the smart card reader 150 at step 200. The detection may be by means of polling an interface in the smart card reader 150 until a signal is received indicating that a smart card 110 has been activated by the reader 150, and is ready to communicate with the reader 150. The smart card is then initialized at step 205, preferably by the operating system internal to the smart card 110. At step 210, optionally upon receipt of a request for authentication received from the smart card reader 150, the smart card 110 generates a challenge comprising at least the public key 124, but most preferably the public key 124 and a nonce generated using the generation function 126, and transmits this challenge to the smart card reader 150, which in turn signals the input device 160 to request authentication information (e.g., a PIN) from the user at step 215. The input device 160 encrypts the entered authentication information using the challenge at step 220. The encrypted authentication information is then transmitted to the smart card 110 via the reader 150 at step 225, and the smart card 110 decrypts the received encrypted authentication information at step 230 using the private key 130 and compares the decrypted information against the previously stored information on the smart card 110. If the information matches, then the smart card authorizes the user at step 235.

Such a method may be employed in a system for encrypting and decrypting messages using a mobile communication device 170. The mobile communication

device 170 may comprise the input device 160. When a user of the mobile communication device 170 wishes to digitally sign a message to be sent from the device 170, the user activates a smart card 110, causing the mobile device 170 to prompt the user for authentication information in accordance with the method  
5 described above. If the user is authenticated, then the mobile communication device 170 is configured to digitally sign the message. Similarly, when a user of the mobile device 170 in receipt of an encrypted message wishes to decrypt the message, the user may activate the smart card 110, proceed through the authentication process described above, and if the user is authenticated, the mobile communication device 170 is  
10 configured to decrypt the message. The decryption may make use of further keys stored in the secure memory 118 of the smart card 110, which are provided to the mobile communication device 170 only after the smart card 110 authenticates the user using the public/private key pair 124,130 stored on the card 110. As would be understood by those skilled in the art, the authentication of the user is necessary only  
15 when the user wishes to either sign a message or decrypt a message, since these activities typically require access to sensitive information, namely, a private key. It is not necessary for the user to be authenticated using the method described above if the user merely wishes to encrypt a message for a recipient, since that encryption may be carried out using the recipient's public key, which may be publicly available. Also, it  
20 will be understood that the public/private key pair that is ultimately used by the mobile communication device 170 for decryption or digitally signing a message need not be the same public/private key pair that is used by the smart card 110 to authenticate the user. A public/private key pair that is used by the mobile communication device 170 may be stored in memory resident in the mobile  
25 communication device 170, or may likewise be stored in memory on the smart card 110.

Various embodiments of the present invention having been thus described in detail by way of example, it will be apparent to those skilled in the art that variations and modifications may be made without departing from the invention. The invention  
30 includes all such variations and modifications as fall within the scope of the appended claims.

A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by any one of the patent document or patent disclosure, as it appears in the Patent and Trademark Office patent file or records, but otherwise reserves all  
5 copyrights whatsoever.

## WHAT IS CLAIMED IS:

1. A smart card for authentication at a user device, the smart card comprising:
  - means adapted to store a private key, a public key, and predetermined authentication information, at least the private key being stored in a secure memory;
  - means adapted to wirelessly communicate with a physically separate smart card reader;
  - means adapted for transmitting a challenge comprising at least the public key to the user device via the smart card reader over a wireless communication link;
  - means adapted for receiving encrypted user-entered authentication information from the user device via the smart card reader over the wireless communication link as a response to the challenge, the encrypted user-entered authentication information being encrypted by the public key;
  - means adapted for executing a decryption algorithm on the received encrypted user-entered authentication information using the private key to obtain decrypted user authentication information;
  - means adapted for comparing the decrypted user-entered authentication information with the predetermined authentication information; and
  - means adapted for generating a verification signal if the decrypted user-entered authentication information and the predetermined authentication information match.
  
2. The smart card of claim 1, further comprising means adapted for generating and storing a nonce, and wherein the means adapted for transmitting the challenge are further adapted to transmit a challenge comprising at least the public key and the nonce; the means adapted for receiving encrypted user authentication information are further adapted to receive encrypted user authentication information comprising the nonce; and the means adapted for comparing the decrypted user authentication information are further adapted to compare the decrypted user authentication information with both the predetermined authentication information and a stored nonce.

3. The smart card of either claim 1 or 2, further comprising means adapted to receive, via the smart card reader, a request for authentication from the user device.
4. The smart card of any one of claims 1 to 3, wherein the private key is used by the user device in digitally signing or decrypting electronic messages.
5. The smart card of any one of claims 1 to 3, further comprising means adapted to store a second private key and a corresponding second public key, the corresponding second private key being usable by the user device in digitally signing or decrypting electronic messages.
6. A system for authentication, the system comprising:
  - a smart card comprising a microprocessor and a memory for storing a private key, a public key, and predetermined authentication information, the memory comprising secure memory for storing at least the private key, and the microprocessor being configured to execute a decryption algorithm using the private key and to perform a comparison of the predetermined authentication information against received authentication information;
  - a user device for receiving user input, the user device being configured to encrypt input; and
  - a smart card reader physically separate from the user device and in wireless communication with the user device, for providing communication means between the smart card and the user device;
 wherein when the smart card is in communication with the user device via the smart card reader, the smart card is configured to transmit to the user device a challenge comprising the public key, the user device is configured to encrypt, using the public key, authentication information received as user input and to transmit the encrypted authentication information to the smart card via the smart card reader in response to the challenge, and the smart card is further configured to decrypt the encrypted authentication information thus received from the user device using the decryption algorithm and the private key to provide decrypted authentication information such that the microprocessor may perform a comparison of the predetermined authentication information against the decrypted authentication

information, and such that the smart card reader avoids receiving or communicating unencrypted authentication information.

7. The system of claim 6, wherein the smart card comprises a smart card as claimed in any one of claims 1 to 5.

8. The system of either claim 6 or 7, wherein the user device comprises a mobile communication device.

9. A smart card adapted for authentication, the smart card comprising:  
a memory adapted to store a private key, a public key, and predetermined authentication information, at least the private key being stored in a secure portion of memory;

an interface adapted to communicate with a smart card reader physically separate from a user device, wirelessly transmit a challenge comprising at least the public key to the user device via the smart card reader over a wireless communication link, and receive encrypted authentication information from the user device over the wireless communication link via the smart card reader in response to the challenge, the encrypted authentication information comprising user-entered authentication information encrypted by the public key; and

a processor adapted to execute a decryption algorithm on the received encrypted authentication information using the private key to obtain decrypted authentication information, compare the decrypted authentication information with the predetermined authentication information, and generate a verification signal if the decrypted authentication information and the predetermined authentication information match.

10. The smart card of claim 9, further comprising a processor adapted to generate a nonce for storage in the memory, and wherein the interface is adapted to transmit a challenge comprising at least the public key and the nonce and to receive encrypted authentication information comprising the nonce, and the processor for comparing the decrypted authentication information is configured to compare the decrypted

information with both the predetermined authentication information and a stored nonce.

11. The smart card of claim 10, wherein the private key is used by the user device in digitally signing or decrypting electronic messages.

12. The smart card of claim 10, wherein the memory is further adapted to store a second private key and a corresponding second public key, the second private key being usable by the user device in digitally signing or decrypting electronic messages.

13. The smart card of any one of claims 9 to 12, wherein the interface is configured to receive, via the smart card reader, a request for authentication from the user device.

14. An authentication method, comprising:

receiving, at a mobile communication device from a smart card via a smart card reader over a wireless communication link, a challenge comprising a public key;

transmitting, from the mobile communication device to the smart card over the wireless communication link via the smart card reader, a response to the challenge, the response comprising user authentication information encrypted using the challenge,

response being verifiable by the smart card by decrypting the encrypted user authentication information using a private key corresponding to the public key and matching the user authentication information thus decrypted with predetermined authentication information stored at the smart card.

15. The authentication method of claim 14, further comprising:

receiving a verification signal at the mobile communication device over the wireless communication link from the smart card, upon determination that user authentication information obtained by decrypting, using a private key corresponding to the public key, the encrypted user authentication information thus transmitted, matches predetermined authentication information, wherein the private key and the

predetermined authentication information are stored in secure memory in the smart card.

16. The method of either claim 14 or 15, further comprising the mobile communication device receiving the user authentication information via a user interface of the mobile communication device.

17. The method of any one of claims 14 to 16, wherein the challenge comprises a nonce generated and stored at the smart card, such that the user authentication information comprised in the response is encrypted using the challenge comprising the nonce, and wherein the encrypted user authentication information thus transmitted is decrypted at the smart card using the private key and the nonce.

18. The method of any one of claims 14 to 17, further comprising authenticating a user if the encrypted user authentication information thus decrypted matches predetermined authentication information.

19. The method of any one of claims 14 to 18, further comprising providing the mobile communication device access to a further private key stored in secure memory.

20. The method of any one of claims 14 to 19, wherein the user authentication information comprises a PIN or password.

21. An authentication method, comprising:

transmitting, from a smart card to an electronic device via a smart card reader communicating with the electronic device over a wireless communication link, a challenge comprising a public key;

receiving, at the smart card from the electronic device via the smart card reader, a response to the challenge, the response comprising input authentication information encrypted using the challenge;

decrypting the input authentication information thus encrypted using a private key corresponding to the public key; and

transmitting a verification signal from the smart card to the electronic device via the smart card reader upon determination that input authentication information thus decrypted matches predetermined authentication information stored at the smart card.

22. The method of claim 21, wherein the input authentication information is user-entered authentication information.

23. The method of either claim 21 or 22, wherein the electronic device is a user electronic device.

24. The method of any one of claims 21 to 23, wherein the electronic device is a mobile communication device.

25. The method of any one of claims 21 to 24, wherein the electronic device is physically separate from the smart card reader.

26. The method of any one of claims 21 to 25, wherein the input authentication information is received by the electronic device via a user interface.

27. The method of any one of claims 21 to 26, wherein the challenge comprises a nonce generated and stored at the smart card, such that the input authentication information comprised in the response is encrypted using the challenge comprising the nonce, and wherein decrypting the input authentication information thus encrypted comprises decrypting using the private key and the nonce.

28. The method of any one of claims 21 to 27, further comprising authenticating a user if the encrypted input authentication information thus decrypted matches the predetermined authentication information.

29. The method of any one of claims 21 to 28, further comprising providing the electronic device access to a further private key stored in secure memory.

30. The method of any one of claims 21 to 29, wherein the input authentication information comprises a PIN or password.
31. The method of any one of claims 21 to 30, wherein transmitting the challenge occurs in response to a received request for authentication.
32. The method of claim 31, further comprising:  
prompting for user input of authentication information at the electronic device upon receipt of the challenge at the electronic device;  
encrypting the input authentication information at the electronic device using the challenge;  
the electronic device transmitting the encrypted input authentication information to the smart card reader; and  
the electronic device receiving the verification signal.
33. The method of any one of claims 21 to 32, further comprising decrypting or digitally signing an electronic message upon receipt by the electronic device of the verification signal from the smart card.
34. The method of claim 33, wherein decrypting or digitally signing the electronic message comprises accessing a second private key for carrying out the decryption or digital signature.
35. A computer program product comprising a computer-readable medium storing executable program code therein, the executable program code being executable by one or more processors for implementing the method of any one of claims 14 to 34.
36. A method implemented at a mobile device, the method comprising:  
receiving, over a wireless link, a challenge comprising a public key stored by an authentication device;  
receiving user-entered authentication information;  
encrypting the user-entered authentication information using the public key;

transmitting, over the wireless link and in response to the challenge, the encrypted user-entered authentication information; and

receiving a verification signal over the wireless link once the encrypted user-entered authentication information is decrypted using a private key stored by the authentication device, and is determined to match authentication information previously stored by the authentication device.

37. The method of claim 36, wherein the mobile device receives the challenge from a reader device in communication with the authentication device, the reader device being configured to communicate with the mobile device over the wireless link.

38. The method of claim 36, wherein the challenge further comprises a value generated by the authentication device, and the generated value is used for encrypting the user-entered authentication information and decrypting the encrypted user-entered authentication information.

39. The method of claim 38, wherein the generated value is a nonce.

40. The method of claim 36, wherein the authentication device is a smart card.

41. A mobile device adapted to carry out the method of any one of claims 36 to 40.

42. A method performed by an authentication system, the method comprising:  
at a mobile device,

receiving, over a wireless link, a challenge comprising a public key stored by an authentication device;

receiving user-entered authentication information;

encrypting the user-entered authentication information using the public key; and

transmitting, over the wireless link and in response to the challenge, the encrypted user-entered authentication information; and

at the authentication device,

receiving the encrypted user-entered authentication information;

decrypting the encrypted user-entered authentication information using  
a private key stored by the authentication device;

determining that the user-entered authentication information obtained  
by decryption matches authentication information previously stored by the  
authentication device; and

transmitting a verification signal for receipt by the mobile device over  
the wireless link.

43. An authentication system, comprising:

a mobile device configured to communicate over a wireless link, the mobile  
device being adapted to:

receive, over the wireless link, a challenge comprising a public key  
stored by an authentication device;

receive user-entered authentication information;

encrypt the user-entered authentication information using the public  
key; and

transmit, over the wireless link and in response to the challenge, the  
encrypted user-entered authentication information; and

the authentication device, the authentication device storing a private key and  
authentication information and being adapted to:

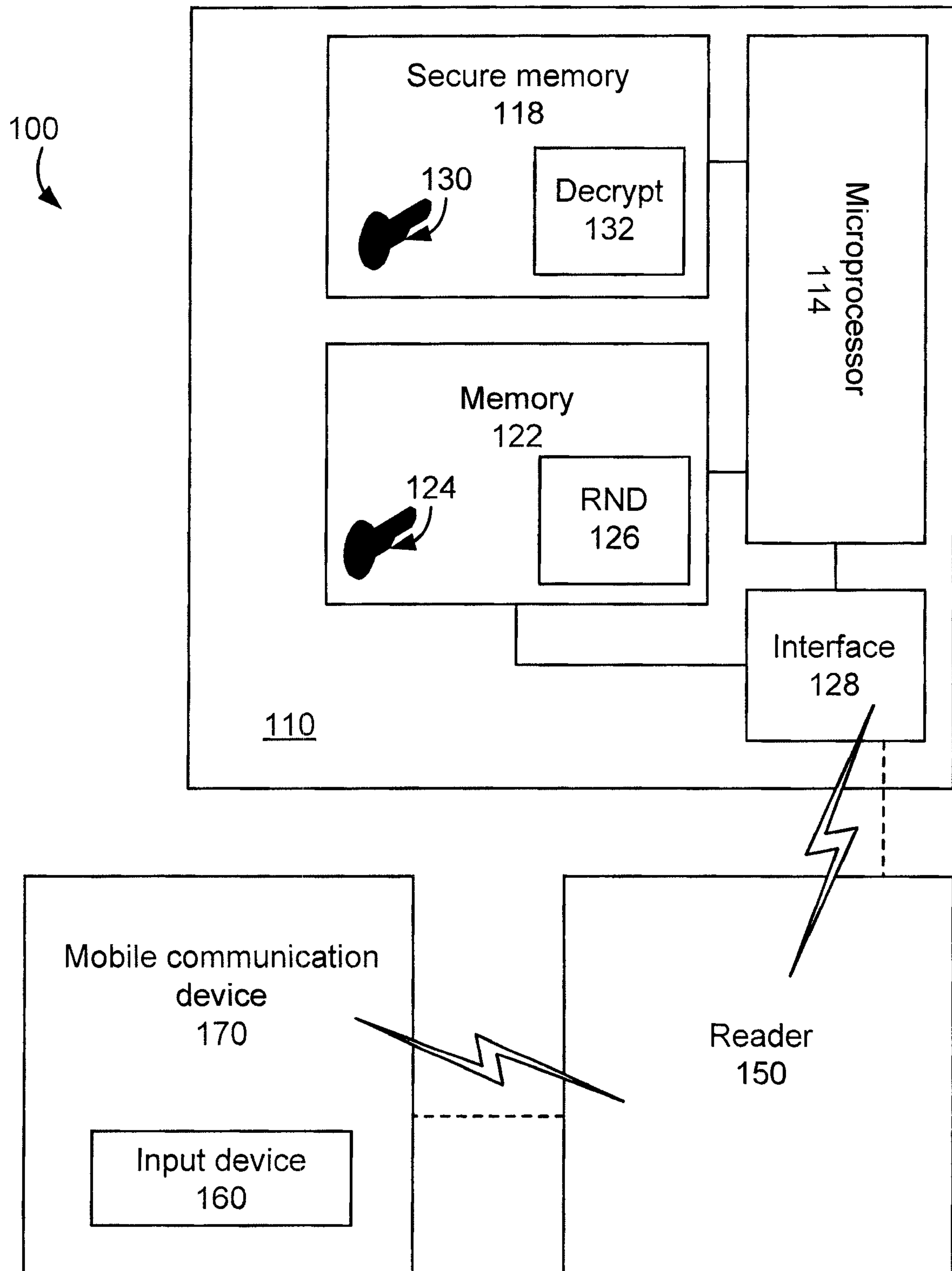
receive the encrypted user-entered authentication information;

decrypt the encrypted user-entered authentication information using  
the private key;

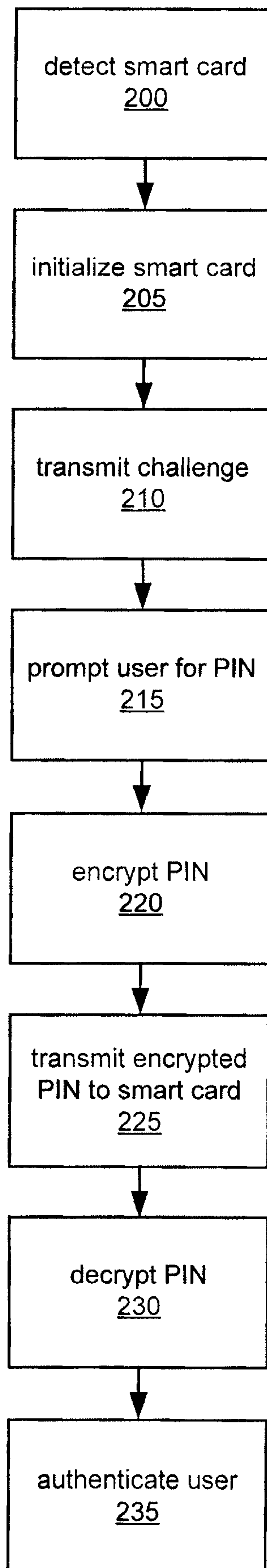
determine that the user-entered authentication information obtained by  
decryption matches the stored authentication information; and

transmit a verification signal for receipt by the mobile device over the  
wireless link.

1/2

**FIG. 1**

2/2

**FIG. 2**

100

