(12) STANDARD PATENT (11) Application No. **AU 2007217172 B2**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
Pin servicing

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

(21) Application No: **2007217172** (22) Date of Filing: **2007.02.19**

(87) WIPO No: **WO07/096590**

(30) Priority Data

(31) Number	(32) Date	(33) Country
0603662.8	**2006.02.23**	**GB**

(43) Publication Date: **2007.08.30**
(44) Accepted Journal Date: **2011.10.06**

(71) Applicant(s)
Barclays Bank PLC

(72) Inventor(s)
Taylor, David

(74) Agent / Attorney
Davies Collison Cave, 1 Nicholson Street, Melbourne, VIC, 3000

(56) Related Art
GB 2412774 B
US 5590198 A
US 4801787 A
US 2005/0166061 A1

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 August 2007 (30.08.2007)

PCT

(10) International Publication Number
WO 2007/096590 A1

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

(21) International Application Number:
PCT/GB2007/000560

(22) International Filing Date:
19 February 2007 (19.02.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0603662.8 23 February 2006 (23.02.2006) GB

(71) Applicant *(for all designated States except US)*: **BARCLAYS BANK PLC** [GB/GB]; Barclays Legal, Corporate & Commercial, 54 Lombard Street, London EC3P 3AH (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **TAYLOR, David** [GB/GB]; Barclays Bank Plc, Barclays Legal, Corporate & Commercial, 54 Lombard Street, London EC3P 3AH (GB).

(74) Agents: **CROSS, James, Peter, Archibald** et al.; R.G.C. Jenkins & Co., 26 Caxton Street, London SW1H 0RJ (GB).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, 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, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, 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, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

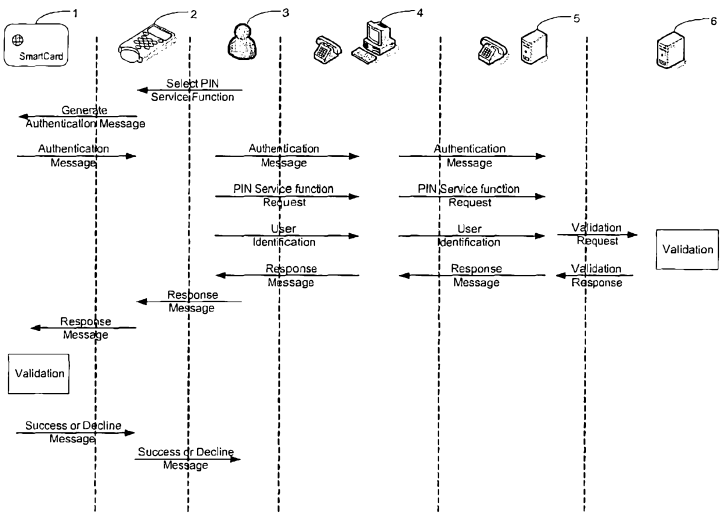
Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: PIN SERVICING



(57) Abstract: A smart card (1) interfaces with a smart card reader (2) to generate an authentication message (PSRQ), which is sent to a PIN servicing centre (5, 6). If the authentication message (PSRQ) is validated by the PIN servicing centre (5, 6), a validation response message (PSRS) is sent back to the user (3). The user (3) enters the validation response message (PSRS) on the reader (2), which authenticates the validation response message (PSRS) with the smart card (1); the PIN servicing function may then be performed. The smart card cryptographic messages are generated internally and solely by the smart card (1) - the reader (2) acts merely as an input mechanism into the smart card (1) or as an output mechanism from the smart card (1) to the display (10). The reader (2), therefore, does not need to contain any customer information or be personalised by the card issuer.

WO 2007/096590 A1

PIN Servicing

Field of the Invention

[0001] The present invention relates to method and system for PIN servicing.

Background of the Invention

[0002] In many transactions (financial or otherwise), a Personal Identification Number (PIN) is used to authenticate that the entity carrying out the transaction or service has proper authority to do so. Banks and credit card issuers provide their customers with a smart card containing a 'Reference PIN'. Commonly for these cards, during a transaction, the customer inputs their PIN into a smart card terminal such as a retailer point-of-sale device which in turn sends it to the smart card for comparison against the reference PIN held on the smart card. If the PIN sent by the terminal matches the Reference PIN, the authentication process has succeeded and it is deemed that the customer is the bona-fide holder of the smart card and, therefore, has the proper authority to carry out the transaction.

[0003] One of the problems in such a system is where the customer has forgotten the PIN. In this situation, the customer may attempt to guess the PIN and after a given number of invalid attempts (normally three) the smart card may become unusable i.e. unable to complete the current and any subsequent transactions. Although methods are available to render the smart card back to its original usable (unlocked) state, these methods normally involve the customer having to physically attend a specific secure terminal, most commonly the card issuer's or reciprocal Automated Teller Machine (ATM), and in the case where the PIN has been forgotten, the customer must first be re-advised of the PIN through the mailing of a secure letter containing the details of the PIN.

[0004] This situation is an inconvenience to customers as not only do they have to "unlock" their smart card at an ATM, but if the PIN has been forgotten there will be a delay before the re-advice of the PIN is received in the mail. The second problem is that for the bank or credit card issuing institution, there are costs associated with the inbound call from the customer to the call centre, the cost of issuing the PIN re-advice but, more importantly, the customer may defect to a competitor's product or use a different product where the PIN is known.

[0005] In another example, a SIM (Subscriber Identification Module) cards used in a digital mobile communication device, such a GSM (Groupe Speciale Mobile) 'phone, may be protected by a PIN so that the device can only be used when a valid PIN is entered. After a

given number of invalid PIN entries, the SIM is locked and can only be unlocked by obtaining an unlocking code from the service provider, following authentication of user details. It is desired to address or ameliorate one or more shortcomings of the prior art, or at least provide a useful alternative.

Summary

[0006] The present invention provides a method of performing a PIN service for a smart card, comprising:

a. initiating a PIN service request by selecting one of a plurality of possible PIN service functions;

b. generating an encrypted authentication message corresponding to the selected PIN service request;

c. sending the authentication message to a PIN servicing facility;

d. receiving from the PIN servicing facility an encrypted response message to the authentication message;

e. validating the response message against the selected PIN service request and, in response to successful validation; and

f. performing the PIN service for the smart card.

[0007] The present invention also provides an apparatus for performing a PIN service for a smart card, comprising:

a. means arranged to initiate a PIN service request by selecting one of a plurality of possible PIN service functions;

b. means arranged to generate an encrypted authentication message corresponding to the selected PIN service request;

c. means for sending the authentication message to a PIN servicing facility;

d. means for receiving from the PIN servicing facility an encrypted response message to the authentication message; and

e. means arranged to validate the response message against the PIN service request and, in response to successful validation, to perform the PIN service for the smart card.

Brief Description of the Drawings

[0008] Specific embodiments of the present invention will now be illustrated with reference to the accompanying drawings, as described below.

Figure 1 is a schematic diagram of a method of PIN servicing in an embodiment of the present invention.

Figure 2 is a representation of a smart card and a smart card reader in the embodiment.

Figure 3 is a more detailed diagram of the method as performed at the user side.

Figure 4 is a more detailed diagram of the method as performed at the service centre side.

Detailed Description

Overview

[0009] According to one aspect of the invention, there is provided a PIN servicing method in which a smart card interfaces with a smart card reader to generate an authentication message, which is sent to a PIN servicing centre. If the authentication message is validated by the PIN servicing centre, a validation response message is sent back to the user. The user enters the validation response message on the reader, which authenticates the validation response message with the smart card; the PIN servicing function may then be performed. For example, if the PIN servicing function is to disclose the reference PIN, then the PIN may be displayed on the smart card reader in response to authentication of the validation response message. If authentication is unsuccessful, the reader may display a suitable message.

[0010] Other PIN servicing functions may include changing the reference PIN held on the smart card to one selected by the user, resetting the number of PIN retries (i.e. unlocking the PIN after a given number of invalid entries) and/or resetting internal configurations or parameters held on the smart card.

[0011] The authentication and response messages preferably consist of dynamic one-time use codes such that the authentication and response messages vary on each PIN service

function requested by the user. In a preferred implementation, the messages are generated using a cryptographic key and one or more counters held within the card using a symmetric key based cipher algorithm such as DES or AES. As the messages only work one time, this provides protection against a user legitimately obtaining a message value but writing it down or storing it, allowing it to be subsequently fraudulently replayed. In a preferred embodiment, the authentication request message and response message are mathematically derived and related so that in order for the PIN servicing function to succeed, the bona-fide smart card must have taken part in the generation of the original authentication message and the authentication of the response message. This binding of messages also protects against the transaction being 'torn' (i.e. messages used at different times from the original transaction) and ensures integrity as both the card and issuer systems mutually authenticate one another.

[0012] An important feature of embodiments of the invention is that the smart card cryptographic messages are generated internally and solely by the smart card - the reader acts merely as an input mechanism into the smart card or as an output mechanism from the smart card to the display (or if in a connected environment, to the connected upstream system). The reader, therefore, does not need to contain any customer information or be personalised by the card issuer and in an unconnected environment, the reader does not need to contain any physical security features other than a form of tamper evidence.

[0013] A method of PIN servicing according to an embodiment of the invention is shown schematically in Figure 1. A user 3 inserts their smart card 1 into a reader 2 and selects the required PIN Servicing Function. The smart card 1 generates an authentication message which is displayed by the reader 2. The user 1 reads the authentication message from a

display of the reader 2 and sends the authentication message, details of the requested PIN servicing function and information to identify the user (i.e. user identification information) via a user interface component 4 (such as a terminal connected to the internet or IVR (Interactive Voice Response) system or voice call using a telephone) to a request receiving component 5, such as a voice system, web server or IVR system.

[0014] The request receiving component 5 sends the information received to one or more validation components 6. The validation component 6 validates the authentication message and, where applicable, the information identifying the user requesting the PIN service. The validation component 6 then generates a validation response message, the contents of which may be dependent on the PIN servicing function requested by the user. The validation response message is transmitted to the request receiving component 5 which in turn relays the validation response message to the user interface component 4 and thereby back to the user 3.

[0015] The user 3 enters the validation response message into the reader 2 which transmits it to the smart card 1 for authentication. If the smart card 1 successfully validates the response message, a success message is generated and returned by the smart card to the reader 2, which success message is then displayed on the reader display. Otherwise, a decline message is generated and returned to the reader 2 for display. One or more success or decline messages may be used. The contents of the success or decline message will be context-specific to the PIN servicing function request and whether the validation was successful or not. For example, where the requested PIN servicing function is to return the value of the PIN stored on the smart card 1, the PIN would be sent back by the smart card 1 and displayed by the reader 2 in the success message.

Specific details of the embodiment

[0016] Figure 2 shows the details of the reader 2, which comprises a numeric keypad 8, function keys 9 corresponding to different PIN servicing functions, an enter key 12 for confirming entries, a display 10 for displaying messages and echoing key presses, and a smart card reader slot 11. Any smart card 1 conforming to the relevant standards (such as ISO-7816 or EMV) can be inserted into the smartcard reader slot 11 by the user. The smart card 1 includes contacts 7 for electrical connection to corresponding contacts within the slot 11, although a contactless connection may be used instead.

[0017] In an alternative embodiment, the functions of the reader 2 could be incorporated into the smart card 1: for example, the smart card may include the numeric keypad 8' and

display 10. Whilst this arrangement would increase the complexity of the smart card and require an integrated power source, it is feasible with current technology and further technological advances are likely to make this arrangement more attractive.

[0018] In another alternative embodiment, the smart card 1 could include a wireless link interface, such as a Bluetooth™ interface, for connection to a wireless device having a keyboard and a display, which then functions as the reader 2. The wireless device could be a Bluetooth™-enabled smartphone or PDA (personal digital assistant), for example, that runs a reader application providing the functions of the reader 2.

[0019] In another alternative embodiment, the reader 2 could provide a wired or wireless interface to a device having a screen and a keyboard, such as a computer. For example, the reader 2 could comprise a smart card interface and a USB (universal serial bus) interface to the computer, which runs a reader application.

[0020] Referring now to Figures 3 and 4: to perform a PIN service function, the user 3 inserts the card 1 into the reader 2 and selects the required function using one of the function keys 9 on the reader 2. The reader 2 sends a request to the card 1 for it to generate a PIN Servicing Request Cryptogram (PSRQ) using a cryptographic algorithm 13 and a cryptographic key held internally within the card 1 and, preferably, including an incremental counter also held within the card 1. The PSRQ contains the result of the cryptographic process as well as sufficient details of the counter to be passed back to the validation component 6 to authenticate the cryptogram.

[0021] In some implementations, other data may also need to be contained within the PSRQ related to the cryptographic process, such as pointers to data elements required by the validation component 6 e.g. master cryptographic derivation keys. The PSRQ is returned by the card 1 to the reader 2, which displays the PSRQ on the reader display 10.

[0022] The PSRQ is passed by the user 3 to the request receiving component 5 via the user interface component 4, which may be, for example, a telephone, web form or other transmission device. As well as the PSRQ, the user 3 also sends to (or provides on request by) the request receiving component 5 the following:

User identification – comprising sufficient material for the validation component 6 to verify the identity of the user –such as date of birth, mother's maiden name and/or memorable words. The type of user identification may be requested by the receiving component 5 where this is interactive, such as a call centre agent or web page.

Card Data - for example, the card account number.

PIN Servicing Request Function (PSRF) – a mnemonic, phrase, word or code representing the PIN servicing function that the user 3 wants to perform.

[0023] Once received from the user interface component 4, the request receiving component 5 sends the data to the validation component 6; this may comprise a number of sub-components or processes that verify the customer identification 17 by looking up expected values using the card data. In addition to this process, the validation component 6 passes the PSRQ, PSRF and card data to verify the card cryptogram to a cryptogram validation process 18. The cryptogram validation process 18 may retrieve data from the card database such as pointers to cryptographic master keys, algorithms and key indexes. The main objective of this part of the cryptogram validation process 18 is to ensure that the request from the user originates from a genuine card. To protect against the replaying of PSRQ messages in subsequent requests, in a preferred embodiment the cryptogram validation component 6 employs a process to keep track of historical card counters. Thus, if the counter transmitted in the PSRQ or derived from the PSRQ is found to be less or equal to the historically held value, then the process will abort.

[0024] If the cryptogram validation process has successfully verified the requesting cryptogram, a further cryptogram will be generated as a PIN service response message (PSRS) 19. In a preferred embodiment, the generation of the PSRS will use data from the original PSRF to cryptographically combine the request and response messages. The PSRS may also combine a value of the original PSRF to ensure that the PIN service response matches the request and also, for greater security, ensure that the PIN service requested by the user 3 cannot be changed into a different service or altered during the transaction, such as changing a PIN unlock function to a PIN display function.

[0025] The PSRS message generated by the cryptogram generation process 19 is transmitted to the user via the validation component 6 and the request receiving component 5. The user 3 submits the PSRS to the card 1 by typing it into the card reader keypad 8.

[0026] To validate the PSRS 14, the card uses the original PSRQ and PSRF to generate its own internal PSRS which it then compares to the PSRS transmitted by the reader 2. Dependent on the usability and display characteristics, the card 1 may have to compare the results of partial cryptograms – such as the rightmost 'n' bytes of the cryptogram where 'n' is either the maximum length of the reader display 10 or the maximum length of digits practical for the user 3. It may, for example, be deemed impractical for users to key in 8-byte cryptograms.

2007217172 13 Sep 2011

[0027] Successful validation requires that the PSRS internally calculated by the card 1 equals that received by the reader 2. If successful, dependent on the PSRF, the security access conditions internally maintained by the card will allow an internal smart card function to either change the PIN status to 'unlock' or transmit the 'Reference PIN' held in the smart card, dependent on the PIN service request. The PSRF therefore has a direct effect on the type of response from the smart card 1 to the reader 2 - either an "OK/Success" status or the value of the clear text 'Reference PIN'.

Alternative Embodiments

[0028] The embodiments described above are illustrative of rather than limiting to the present invention. Alternative embodiments apparent on reading the above description may nevertheless fall within the scope of the invention.

[0029] Throughout this specification and the claims which follow, unless the context requires otherwise, the word "comprise", and variations such as "comprises" and "comprising", will be understood to imply the inclusion of a stated integer or step or group of integers or steps but not the exclusion of any other integer or step or group of integers or steps.

[0030] The reference in this specification to any prior publication (or information derived from it), or to any matter which is known, is not, and should not be taken as an acknowledgment or admission or any form of suggestion that that prior publication (or information derived from it) or known matter forms part of the common general knowledge in the field of endeavour to which this specification relates.

2007217172 13 Sep 2011

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A method of performing a PIN service for a smart card, comprising:

   a. initiating a PIN service request by selecting one of a plurality of possible PIN service functions;

   b. generating an encrypted authentication message corresponding to the selected PIN service request;

   c. sending the authentication message to a PIN servicing facility;

   d. receiving from the PIN servicing facility an encrypted response message to the authentication message;

   e. validating the response message against the selected PIN service request and, in response to successful validation; and

   f. performing the PIN service for the smart card.

2. The method of claim 1, wherein the authentication message comprises a one time cryptogram.

3. The method of claim 2, wherein the cryptogram is generated by the smart card.

4. The method of any preceding claim, wherein step c includes transmitting to the PIN service facility user identification information identifying an authorised user of the card.

5. The method of any preceding claim, wherein step f further includes displaying a PIN service message indicating successful validation.

6. The method of claim 4, wherein step f is performed by a smart card reader connected to the smart card.

7. The method of any preceding claim, wherein step b and/or step e is performed by the smart card.

8. The method of claim 7, wherein step e includes providing the response message to the smart card by means of a smart card reader connected to the smart card.

2007217172 13 Sep 2011

9. The method of any preceding claim, wherein step a is performed by a smart card reader connected to the smart card.

10. The method of claim 9, wherein the smart card reader aincludes a plurality of function keys for selection of a corresponding one of the PIN services.

11. The method of any preceding claim, further comprising, at the PIN servicing facility, between steps c and d, validating the authentication message and generating the response message in response to successful validation of the authentication message.

12. The method of claim 11, wherein the authentication message includes a component that varies between PIN service requests for the smart card according to a predetermined relationship, and the authentication message is validated against the predetermined relationship.

13. Apparatus for performing a PIN service for a smart card, comprising:

a. means arranged to initiate a PIN service request by selecting one of a plurality of possible PIN service functions;

b. means arranged to generate an encrypted authentication message corresponding to the selected PIN service request;

c. means for sending the authentication message to a PIN servicing facility;

d. means for receiving from the PIN servicing facility an encrypted response message to the authentication message; and

e. means arranged to validate the response message against the PIN service request and, in response to successful validation, to perform the PIN service for the smart card.

14. The apparatus of claim 13, wherein the means arranged to initiate the PIN service request comprises a smart card reader.

15. The apparatus of claim 14 , wherein the smart card reader includes a plurality of function keys for selection of a corresponding one of the PIN services.

16. A method of performing a PIN service for a smart card, substantially as hereinbefore described with reference to the accompanying drawings.

17. An apparatus for performing a PIN service for a smart card, substantially as hereinbefore described with reference to the accompanying drawings.

Fig. 1

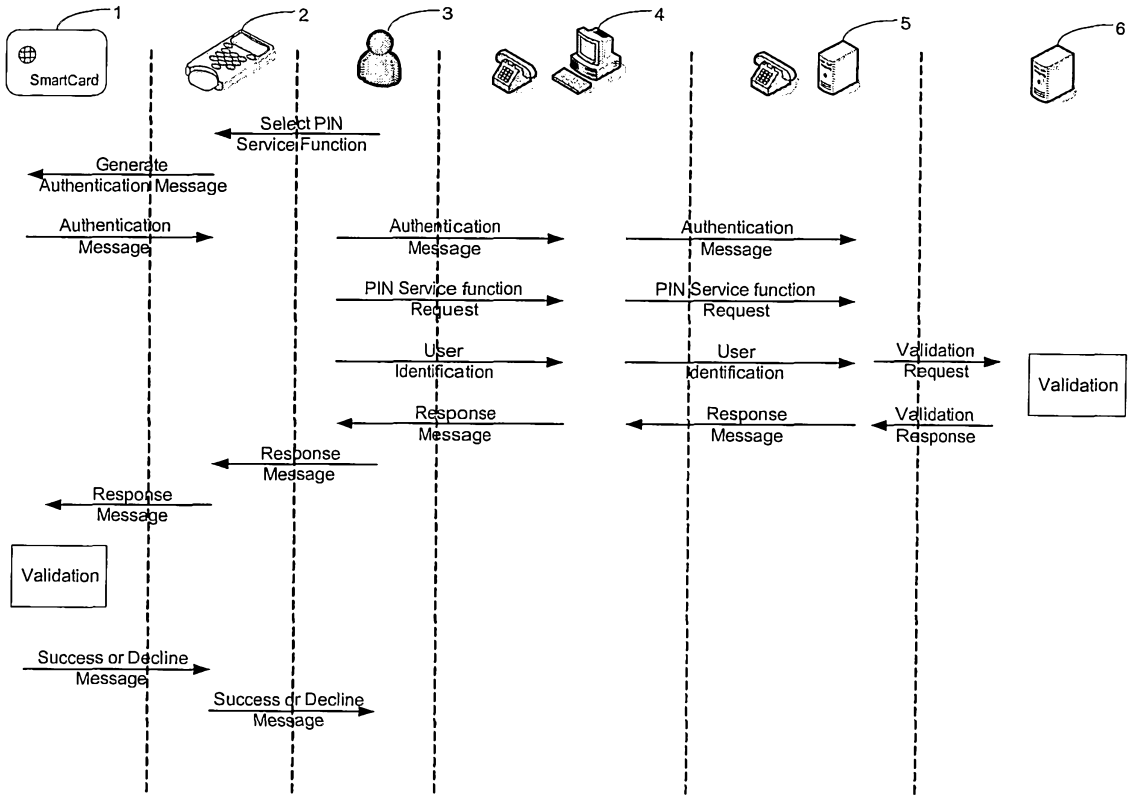

1
2
3
4
5
6
SmartCard
Select PIN Service Function
Generate Authentication Message
Authentication Message
Authentication Message
Authentication Message
PIN Service function Request
PIN Service function Request
User Identification
User Identification
Validation Request
Validation
Response Message
Response Message
Validation Response
Response Message
Response Message
Validation
Success or Decline Message
Success or Decline Message

Fig. 2

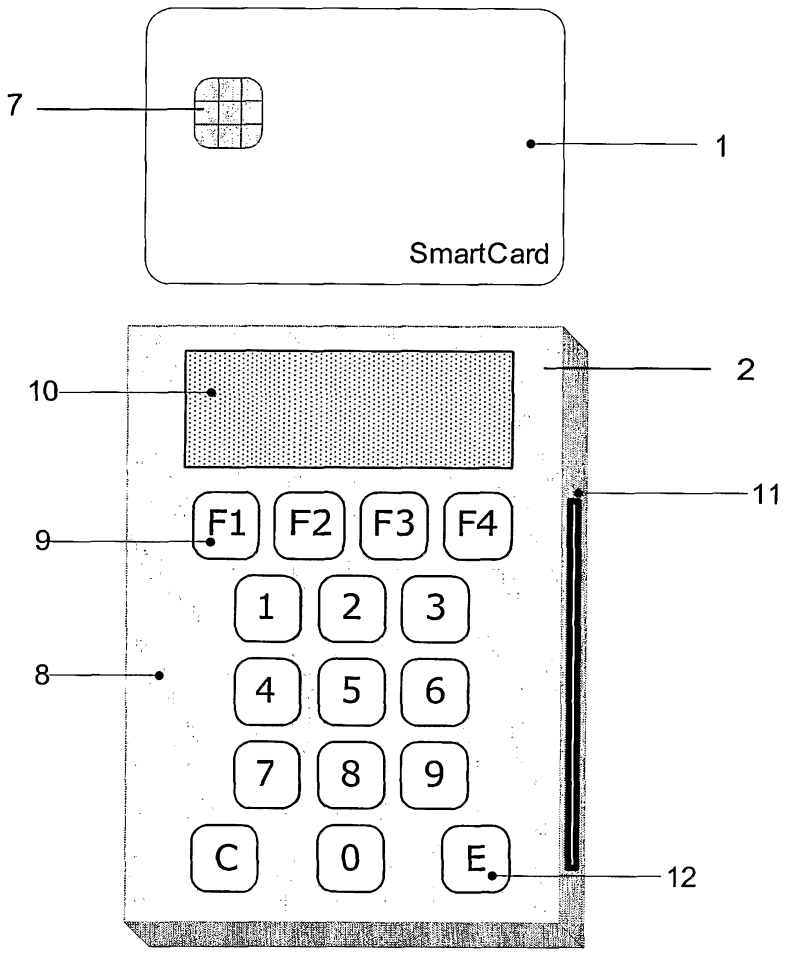


Fig. 3

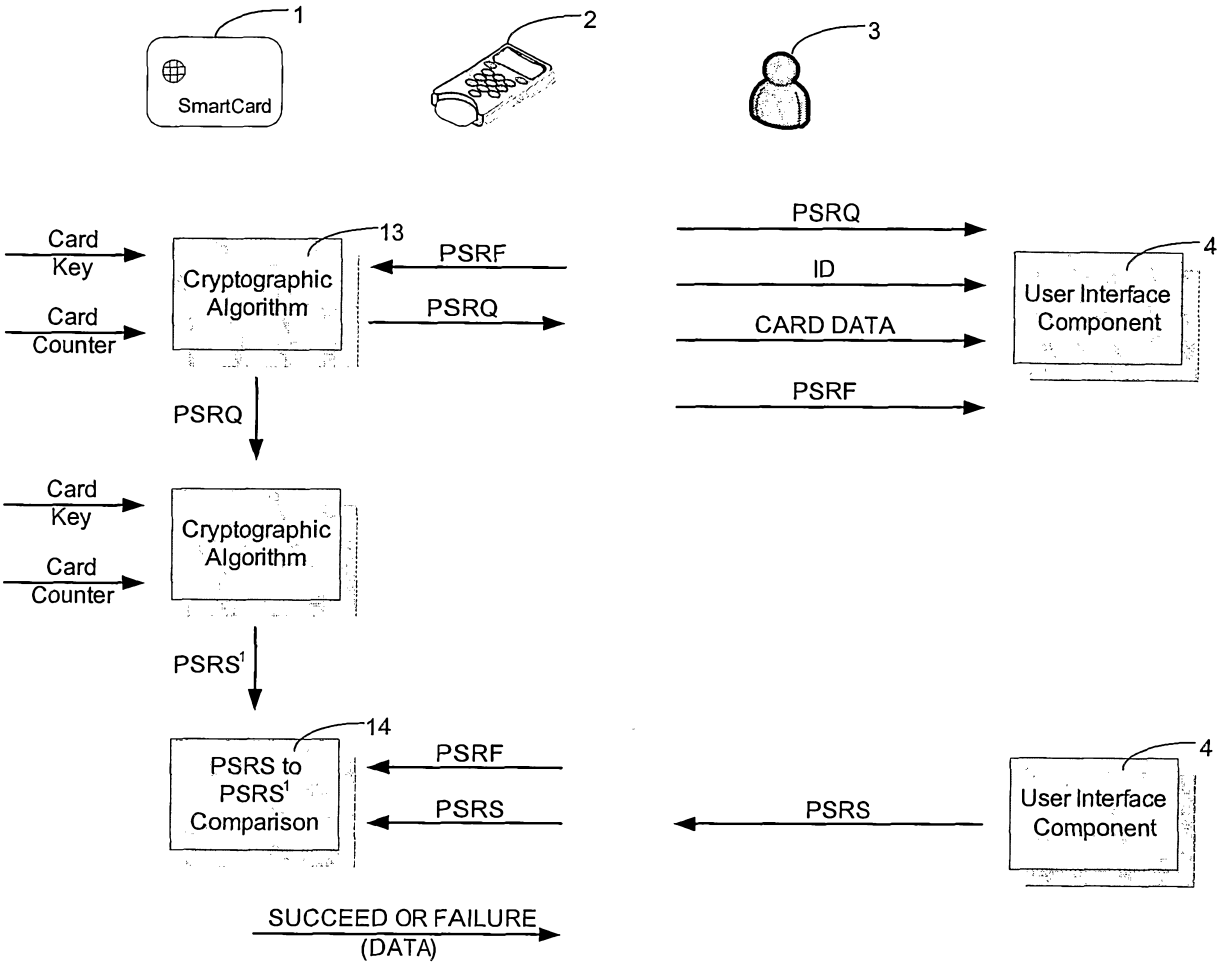
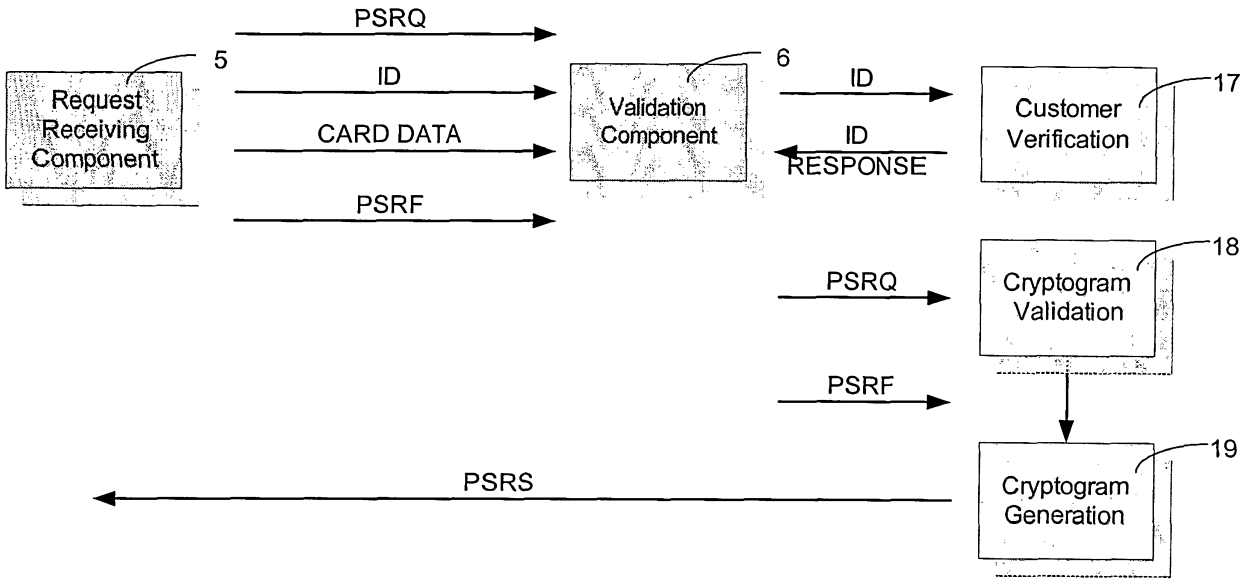

1
SmartCard
2
3
PSRQ
ID
CARD DATA
PSRF
4
User Interface Component
Card Key
Card Counter
13
Cryptographic Algorithm
PSRF
PSRQ
PSRQ
Card Key
Card Counter
Cryptographic Algorithm
PSRS1
14
PSRS to PSRS1 Comparison
PSRF
PSRS
PSRS
4
User Interface Component
SUCCEED OR FAILURE
(DATA)

Fig. 4


PSRQ
ID
CARD DATA
PSRF
5
Request Receiving Component
6
Validation Component
ID
ID RESPONSE
Customer Verification
17
PSRQ
PSRF
Cryptogram Validation
18
Cryptogram Generation
19
PSRS