



166166

Title: System for electronic delivery of a personal identification code.

Technical Field

The invention relates to a system for electronic delivery of a PIN (Personal Identification Number) code and comprising a server secured by means of a number
5 of encryption keys and provided with a reference code for generating the PIN code, said system further comprising means for encrypting the reference code and the PIN code generated by means of the encryption keys and via connected communications means being adapted to transmit a SMS (Short Message Service) message containing
10 an electronic signature based on the reference code to a SIM (Subscriber Identity Module) card connected to a terminal with input and display means.

Background Art

Personal identification numbers, so-called PIN codes, are presently used in many different situations, in particular in connection with economic transactions, in which a credit card or a similar means of payment is used together with a terminal. The
15 information stored on the credit card is verified by the card user during completion of the transaction by entering a PIN code on the terminal's keyboard, said code being agreed with the card issuer. It is thus ensured that the user of the card is identical to the owner of the card.

The PIN code is usually assigned to the credit card in connection with the issuance
20 thereof and generally forwarded to the user under separate cover as ordinary mail. This method is neither completely secure nor very fast, as it may take several days for the letter to reach the card owner and thus before the owner can use his card.

WO 99/39524 relates to telecommunication systems and discloses a procedure and a system for transmission of encrypted SMS messages to a mobile station. The system



G00001

comprises a telecommunication network, a mobile station connected to it and a subscriber identity module (SIM) connected to the mobile station, a message switching centre, and transmission software connected to the message switching centre. The transmission software comprises applications and parameters of the encryption
5 algorithm to be used. Hereby, SMS messages may be generated and sent to the mobile station via the message switching centre. The SIM card in the mobile station is adapted for receiving and storing an encrypted SMS message.

Brief Description of the Invention

The object of the invention is to provide a secure, fast and efficient system which is
10 able to deliver PIN codes to the customers in a more advantageous manner.

A system of the above type is according to the invention characterised in that

said server is adapted for receiving unique information in the form of a reference code, said encryption means is adapted for computing a first electronic signature based on the reference code, and the server being adapted for transmitting the first electronic
15 signature as encrypted electronic information in said SMS message, and

said SIM card comprises means for comparing the first electronic signature in the SMS message with a second electronic signature being generated from a reference code entered by a user of the terminal and by means of a corresponding encryption key in the SIM card, and means for allowing subsequent display of a PIN code associated
20 with the signatures on the display means of the terminal, if the first electronic signature and the second electronic signature match.

It is thus only possible to be advised of a PIN code, if the user of a specific terminal enters the associated reference code. The exchange of the PIN code and the reference code is made exclusively in form of encrypted data signals which can only be

decrypted by using the two unique encryption keys. A high degree of security delivery of PIN codes is thus obtained.

Furthermore according to the invention said SIM card is adapted for being provided with the PIN code when supplying the SIM card with a unique identity code. Hereby,
5 the PIN code never needs to be transmitted and therefore unauthorised decryption of the PIN code can be prevented.

Moreover, according to a preferred embodiment of the invention, said SIM card is adapted to receive the PIN code in the form of an encrypted data signal.

The invention also relates to a mobile telephone comprising a terminal with input
10 means and display means, and a SIM card including means adapted for receiving and storing an encrypted SMS message, characterised in that the SIM card comprises:

comparator means adapted for comparing a first electronic signature in the encrypted SMS message with a second electronic signature being generated from a reference code entered by a user of the terminal and by means of a corresponding encryption key in
15 the SIM card, and

means for allowing subsequent display of a PIN code associated with the signatures on the display means of the terminal, if the first electronic signature and the second electronic signature match.

Preferred embodiment of the mobile phone according to the invention is claimed in the
20 dependent claims 5 and 6.

Finally, the invention relates to a SIM card including storage means adapted for receiving and storing an encrypted SMS message, characterised in that said SIM card comprises:

encryption means adapted for generating a second electronic signature from a reference code entered by a user of the terminal and by means of a corresponding encryption key in the SIM card, and

comparator means adapted for comparing a first electronic signature in the encrypted
5 SMS message with said second electronic signature and transmitting a signal to a control means indicating that a PIN code is to be delivered to a user.

Preferred embodiment of a SIM card according to the invention are claimed in the dependent claims 8 and 9.

Brief Description of the Drawing

10 The invention is explained in greater detail below with reference to the accompanying drawing illustrating a flow chart of a preferred embodiment of the invention.

Best Mode for Carrying Out the Invention

The system for electronic delivery of a PIN code shown in the drawing comprises a secured server 3 adapted to receive unique information 1 (illustrated as a chart for
15 filling-in personal data) in form of reference codes 2, and encryption means 4 subsequently computing the electronic signature 5 based on the reference code 2 in the server 3. The server 3 communicates with a so-called over-the-air platform 6 (OTA) communicating with a SMS service centre 8 adapted to receive encrypted information 7 from the platform 6. The SMS service centre 8 is connected to a SIM
20 card 10 which communicates with a mobile handset 12 of the GSM type comprising a keyboard 13 and a display means in form of a display 14, said service centre being able to transmit completed SMS messages to the SIM card 10. The SIM card 10 comprises a storage 11 for storing encrypted SMS messages 9, encryption means 16 for encrypting data 15 entered by a user of the terminal 12 via the keyboard 13 and

comparison means 17 connected to the storage 11 and the keyboard 13 for comparing the stored data with entered data. The comparison means 17 are further connected to means 18 for displaying the PIN code on the display 14 of the terminal 12.

When using the system the user delivers unique information 1 in form of a reference code 2 to the secured server 3. The reference code 2 is used as an input signal for generating an electronic signature 5 in the server 3 by means of the encryption means 4. The electronic signature 5 is transmitted via the over-the-air platform 6 to the SMS service centre 8 for administration of the SIM card, said service centre 8 converting the electronic signature 5 to a SMS message 9 suitable for transmission thereof to the SIM card 10 in question connected to the mobile handset 12. The SIM card 10 comprises a storage 11 adapted to receive and store the encrypted SMS message 9. The comparison means 17 are used for comparing the electronic signature 5 in the encrypted SMS message 9 with the electronic signature 20 generated by the encryption means 16, said signature 20 being generated on the basis of data entered on the keyboard in the terminal 12. If the electronic signature 5 and the electronic signature 20 entered by the user match, the comparison means 17 transmits a signal to the guide means 18 that the PIN code 19 is to be displayed on the display 14 of the mobile handset 12, whereby the PIN code is delivered to the user.

In a preferred embodiment of the invention the terminal 12 is a mobile handset such as a cellular telephone. A SIM card (Subscriber Identity Module) is required for operating mobile handsets adapted for communication via an existing GSM network. The SIM card, which in use forms an integrated part of the electronics of the mobile handset, contains *inter alia* codes identifying the mobile handset in relation to the GSM network. This identification is necessary to enable the network to determine for instance the position of the mobile terminal for transmission of mobile telephony via the most advantageous transmission tower(s) in the network at the specific time.

The server 3 comprises software (not shown) for generating PIN codes, a triple DES

(Data Encryption Standard) encryption algorithm (reference numeral 4), an encrypted database (not shown) containing encryption keys to all of the SIM cards registered in the system and information about the connection between the numbers of the mobile handsets and the numbers of the associated SIM cards. A triple DES
5 algorithm is an encryption process in three levels which is considered particularly secure against unauthorised decryption.

When the secured server 3 has received the reference code from a new user and verified that the user's SIM card number is valid in the system, the server 3 generates an electronic signature 5 preferably by means of the triple DES algorithm 4
10 combined with the two keys of at least 56 bit belonging to the user's SIM card number. The electronic signature 5 is transmitted to the user's SIM card 10 as an uniquely formatted GSM 8 bit SMS (Short Message System) message. The coding of the SMS messages is adapted such that the electronic signature 5 of the reference code 2 is stored in the storage 11 of the SIM card 10 and the user is notified that the
15 generated PIN code is ready for use when a SMS message 9 is received by the user's SIM card 10.

When the user subsequently runs the program in the SIM card 10 enabling delivery of the PIN code, the user is requested by the program via the display 14 of the terminal to enter the reference code 15 on the keyboard 13 of the terminal 12. For
20 generating another electronic signature 20, the reference code 15 is coded by the encryption means 16 in the SIM card 10 by means of the same encryption algorithm used by the encryption means 4 in the secured server 3 when the reference code 2 was supplied to the secured server 3. The comparison means 17 in the SIM card 10 then compares the electronic signature 5 stored in the storage 11 and based on the
25 reference code 2 with the electronic signature 20 generated by the encryption means 16. If the two signatures match, the comparison means 17 transmits a signal to the guide means 18 indicating that the PIN code 19 is to be displayed on the display 14 of the terminal 12. If the two electronic signatures are not identical, the user is

advised on the display 14 that the reference code 15 has not been accepted and is asked to enter the reference code 15 once more. If the reference code 15 after two additional attempts still is incorrect, the program is interrupted and the PIN code 19 is not delivered until the user has fetched a new reference code 2 from the secured
5 server 3, said code being either identical to or different from the initial reference code 2.

In order to ensure that the delivered PIN code is read correctly, the user may be offered validation of the delivered PIN code. The validation process is performed by the user entering the PIN code shown on the display 14 by means of the keyboard,
10 whereafter the user is advised whether the PIN code has been entered correctly. If not, the PIN code is shown once more on the display 14 and the validation process can be repeated.

In an alternative embodiment the PIN code may be provided in the SIM card, when the card is supplied with a unique identity code, whereby the PIN code never need
15 be transmitted. This is considered a more secure embodiment, unauthorised decryption of the PIN code during transmission thereof thus being prevented.

The invention is not restricted to the above preferred embodiment, but may be altered in many ways without thereby deviating from the scope of the invention.

Claims

1. A system for electronic delivery of electronic information and comprising a server (3) secured by means of a number of encryption keys, said system comprising encryption means (4) for encrypting the electronic information and via connected communications means (6, 8) being adapted to transmit a SMS message (9) containing the encrypted electronic information to a SIM card (10) connected to a terminal (12) with input means (13) and display means (14), said SIM card comprising means (11) for receiving and storing the encrypted SMS message (9), characterised in that
- said server (3) is adapted for receiving unique information in the form of a reference code (2), said encryption means (4) is adapted for computing a first electronic signature (5) based on the reference code (2), and the server being adapted for transmitting the first electronic signature (5) as encrypted electronic information in said SMS message (9), and
- said SIM card (10) comprises means (17) for comparing the first electronic signature (5) in the SMS message (9) with a second electronic signature (20) being generated from a reference code (15) entered by a user of the terminal (12) and by means of a corresponding encryption key (16) in the SIM card (10), and means (18) for allowing subsequent display of a PIN code associated with the signatures (5, 20) on the display means (14) of the terminal (12), if the first electronic signature (5) and the second electronic signature (20) match.
2. A system according to claim 1, wherein said SIM card (10) is adapted for being provided with the PIN code when supplying the SIM card (10) with a unique identity code.
3. A system according to claim 1, wherein said SIM card (10) is adapted to receive the PIN code in the form of an encrypted data signal.

4. A mobile phone comprising a terminal (12) with input means (13) and display means (14), and a SIM card (10) including means (11) adapted for receiving and storing an encrypted SMS message (9), characterised in that the SIM card (10) comprises comparator means (17) adapted for comparing a first electronic signature (5) in the
5 encrypted SMS message (9) with a second electronic signature (20) being generated from a reference code (15) entered by a user of the terminal (12) and by means of a corresponding encryption key (16) in the SIM card (10), and

means (18) for allowing subsequent display of a PIN code associated with the signatures (5, 20) on the display means (14) of the terminal (12), if the first electronic
10 signature (5) and the second electronic signature (2) match.

5. A mobile phone according to claim 4, wherein said SIM card (10) is adapted for being provided with the PIN code when supplying the SIM card (10) with a unique identity code.

6. A mobile phone according to claim 4, wherein said SIM card (10) is adapted to
15 receive the PIN code in the form of an encrypted data signal.

7. A SIM card including storage means (11) adapted for receiving and storing an encrypted SMS message (9), characterised in that said SIM card (10) comprises

encryption means (16) adapted for generating a second electronic signature (2) from
20 a reference code (15) entered by a user of the terminal (12) and by means of a corresponding encryption key (16) in the SIM card (10), and

comparator means (17) adapted for comparing a first electronic signature (5) in the encrypted SMS message (9) with said second electronic signature (20) and transmitting

a signal to a control means (18) indicating that a PIN code (19) is to be delivered to a user.

8. A SIM card according to claim 7, wherein said SIM card (10) is adapted for being provided with the PIN code when supplying the SIM card (10) with a unique identity
5 code.

9. A SIM card according to claim 8, wherein said SIM card (10) is adapted to receive the PIN code in the form of an encrypted data signal.