Fig. 3a

Fig. 3b

Title: A SMART CARD

Abstract: A smart card on which the card information that is required for making a purchase is non-visible on the card, and retrievable on a display (7) only after reception of a valid authenticating information, e.g. a PIN code, inputted by the card holder on input means (8), e.g. a key set. The card information comprises at least a card number and a card verification code, and the authenticating information is checked by suitable verification means (9) integrated in the smart card.
A Smart card

TECHNICAL FIELD

The present invention relates to a method for enabling a card holder of a smart card to retrieve card information, and to a smart card enabling a card holder to retrieve card information.

BACKGROUND

A conventional credit card is a smart card that can be used both for direct payments in a store or in a restaurant, and for payments on the Internet. The smart card is provided with the name of the card holder, as well as several security features that are required for performing a payment transaction, such as e.g. the card number, the CVC (Card Verification Code) number, and the expiration date of the card. This card information is normally indicated both visibly, as printed or embossed numbers and letters on the card surface, as well as non-visibly, such as stored on a magnetic strip and in an encrypted chip on the smart card.

Printed or embossed numbers and letters are an unsecure storage of card information, since they are visually readable by anyone. A magnetic strip and a chip is a more secure storage of card information, since the card information is only retrievable by a magnetic reader or a chip reader. However, by having both visible card information, as printed or embossed letters and number, as well as non-visible, as a magnetic strip and a chip, different types of card readers can be used, such as a carbon paper slip, a magnetic reader and a chip reader. Further, when a transaction is carried out by telephone or on the Internet, the card holder is able to read the visible card information and enter it in the phone or in the computer. Similarly, when a magnetic reader or a chip reader is unavailable or out of
function, a sales person is able to carry out a transaction by reading the visible card information, and enter it manually. However, an important drawback with conventional credit cards is that the visual card information could easily be copied, especially when the card is out of sight from the card holder, e.g. used by a waiter in restaurant. By copying or photographing the card, all the card information that is required for performing a payment transaction can be obtained, and an unscrupulous person could use the card information without the card for unauthorized purchases, e.g. on the Internet.

Figure 1a shows the front side of a typical smart card, with the chip 1 storing the encrypted card information, the visible printed or embossed card number 4 or card account number, the visible printed or embossed expiration date 5, and the visible printed or embossed name 6 of the card holder. It should be noted that additional information can be printed or embossed on the card. Furthermore, the information stored in the chip 1 can also store additional information. Figure 1b shows the back side of the same card, with a magnetic strip 2 storing the card information, and the printed and visible CVC (card verification code) number 3. The CVC number is a security code. The CVC code is also known as the Card Security Code (CSC), sometimes called Card Verification Value (CVV or CV2), Card Verification Value Code (CVVC), Verification Code (V-Code or V Code) or Card Code Verification.

As described above, the smart card illustrated in the figures 1a and 1b is provided with visible card information, i.e. printed or embossed letters and numbers, as well as card information stored non-visibly both in a magnetic strip and encrypted in a chip, but a conventional smart card could also be provided with either a magnetic strip or a chip, together with the visible printed or embossed letters and numbers.
Figure 2a and 2b illustrates another known smart card, which provides a higher security than the smart card illustrated in figure 1, and provided with an embedded display 7 for retrieval of the previously described security code number (i.e. CVC, or CVV or CV2 or CVVC) using a PIN code (Personal Identification Number) inputted on a keyboard 8. The front side of the smart card, illustrated in figure 2a, is provided with a chip 1 for storing the card information in encrypted form, the printed or embossed card number 3, the expiration date 4, and the name of the card holder 5. The back side of the smart card is illustrated in figure 2b, and it is provided with a magnetic strip 2 for storing the card information. However, this smart card is not provided with any printed and visible CVC number, since the CVC number is retrievable only on the display using a PIN code.

Another known type of smart card displays information in response to biometrical input means, which comprises a sensor element capable of identifying the fingerprint of the card holder.

However, it still presents a problem to achieve a high security smart card, from which the card information that is required for performing a payment could not be copied by an unauthorized person, but is still available to the card holder.

SUMMARY

The object of the present invention is to address the problem outlined above, and this object and others are achieved by the method and the smart card according to the appended independent claims, and by the embodiments according to the dependent claims.
According to one aspect, the invention provides a method for enabling a card holder of a smart card to retrieve card information. Said smart card comprises a display for displaying information, and further comprises input means, and the method comprises the following steps:
- receiving, by means of said input means, authentication information inputted by the card holder;
- verifying if the authentication information is valid;
- displaying card information necessary for making a purchase, only when the authentication information is valid; said card information comprising at least a card number and a card verification code.

According to a second aspect, the invention provides a smart card enabling a card holder to retrieve card information. The smart card comprises:
- input means configured to receive authentication information from the card holder;
- verification means configured to verify that the authentication information is valid;
- a display configured to display card information necessary for making a purchase only when the authentication information is valid; said card information comprising at least a card number and a card verification code.

An advantage with the present invention is that the card information that is required for performing a purchase can not be copied and used by an unauthorized person, since it is not printed or embossed on the surface of the smart card, but the card information is still available to the card holder on the display, after input of valid authenticating information, e.g. a PIN code.
BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will now be described in more detail, and with reference to the accompanying drawings, in which:

- Figure 1a and 1b illustrate the front side and the back side, respectively, of a conventional smart card;
- Figure 2a and 2b illustrate the front side and the back side, respectively, of a conventional smart card provided with a display;
- Figure 3a and 3b illustrate the front side and the back side, respectively, of a smart card according to an embodiment of the invention;
- Figure 4 is a flow diagram illustrating a method for retrieving card information, according to an embodiment of the invention.

DETAILED DESCRIPTION

In the following description, specific details are set forth, such as a particular architecture and sequences of steps in order to provide a thorough understanding of the present invention. However, it is apparent to a person skilled in the art that the present invention may be practised in other embodiments that may depart from these specific details.

Moreover, it is apparent that the described functions may be implemented using software functioning in conjunction with a programmed microprocessor, and/or using an application-specific integrated circuit. Where the invention is described in the form of a method, the invention may also be embodied in a computer program product, as well as in a system comprising a computer processor and a memory, wherein the memory in encoded with one or more programs that may perform the described functions.
The basic concept of the invention is to provide a smart card on which the card information that is required for a payment transaction is retrievable by the card holder on an embedded display in the smart card only after input of valid authentication information, e.g. a PIN code. The smart card, in accordance with the invention, thus provides a much higher security for the card holder since all the information necessary to perform a purchase is only retrievable by the card holder after that a validity check has been performed.

Referring to figure 3, there is illustrated a smart card according to an exemplary embodiment of the invention. One side of the smart card, illustrated on figure 3a, is provided with e.g. the name 6 of the card holder, printed or embossed on the card surface. Note that additional information such as the name of the card provider can also be printed or embossed on the card surface. Further, the smart card is provided with the card information that is required for performing a payment stored encrypted in a chip 1, and/or on a magnetic strip 2 located on the other side of the smart card, as illustrated in figure 3b. Thus, the card information that is required to perform a payment is only provided non-visibly on the smart card, i.e. on the magnetic strip and/or in the chip, in order to achieve a high security and prevent copying and unauthorized use of the card information for purchases, e.g. on the Internet. However, in order to enable the card holder to obtain the card information, said information is retrievable on a display 7 embedded in the smart card.

Additionally, the smart card illustrated in figure 3a is provided with input means 8, i.e. two key buttons, for receiving authentication information, such as e.g. a PIN code, inputted by an authorized user, normally the card holder. The smart card is further provided with verification means 9, comprising suitable processing means that is capable of determining if the inputted
authentication information is correct, e.g. by comparing it with a pre-stored authentication information. If the verification means 9 verifies that the inputted authentication information is valid, then the required card information, comprising at least a card number (e.g. card account number) and a card verification code (i.e. CVC number, or CVV number or CV2 number or CVVC number), is indicated on the display 7, and is thereby visible to the authorized user.

According to other exemplary embodiments of the invention, the smart card is provided with either a magnetic strip or a chip, instead of both. Further, the name of the card holder could be omitted, and/or the expiration date of the card could be printed or embossed on the card. In case the expiration date is not printed or embossed on the smart card, then the expiration date is preferably also retrievable on the display.

Thus, a smart card according to the invention is not provided with the card information that is required for performing a purchase printed or embossed in the card surface. Instead, this card information is only provided non-visibly on the smart card, on a magnetic strip 2 and/or in a chip 1, and is retrievable on a display 7 only after input of authenticating information on suitable input means 8.

The key buttons of the input means 8 according to the above-described exemplary embodiment are preferably arranged such that one of the key buttons is able to select a position of a digit, and the other key button is able to select the digit of a selected position. More specifically, according to an exemplary embodiment of the input means 8, a new digit position is selected by a consecutive pressing of a first key button, and the digit of a selected position is increased with one for each consecutive pressing of the second key button, the display of
the digits controlled e.g. by a suitable timer or counter comprised in the input means.

According to other exemplary embodiments, the input means comprises any suitable type of key set, such as e.g. a key board comprising at least the digits 1-9, a biometric sensor, or a radio frequency receiver capable of remote reception of authentication information.

The biometric sensor comprises a sensor element that is capable of identifying the fingerprint of the card holder when he/her presses a fingertip against the sensor.

Input means comprising a radio frequency receiver is combined with suitable remote input means that are available to the card holder and comprising a corresponding radio frequency transmitter.

Figure 4 is a flow diagram illustrating a method for enabling a card holder of a smart card to retrieve card information required for performing a payment, according to an exemplary embodiment of the invention. In step 41, the card receives authenticating information, e.g. a PIN code, inputted e.g. by a card holder using input means 8, e.g. a key set. In step 42, verification means 9 determines whether the received authenticating information is valid or not, e.g. by comparing the inputted authenticating information with correct information pre-stored in a memory of the verification means. If the authenticating information is valid, then the card information required for performing a payment is displayed on the display 7, in step 43, the card information comprising at least the card number and the CVC number.
According to other exemplary embodiments of the method, the inputted authenticating information, such as a PIN code, is also displayed on the display.

According to further exemplary embodiments, the authenticating information is received biometrically using a biometric sensor of the smart card, the biometric sensor capable of recognizing the fingerprint or a card holder. Alternatively, the authenticating information is received by a radio frequency receiver of the smart card.

Additionally, according to another exemplary embodiment, the displayed card information further comprises the expiry date of the card. However, if the expiry date of the card is not comprised in the displayed card information, the expiry date will be indicated visible on the smart card, printed or embossed in the card surface.

While the invention has been described with reference to specific exemplary embodiments, the description is in general only intended to illustrate the inventive concept and should not be taken as limiting the scope of the invention.
CLAIMS

1. A method for enabling a card holder of a smart card to retrieve card information, said smart card comprises a display (7) for displaying information and further comprising input means (8), the method comprising:
- receiving (41) by means of said input means (8), authentication information inputted by the card holder;
- verifying (42) if the authentication information is valid;
- displaying (43) card information necessary for making a purchase, only when the authentication information is valid; said card information comprising at least a card number and a card verification code.

2. The method according to claim 1 wherein receiving (41) comprises receiving authentication information corresponding to a personal identification number, PIN, inputted by the card holder and displayed on said display (7).

3. The method according to claim 1 wherein receiving (41) comprises receiving authentication information biometrically using a sensor integrated in the smart card.

4. The method according to claim 1 wherein receiving (41) comprises remotely receiving authentication information by means of a radio frequency receiver of the smart card.

5. The method according to claim 1 wherein receiving comprises receiving authentication information by means of a key set provided on the smart card on which the card holder enters authentication information.

6. The method according to anyone of claims 1-5 wherein verifying comprises verifying that the authentication
information corresponds to a pre-stored authentication information.

7. The method according to anyone of claims 1-6 wherein displaying further comprises displaying an expiration date of the smart card.

8. A smart card enabling a card holder to retrieve card information, the smart card comprising:
- input means (8) configured to receive authentication information from the card holder;
- verification means (9) configured to verify that the authentication information is valid;
- a display (7) configured to display card information necessary for making a purchase only when the authentication information is valid; said card information comprising at least a card number and a card verification code.

9. The smart card according to claim 8 wherein the input means (8) comprises a first key button and a second key button; the first key button, when operated by the card holder, indicating a position of a digit on the display, and the second key button, when operated, displaying the digit on said position on the display.

10. The smart card according to claim 9 wherein each consecutive pressing of the first key button corresponds to a new position of a digit on the display; and each consecutive pressing of the second button corresponds to an increase of the digit which is displayed.

11. The smart card according to 8 or claim 9 wherein the authentication information corresponds to a personal identification number, PIN.
12. The smart card according to claim 8 wherein said input means (8) comprises at least one biometric sensor configured to receive authentication information when the card holder presses the sensor.

5

13. The smart card according to claim 8 comprises wherein the input means (8) comprises a radio frequency receiver configured to remotely receive authentication information.

10 14. The smart card according to claim 8 wherein the input means comprises a key set (8) on which the card holder can enter authentication information.
PRIOR ART:

Fig. 1a

Fig. 1b
Receiving authenticating information

Authenticating information valid?

No

Yes

Displaying at least card number and CVC number

Stop

Fig. 4
INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2009/050570

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet

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)

IPC: G06K, G07F, G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE, DK, FI, NO classes as above

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-INTERNAL, WPI DATA, PAJNSPECCMPDX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 20070073619 A1 (SMITH), 29 March 2007 (29.03.2007), paragraphs [0004], [0008], [0018-0019], [0029-0033], [0037], [0044], fig. 1</td>
<td>1-14</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>US 6163771 A (WALKER ET AL), 19 December 2000 (19.12.2000), column 5, line 46 - column 6, line 59, figure 1, claims 1,14</td>
<td>1-14</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>US 20060218097 A1 (WALKER ET AL), 28 Sept 2006 (28.09.2006), figure 1, claim 14, abstract</td>
<td>1-14</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>WO 2007146159 A2 (RIVERA), 21 December 2007 (21.12.2007), figure 7, claims 1-5,18-34</td>
<td>1-14</td>
</tr>
</tbody>
</table>

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 application or patent 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
  *T* document published prior to the international filing date but later than the priority date claimed

Date of the actual completion of the international search

25 June 2009

Date of mailing of the international search report

17-07-2009

Name and mailing address of the ISA/
Swedish Patent Office
Box 5055, S-102 42 STOCKHOLM
Facsimile No. +46 8 666 02 86

Authorized officer
Frida Holmberg / ITW
Telephone No. +46 8 782 25 00

Form PCT/IS A/210 (second sheet) (July 2008)
<table>
<thead>
<tr>
<th>Category*</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>WO 02088931 Al (MCGREGOR), 7 November 2002</td>
<td>1-14</td>
</tr>
<tr>
<td></td>
<td>(07.11.2002), page 5, line 25 - page 7, line 6; page 10, line 31 - page 11, line 30, figures 2,8, claims 25-35</td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>US 20080067247 Al (MCGREGOR ET AL), 20 March 2008</td>
<td>1-14</td>
</tr>
<tr>
<td></td>
<td>(20.03.2008), paragraphs [0015], [0030-0031], fig.1-2, claims 1,abstract</td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>US 20040050930 Al (ROWE), 18 March 2004</td>
<td>1-14</td>
</tr>
<tr>
<td></td>
<td>(18.03.2004), paragraphs[0008], [0025-0030], fig.1, abstract</td>
<td></td>
</tr>
<tr>
<td>P,X</td>
<td>US 20080223937 Al (PRETA ET AL), 18 Sept 2008</td>
<td>1-14</td>
</tr>
<tr>
<td></td>
<td>(18.09.2008), figure 2, claim 1, abstract</td>
<td></td>
</tr>
</tbody>
</table>
INTERNATIONAL SEARCH REPORT

International patent classification (IPC)
G06K 19/073 (2006.01)

Download your patent documents at www.prv.se
The cited patent documents can be downloaded:
• From "Cited documents" found under our online services at www.prv.se (English version)
• From "Anförda dokument" found under "e-tjanster" at www.prv.se (Swedish version)

Use the application number as username. The password is IRRMVGXPAA.

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.
<table>
<thead>
<tr>
<th>Country</th>
<th>Application Number</th>
<th>Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td>20070073619</td>
<td>29/03/2007</td>
<td>NONE</td>
</tr>
<tr>
<td>US</td>
<td>20060218097 A</td>
<td>28/09/2006</td>
<td>NONE</td>
</tr>
<tr>
<td>WO</td>
<td>02088931 A</td>
<td>07/11/2002</td>
<td>NONE</td>
</tr>
<tr>
<td>US</td>
<td>20080067247 A</td>
<td>20/03/2008</td>
<td>NONE</td>
</tr>
<tr>
<td>US</td>
<td>20040050930 A</td>
<td>18/03/2004</td>
<td>NONE</td>
</tr>
<tr>
<td>US</td>
<td>20080223937 A</td>
<td>18/09/2008</td>
<td>NONE</td>
</tr>
</tbody>
</table>