(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 316 689 B1**

(12) # EUROPEAN PATENT SPECIFICATION

(45) Date of publication of patent specification: **06.07.94** (51) Int. Cl.5: **G07F 7/10**

(21) Application number: **88118450.1**

(22) Date of filing: **04.11.88**

(54) **Portable electronic apparatus.**

(30) Priority: **13.11.87 JP 288120/87**

(43) Date of publication of application:
24.05.89 Bulletin 89/21

(45) Publication of the grant of the patent:
06.07.94 Bulletin 94/27

(84) Designated Contracting States:
DE FR GB

(56) References cited:
EP-A- 0 174 016
EP-A- 0 216 375
WO-A-86/03040
DE-A- 3 222 288
FR-A- 2 600 444
US-A- 4 443 027

(73) Proprietor: **KABUSHIKI KAISHA TOSHIBA**
72, Horikawa-cho
Saiwai-ku
Kawasaki-shi Kanagawa-ken 210(JP)

(72) Inventor: **Tamada, Masuo c/o Patent Division**
Kabushiki Kaisha Toshiba
1-1 Shibaura 1-chome
Minato-ku Tokyo 105(JP)
Inventor: **Matsuoka, Hideo c/o Patent Division**
Kabushiki Kaisha Toshiba
1-1 Shibaura 1-chome
Minato-ku Tokyo 105(JP)
Inventor: **Tanaka, Tsutomu c/o Patent Division**
Kabushiki Kaisha Toshiba
1-1 Shibaura 1-chome
Minato-ku Tokyo 105(JP)

(74) Representative: **Henkel, Feiler, Hänzel & Partner**
Möhlstrasse 37
D-81675 München (DE)

EP 0 316 689 B1

Description

The present invention relates to an IC card used, for example, as a credit card, a cash card, and the like.

The conventional magnetic card, having a magnetic stripe for storing data, is in widespread use as a credit card or a cash card. Recently, however, an IC card incorporating a nonerasable nonvolatile memory controlled by a CPU built into an IC chip, has been receiving considerable attention as a replacement for the magnetic card, since the greatly increased memory capacity of the IC card over that of the magnetic card makes it possible for the IC card to be used in a much wider range of applications than is possible with a magnetic card. Recently, a multifunctional IC card has been developed which incorporates a battery therein, as well as a keyboard and a display section. This particular IC card, moreover, can be operated in an off-line manner; i.e. without having to be connected to a terminal device or the like.

When this IC card is used as a credit card or a cash card, a transaction valid date, representing a period for which transactions can be made, and a transaction limit amount, representing a maximum amount with which transactions can be made, are set and checked prior to the transactions. These transaction valid date data and transaction limit amount data are stored in a memory of the IC card, and can be externally updated, if desired.

In the conventional case, when the transaction valid date data and the transaction limit amount data are updated, there is no means by which the validity of externally input data can be authenticated. Therefore, the possibility exists that internally stored data may be updated, illegally, for fraudulent purposes. The transaction valid date data and the transaction limit amount data are particularly important data, and these data must not be illegally updated.

Note that the related art for generating a sales approval number on the basis of an input PIN and total amount is disclosed in USP No. 4,697,072 (Inventor: Shigeyuki Kawana, Title: "IDENTIFICATION CARD AND AUTHENTICATION SYSTEM THEREFOR").

Prior art document WO-A-86/03040 discloses a portable electronic apparatus comprising data storing means for storing transaction data, input means for inputting the transaction data to be stored in said data storing means, and control means for controlling said transaction data storing means and said input means. This known apparatus further comprises means for generating additional data in the form of a transaction key number differing from one another for every generation. This additional data is used together with the transaction data input from said input means to generate a transaction identification code which can be checked in a manner similar to a parity check to determine the validity of the transaction identification code, e.g. by entering it in an automatic teller machine.

Further, prior art document DE-A-32 22 288 discloses an identity card comprising a microprocessor, input means and display means. The microprocessor is connected to timer means. The data supplied to the display means can also be applied to external terminal means, and it is possible to supply data to the microprocessor through the external terminal means.

It is an object of the present invention to provide a portable electronic apparatus which is capable of authenticating the validity of externally input data and, in particular, an apparatus which can prevent illegal updating of important data, and the like.

To solve this object the present invention provides a portable electronic apparatus as specified in claim 1.

According to the portable electronic apparatus of the present invention, the validity of all externally input transaction data can be authenticated, with update processing being executed, only when the result of authentication is affirmative. In this way, important data stored in the memory is protected against illegal updating.

Other objects and features of the present invention will be apparent from the following description taken in connection with the accompanied drawings, of which:

Fig. 1 is a view showing the outer appearance of a portable electronic apparatus according to an embodiment of the present invention;

Fig. 2 is a block diagram showing a detailed arrangement of an integrated circuit shown in Fig. 1; and

Fig. 3 is a flow chart for explaining update processing of the transaction limit amount and the transaction valid date in regard to the embodiment shown in Figs. 1 and 2.

Fig. 1 shows the outer appearance of a multifunctional IC card used, for instance, as a credit card, and being an example of a portable electronic apparatus according to the present invention. This IC card is designed such that it can be used both in on-line and off-line modes. For example, the IC card has a transaction function by means of which it can perform transactions in relation to a plurality of accounts (available as, e.g., a plurality of types of credit card and cash card), a time-piece function for displaying time-related data including the date and the time, a calculation function capable of executing at least four operations; and an electronic notebook function for storing and reading out addresses, names, phone numbers, and the like.

Fig. 1 shows card main body 1 which can be constituted by, for example, a thin plastic board of rectangular shape. Card main body 1 includes contact section 3, which is electrically connected to integrated circuit (IC) 2 buried in main body 1, for electrically communicating with a terminal device (not shown) in the on-line mode, liquid crystal display section 4 for displaying input/output data, time-related data, and the like, and keyboard 5, all of these units being arranged at predetermined positions on the front surface of main body 1. Card main body 1 additionally contains battery 6 for supplying a power source voltage.

Keyboard 5 includes account keys 7, 8, 9, and 10 for designating an account; numeric keys 11; addition key 12, subtraction key 13, division key 14, and multiplication key 15, these being the four-operation keys; decimal key 16; equal key 17; and the like.

Account key 7 designates a first operation (processing) for a first account (e.g., account data of a first credit company), account key 8 designates a second operation for a second account (e.g., account data of a second credit company), account key 9 designates a third operation for a third account (e.g., account data of a first bank), and account key 10 designates a fourth operation for a fourth account (e.g., account data for a second bank).

Addition key 12 is used as a "next" key for advancing the display state of liquid crystal display section 4, and for mode-selection; subtraction key 13 is used as a "back" key for restoring display section 4 to its previous display state; and equal key 17 serves a dual purpose, being the used as "yes" key and also as the initialization key (power-on key).

Embossed data (not shown) is formed at a predetermined position of the rear surface of card main body 1 as card holder data.

Fig. 2 shows a circuit arrangement of the integrated circuit shown in Fig. 1. Communication control circuit 21, reset control circuit 22, and power source control circuit 23 are connected to contact section 3. In addition, battery check circuit 24 for checking whether the voltage of battery 6 is more than a predetermined value or not is connected to power source control circuit 23. Internal bus 38 is connected to program memory 28 for storing a control program, working memory 29 used for arithmetic operations, data memory 30 consisting of a nonvolatile memory such as an EEPROM for storing transaction data, timer circuit 31 used when time is counted during program execution, and timer circuit section 32 for generating time-piece data including time data and date data. This timer circuit section 32 includes timer circuits 322 and 323, and frequency divider 311. Oscillator 33 having a frequency of 32.768 kHz is connected to timer circuit section 32.

Display section 4 is connected to internal bus 38 through display control circuit 34 and display driver 35. Keyboard 5 is also connected to internal bus 38 through keyboard interface 36. In addition, confirmation data generating circuit 37 for generating the confirmation data of the input transaction data using key data based on DES (Data Encryption Standard) and CPU (Central Processing Unit) 27 for controlling the entire circuit shown in Fig. 2 are connected to internal bus 38.

Communication control circuit 21 is operated in the on-line mode. More specifically, serial data supplied from the terminal equipment (not shown) through contact section 3 is converted into parallel data and output to data bus 38. Otherwise, parallel data supplied from data bus 38 is converted into serial data and output to the terminal equipment through contact section 3.

Reset control circuit 22 is operated in the on-line mode. This circuit 22 receives a reset signal supplied from the terminal equipment through contact section 3 to initialize CPU 27.

After the predetermined time is elapsed in the on-line mode, power source control circuit 23 is switched to be driven by an external power source (supplied from the terminal equipment through contact section 3) in place of battery 6. In the off-line mode, i.e., when the voltage of the external power source is decreased, power source circuit 23 is switched to be driven by battery 6 in place of the external power source. When key input is not performed (in a stand-by state) in the off-line mode, clock control circuit 25 stops the operation of oscillator 26 for generating a clock having a frequency of 1 MHz. In addition, the clock is not supplied to CPU 27, and the circuit is completely stopped. In this state, when initialization key 17 is turned on, oscillator 26 is operated. In addition, a time-piece clock of 32.768 kHz output from timer circuit section 32 is supplied to CPU 27. When the next key operation is performed after initialization key 17 is turned on, the clock of 1 MHz output from oscillator 26 is supplied to CPU 27. In the on-line mode, by supplying a reset signal from reset control circuit 22, the clock supplied from the terminal equipment through contact section 3 is input to CPU 27.

A transaction function program, a time-piece function program, a calculation function program, an electronic memorandum notebook function program, and the like are stored in program memory 28. CPU 27 selectively executes and processes these programs in program memory 28, so that the transaction function, the time-piece function, the calculation function, the electronic memorandum notebook function, and the like are selectively op-

erated.

Account data (including transaction valid date data, transaction limit amount data, PIN, the renewal number of the transaction valid date and transaction limit amount) corresponding to the first through fourth accounts as described above are stored in data memory 30. When one of the above account keys 7 through 10 is pushed, the corresponding account data is selected and the corresponding processing is executed in accordance with the account data. In an electronic memorandum notebook area in data memory 30, addresses, names, and phone numbers are stored.

Timer circuit section 32 comprises frequency divider 321 which frequency-divides a clock of 32.768 kHz output from oscillator 33, and generates a one-second clock, and first and second timer circuits which generate time-piece data consisting of year-month-date data and time data by counting the clock generated from frequency divider 321. First timer circuit 322 is a display timer circuit which can freely set and change the time-piece data in accordance with the operation of keyboard 5 by a card holder. Second timer circuit 323 is, e.g., a timer circuit in which time-piece data is set when the card is issued and which cannot change setting of the time-piece data unless the validity of the operation is proved by the predetermined procedures.

Display control circuit 34 converts display data supplied from CPU 27 into a character pattern using a character generator (not shown) comprising an internal ROM, and displays the converted character pattern on liquid crystal display section 4 through display driver 35.

Confirmation data generating circuit 37 generates reference confirmation data for confirming the validity of input data. For example, as shown in Fig. 3, confirmation data generating circuit 37 generates confirmation data encrypted using the predetermined key data on the basis of the input data such as an account type, a supplementary amount of the transaction limit amount, and the transaction valid date (year, month, and day), and encryption generating data (inherent data) within the card such as a renewal number of the transaction limit amount and the transaction valid date stored in data memory 30.

With this arrangement, the case where an IC card holder purchases a desired item using this IC card, e.g., in the off-line mode will be described hereinafter. At first, the card holder presents the IC card to a store clerk of a retail store. The store clerk receives the IC card, and imprints embossed data on the IC card in an emboss imprint section of a transaction slip by an emboss imprinter. Then, the store clerk returns the IC card to the card holder, and writes transaction data such as a transaction amount and transaction date in the corresponding space of the transaction slip.

The card holder selects an account type by account keys 7 through 10 of keyboard 5. CPU 27 reads out account data corresponding to the selected account type from data memory 30. CPU 27 displays the account type on liquid crystal display section 4, and also displays a message for urging the card holder to input a PIN. Then, the card holder inputs the PIN by ten keys 11 of keyboard 5. Therefore, CPU 27 compares and verifies the input PIN with the PIN in the account data which is read out from data memory 30, and the validity of the card holder is judged. As the result of the judgement, if the card holder is invalid, the message representing this fact is displayed on liquid crystal display section 4, and the transaction is ended. However, if the card holder is valid, CPU 27 displays the message "Shopping?". When the card holder pushes "yes" key 17 of keyboard 5, CPU 27 sets a "shopping" mode. In addition, CPU 27 compares and verifies transaction valid date data in the account data read out from data memory 30 with date data generated from second timer circuit 323 to judge the valid date. As a result of the judgement, if the transaction date is not within the valid period of the IC card, the message representing that the valid date is exceeded is displayed on liquid crystal display section 4, and this transaction is ended. As a result of the judgement, if the transaction data is within the valid period, CPU 27 displays the message for urging the card holder to input the transaction amount.

When the card holder, therefore, inputs the transaction amount by ten keys 11 of keyboard 5, CPU 27 compares and verifies the input transaction amount with the transaction limit amount data in the account data read out from data memory 30 and judges whether the transaction is possible or impossible. As a result of the judgement, if the transaction is impossible, the message representing that the transaction is impossible is displayed on liquid crystal display section, and this transaction is ended. On the contrary, if the transaction is possible, CPU 27 substracts the input transaction amount from the transaction limit amount data in the account data read out from data memory 30, and updates the transaction limit amount data in data memory 30 using the subtracted result as new transaction limit amount data.

Then, the card holder presents the IC card to the store clerk. The store clerk receives the IC card, writes the displayed account type into the corresponding space of the transaction slip, and passes the transaction slip to the card holder. The card holder writes his or her name into the space for a signature of the transaction slip, and returns the transaction slip to the store clerk. Then, the

shopping procedures are completed.

Update processing of the transaction limit amount and the transaction valid date of the designated account type as an example of the validity of the input data will be described below with reference to Fig. 3.

The card holder selects the account type by account keys 7 through 10 of keyboard 5. Then, CPU 27 reads out the account data corresponding to the selected account type from data memory 30, displays the account data on liquid crystal display section 4, and displays the message for urging the card holder to input the PIN. When the card holder inputs the PIN by numeric keys 11 of keyboard 5, CPU 27 compares and verifies the input PIN with the PIN in the account data read out from data memory 30 and judges the validity of the card holder. As a result of the judgement, if the card holder is invalid, the message representing the invalidity of the card holder is displayed on liquid crystal display section 4, and the operation is ended. As the result of the above judgement, if the card holder is valid, CPU 27 displays the message "Shopping?" on liquid crystal display section 4. At this time, the card holder repeatedly pushes "next" key 12 of keyboard 5 to select a mode. When the message "Update?" is displayed on liquid crystal display section 4, pushing of "next" key 12 is stopped. When the card holder pushes "yes" key 17 of keyboard 5, CPU 27 sets the update mode, and displays the message for urging the card holder to input the amount on liquid crystal display section 4.

When the card holder, therefore, inputs the supplementary amount of the transaction limit amount to be updated by numeric keys 11 of keyboard 5, CPU 27 displays the message for urging the card holder to input the data on liquid crystal display section 4. The card holder inputs the confirmation data by keyboard 5. The confirmation data input from keyboard 5 is generated as follows. The card holder calls, e.g., a credit company and informs the account type, and the transaction amount and the transaction valid date which are to be updated to the company. As a result, the credit company encrypts a data string of the account type, the transaction amount and transaction valid date to be updated, and the renewal number with key data based on DES, using a host system and the same algorithm as confirmation data generating circuit 37. Then, the confirmation data is generated. The generated confirmation data is informed to the card holder by a phone call. The card holder inputs the confirmation data from keyboard 5.

When the input of the confirmation data is completed as described above, the card holder inputs the account type, and the transaction amount and transaction valid date (year, month, and day) which are to be updated as the transaction data to be updated. CPU 27 receives these input data and supplies a renewal number (sequence number) in the account data readout from data memory 30 to confirmation data generating circuit 37. Note that the renewal number is updated upon every updating of the transaction limit amount and transaction valid date. Confirmation data generating circuit 37 encrypts the data string of the supplied account type, transaction amount and transaction valid date which are to be updated, and renewal number (stored in the predetermined region of the data memory) using the key data in accordance with DES to generate reference confirmation data. CPU 27 compares the input confirmation data with the reference data. When these data coincide with each other, CPU 27 judges that input data and the input confirmation data are valid, and updates the transaction limit amount data and the transaction valid date data in the selected account data on the basis of the input data. On the other hand, when the above data do not coincide with each other, CPU 27 judges that at least one of the input data and the input personal data is invalid, and stops the update processing.

When the transaction limit amount and the transaction valid date are updated as described above, by inputting the data for updating (account type, supplementary amount, date) from the keyboard, the confirmation data encrypted using the predetermined key data is generated on the basis of the input data and the encryption generating data within the card such as a renewal number stored in the data memory. Then, the generated confirmation data is verified with the confirmation data which is input from the keyboard, and the validity of the above input data is judged. Therefore, the validity of the input data from the keyboard can be judged. When the result of the judgement is negative, the update processing is stopped. Only when the result of the judgement is affirmative, the update processing is executed and the illegal updating of the transaction limit amount data and transaction valid date data which are stored in data memory 30 can be prevented.

When the renewal number (sequence number) is used as the encryption generating data within the card, it can be controlled so that the encryption generating data which was once used cannot be used again. More specifically, the latest renewal number is input with the confirmation data at the next renewal. By comparing the input renewal number with the renewal number in the data memory, when the same or smaller renewal number is input, the update processing can be prohibited.

Note that, although the above-described embodiment is described with reference to the off-line

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.