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

(11) Publication number: **0 588 339 A2**

(12) # EUROPEAN PATENT APPLICATION

(21) Application number: **93114917.3**

(51) Int. Cl.[5]: **G07F 7/10**, G06F 15/30

(22) Date of filing: **16.09.93**

(30) Priority: **18.09.92 JP 249293/92**
18.09.92 JP 249294/92
18.11.92 JP 308688/92
26.11.92 JP 317254/92
26.11.92 JP 317255/92

(43) Date of publication of application:
23.03.94 Bulletin 94/12

(84) Designated Contracting States:
DE FR GB

(71) Applicant: **NIPPON TELEGRAPH AND TELEPHONE CORPORATION**
1-6 Uchisaiwai-cho 1-chome
Chiyoda-ku
Tokyo(JP)

(72) Inventor: **Ishiguro, Ginya**
Gurin Haitsu 12-2-403,
580, Nagasawa
Yokosuka-shi, Kanagawa(JP)
Inventor: **Muta, Toshiyasu**
1927, Nagasawa
Yokosuka-shi, Kanagawa(JP)
Inventor: **Sakita, Kazutaka**
2-14-1-613, Kaneya
Yokosuka-shi, Kanagawa(JP)
Inventor: **Miyaguchi, Shoji**
5-20-19, Bessho,
Ninami-ku
Yokohama-shi, Kanagawa(JP)
Inventor: **Okamoto, Tatsuaki**
94-2-5-503, Nagasawa
Yokosuka-shi, Kanagawa(JP)
Inventor: **Fujioka, Atsushi**
B-305, 9-2-12, Sugita,
Isogo-ku
Yokohama-shi, Kanagawa(JP)

(74) Representative: **Hoffmann, Eckart**
Patentanwalt,
Blumbach & Partner,
Bahnhofstrasse 103
D-82166 Gräfelfing (DE)

(54) **Method and apparatus for settlement of accounts by IC cards.**

(57) An IC card (6) has a card information memory area wherein there are written a master public key nA, card secret keys pU and qU, a card public key nU, a card identification number IDU, and a first master digital signature SA1 for information including the card identification number. An IC card terminal (2a,2b) has terminal information memory area wherein there are written a master public key nA, terminal secret keys pT and qT, a terminal public key nT, a terminal identification number IDT, and a second master digital signature SA2 for information including the terminal identification number IDT. When inserted into the IC card terminal, the IC card sends thereto the data nU, IDU, and SA1. The IC card terminal verifies the digital signature SA1 by the master public key nA and, if it is valid, transmits the data nT, IDT and SA2 to the IC card. The IC card verifies the digital signature SA2 by the master public key nA and, if it is valid, transmits information corresponding to the current remainder value V to the IC card terminal. The IC card terminal makes a check to see if the received information corresponding to the remainder value V is appropriate, and if so, becomes enabled for providing a service.

EP 0 588 339 A2

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

BACKGROUND OF THE INVENTION

The present invention relates to a method and apparatus for settlement of accounts by IC cards which are used as prepaid cards of credit cards.

For instance, in an IC card which is used as a prepaid card, there is written the amount of money paid for its purchase, and before or after receiving a service the card user inserts the IC card into an IC card terminal, wherein the remaining value after subtracting the charge for the service from the initial value is transmitted to and written into the IC card.

In a conventional system of this kind, the IC card and the IC card terminal use the same cipher system and have the same secret key and communicate to each other the balance information enciphered by the common secret key. IC card and IC card terminal are designed so that such a secret key cannot be found nor can it be altered even if IC card terminal should be revealed to an outsider.

On the other hand, in the case of an IC card for use as a credit card, its identification number and other necessary information are preregistered and the user is allowed to receive his desired service when inserting the IC card into an IC card terminal and is charged for the service afterward. In a conventional IC credit card system, upon insertion of the IC card into the IC card terminal, the latter is connected online to a management center where IC card identification numbers and other user information are registered, then the user inputs his registration number and other required information by dialing, the thus input information is sent to the management center, wherein the user information registered in advance is used to verify the validity of the user. After the user's validity is thus proved, the user is allowed to receive his or her desired service at the IC card terminal.

Such an IC credit card system similarly adopts, with a view to providing increased security, a method in which: the IC card and the IC card terminal use the same cryptographic scheme and have the same secret key and they each authenticate the other's validity; a password input into the IC terminal is checked with its counterpart prestored in the IC card; the IC card identification number read out of the IC card is sent from the IC card terminal to the management center which has a data base of identification numbers and other information of IC cards; the IC card identification number is verified in the management center; the result of the verification is transmitted to the IC card terminal; and when the IC card identification thus checked in the management center is valid, the service specified by the card user starts through the IC card terminal. In some cases, the IC card and the management center each authenticate the other's validity directly through use of the same secret key.

The conventional methods mentioned above all call for communication between the management center and the IC card terminal and online processing for verification before or after the service is provided, and hence they have shortcomings that the management center facility is inevitably large-scale and that the charge for the service includes communication expenses. Moreover, the history of service can be stored in the management center or IC card but difficulty is encountered in proving that the stored contents are not false. Although it is almost impossible to falsify the stored contents of the IC card unless the secret key is let out, the secret key information in the IC card or IC card terminal is not perfectly protected and may in some cases leak out in a long time. In the case where the cryptographic scheme used is broken by third parties and many IC terminals are used by them, particularly in the event that IC cards and IC terminals are abused by unauthorized persons over a wide range, it is very difficult to change all of the secret keys at the same time--this poses a serious social problem as well-intentioned users cannot use their IC cards for a long period of time, for instance.

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide a method and apparatus for the payment of charges by IC cards which eliminate the need for communication between the management center and the IC card terminal each time the card user inserts his IC card into the latter to receive his desired service and which permit detection of abuse of a forged IC card or intentionally altered IC card terminal.

In the method for the payment of charges by IC cards according to a first aspect of the present invention, the respective IC card has prestored in its memory means a master public key nA for verifying a master digital signature SA, a card identification number IDU for specifying the IC card and a first master digital signature SA1 for information containing at least the card identification number IDU, and the IC card terminal has prestored in its terminal memory the above-mentioned master public key nA, a terminal identification number IDT for specifying the IC card terminal and a second master digital signature SA2 for information including at least the above-mentioned terminal identification number IDT. This method includes:

a step wherein the IC card transmits at least the card identification number IDU and the first master digital signature SA1 to the IC card terminal;

a step wherein the IC card terminal vertifies the

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

validity of the first master digital signature SA1 through use of the master public key nA and the card identification number IDU received from the IC card;

a step wherein when the first master digital signature SA1 is valid, the IC card terminal transmits at least the terminal identification number IDT and the second master digital signature SA2 to the IC card;

a step wherein the IC card verifies the validity of the second master digital signature SA2 through use of the master public key nA and the terminal identification number IDT received from the IC card terminal; and

a step wherein when the second master digital signature SA2 is valid, the IC card terminal generating a value V corresponding to the charge for a service specified by the IC card after the service is provided.

In the method for the payment of charges by IC cards according to a second aspect of the present invention, the respective IC card has card information memory means wherein there are written, as card information, from a management center a card identification number IDU, a predetermined password setting number Ns, a second master digital signature SA2 for the password setting number Ns, a first master digital signature SA1 for information containing the card identification number IDU and the second master digital signature SA2 and an IC card terminal has terminal information memory means wherein there are written, as terminal information, from the management center a master public key nA for verifying the master digital signatures, terminal secret keys pT and qT for creating a terminal digital signature and a terminal public key nT for verifying the terminal digital signature. This method includes:

a step wherein the IC card transmits the card identification number IDU and the first and second master digital signatures SA1 and SA2 to the IC card terminal;

a step wherein the IC card terminal verifies the validity of the first master digital signature SA1 and, if it is valid, prompts the card user to input a password Nc' and transmits it to the IC card after it is input;

a step wherein the IC card matches the password Nc' received from the IC card terminal with the password Nc stored in the card information memory and, if they match, transmits an authentication signal to the IC card terminal; and

a step wherein upon receiving the authentication signal, the IC card terminal becomes enabled for providing a service, and after the service, the IC card terminal records information including a value V corresponding to the charge for the service rendered and the card identification number IDU received from the IC card, as usage/management information, in usage/management information memory means.

According to a third aspect of the present invention, the IC card includes:

card information memory means for recording a master public key nA for verifying a master digital signature SA created using master secret keys pA and qA, a card identification number IDU for specifying or identifying the IC card, card secret keys pU and qU for creating a digital signature, a card public key nU for verifying the digital signature, and a first master digital signature SA1 for information containing the card identification number IDU and the card public key nU, the first master digital signature SA1 being created using the master secret keys pA and qA;

means for transmitting the card identification number IDU, the card public key nU and the first master digital signature SA1 to the IC card terminal;

means which receives a terminal identification number IDT, a terminal public key nT and a second master digital signature SA2 from the IC card terminal, verifies the second master digital signal SA2 through use of the master public key nA recorded in the card information memory means and, if it is valid, transmits to the IC card terminal an authentication signal which enables it for providing a service; and

usage information memory means for recording usage information including the remaining value V' updated by subtracting using the charge for the service rendered.

According to a fourth aspect of the present invention, the IC card terminal includes:

memory means for recording a master public key nA for verifying a master digital signature SA created using master secret keys pA and qA, a terminal identification number IDT for identifying the IC card terminal, terminal secret keys pT and qT for creating a terminal digital signature, a terminal public key nT for verifying the terminal digital signature and a second master digital signature SA2 for information including the terminal identification number IDT and the terminal public key nT, the second master digital signature SA2 being created using the master secret keys pA and qA;

means for transmitting the terminal public key nT, the terminal identification number IDT and the second master digital signature SA2 to an IC card;

means which receives a card identification number IDU, a card public key nU and a first master digital signature SA1 from the IC card, verifies the first master digital signature through use of the master public key recorded in the memory means and, if it is valid, enables the IC card terminal for providing a service; and

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

means which updates remaining value through use of the charge for the service rendered and transmits to the IC card usage information including the updated remaining value.

A digital signature scheme capable of proving that a person who transmitted digital information acknowledged it, just like he puts his seal to a document, is already established as disclosed in, for example, "ESIGN: An Efficient Digital Signature Scheme," NTT R & D Vol. 40, No. 5, 1991, pp687-686, or U.S. Patent No. 4,625,076. According to the digital signature scheme, a document M and a secret key Q are used and a digital signature S(M) is created using a signature creating function, then the signature S(M) and the document M are transmitted to the other party. The other party performs a computation by substituting the received document M and signature S(M) and a public key U into a signature verifying function. If the computed result satisfies predetermined conditions, then it is verified that the digital signature S(M) was attached to the document M by a person having the secret key Q, and he cannot deny the fact. In this instance, the Q and U are different prime numbers of extremely large values (that is, $Q \neq U$), and this scheme features a mathematical property that the value Q cannot be computed even if the value of U is known. Furthermore, even if slightly altered, the document can be proved invalid. It is set forth in the above-noted literature that these digital signature functions could be executed within a practical processing time on the scale of a program mountable on IC cards, through utilization of an algorithm called ESIGN.

Other digital signature schemes applicable to the present invention are an ElGamal scheme (T. E. ElGamal: A public key cryptosystem and a signature scheme based on discrete algorithm, Proc. of Crypto'84, 1984), a DSA (Digital Signature Algorithm, made public by the National Institute of Standards and Technology of the U.S. Department of Commerce) scheme, and a Micali-Shamir scheme (S. Micali and A. Shamir: An improvement of the Fiat-Shamir identification and signature scheme, Proc. of Crypto '88, pp244-247, 1988), for instance.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram illustrating the system configuration of an embodiment of the present invention;

Fig. 2 is a block diagram showing an example of the configuration of an IC card terminal;

Fig. 3 is a block diagram showing an example of the configuration of an IC card;

Fig. 4A is a diagram showing processing of a management center for setting the IC card terminal;

Fig. 4B is a diagram showing processing of an IC card dispenser when dispensing the IC card;

Fig. 4C is a diagram showing procedures between the IC card and the IC card dispenser for dispensing and recharging the latter;

Fig. 5 is a diagram showing procedures between the IC card and the IC card terminal;

Fig. 5A is a functional block diagram of the IC card in the embodiment of Fig. 5;

Fig. 5B is a functional block diagram of the IC card terminal in the embodiment of Fig. 5;

Fig. 6 is a diagram showing another example of the procedure between the IC card and the IC card terminal;

Fig. 7 is a diagram showing, by way of example, procedures between the IC card, the IC card terminal and the management center at the time of writing amount-of-money information into the IC card;

Fig. 8 is a block diagram showing the distribution of encrypting keys for cipher communication between the IC card, the IC card terminal, the IC card dispenser and the management center;

Fig. 9 is a diagram showing the payment of charges by the IC card according to another embodiment of the present invention;

Fig. 10 is a diagram illustrating a modified form of the Fig. 5 embodiment which utilizes a time stamp;

Fig. 11 is a diagram showing a time stamp updating algorithm;

Fig. 12 is a diagram illustrating a modification of the Fig. 10 embodiment which employs random numbers;

Fig. 13 is a diagram showing procedures for registering a password in an IC card applied to a credit card, by use of the IC card terminal;

Fig. 14 is a diagram showing procedures for receiving a service by use of the IC card with the password registered therein by the process depicted in Fig. 13;

Fig. 15 is a diagram showing another example of the password registration procedure;

Fig. 16 is a diagram showing procedures for receiving a service by use of an IC card with the password registered therein by the process depicted in Fig. 15; and

Fig. 17 is a diagram illustrating another embodiment of procedures for receiving a service by use of an IC card applied to a credit card.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

In Fig. 1 there is illustrated in block form an example of the configuration of a card system for

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

making the payment of charges through use of an IC card according to the present invention. IC card terminals 2a, 2b, ... perform processing for the payment of charges for services rendered to an IC card 6. For example, when the IC card 6 is a prepaid telephone card, the IC card terminals 2a, 2b, ... provide service by telephone. The IC card terminals 2a, 2b, ..., when installed, are each connected via a communication network 3 to a management center 4 which sets and holds security information under its control. In the following description the IC card terminals will be indicated generally by a numeral 2 except when a particular one of them is intended. The IC card 6 has initial data written by the IC card dispenser 5 when it is issued, and security information necessary for the IC card 6 is provided from the management center 4. Incidentally, in the case where some functions of the management center 4 are mounted on a portable telephone terminal or the like so that they are brought to the place where the IC card terminal 2 is located, the IC card terminal 2 need not always be connected via the communication network 3 to the management center 4 when it is installed.

Fig. 2 illustrates an example of the internal configuration of the IC card terminal 2 and Fig. 3 an example of the internal configuration of the IC card 6. The IC card terminal 2 comprises an IC card reader/writer 11 which reads and writes the IC card 6 inserted thereinto, function buttons 12 as of a keyboard, a display 13, a telephone controller 14, a network interface 15 for processing communication via the communication network 3, a handset 16 and a speech circuit 17.

In the IC card 6 there are stored in a ROM 61 programs for IC card procedures, digital signature creating and verifying algorithms and so forth, and a CPU 63 controls the entire processing of the IC card while utilizing a RAM 62 as a work area and communicates with the IC card reader/writer 11 of the IC card terminal 2 via an I/O interface 65 and contacts 66.

Fig. 4A shows the process that is performed when the IC card terminal 2 is installed. The IC card terminal 2 receives from the management center 4 such pieces of terminal information as listed below when it is installed.

(1) Master public key nA for verifying a master digital signature of the management center 4;

(2) Terminal secret keys pT and qT for the IC card terminal 2 to create a digital signature;

(3) Terminal public key nT for verifying the digital signature of the IC card terminal 2;

(4) Terminal identification number IDT for identifying the IC card terminal 2; and

(5) Master digital signature SA(nT:*IDT) by the management center for the terminal public key nT and the terminal identification number IDT, where the symbol "*" represents concatenation--for example, 001*0101 = 0010101.

After receiving these pieces of information, the IC card terminal 2 verifies the validity of the master digital signature SA(nT*IDT) through use of the terminal public key nT, the terminal identificaion number IDT and the master public key nA, and if the master digital signature SA(nT*IDT) is valid, then the IC card terminal 2 records these pieces of information in a terminal information area $2M_1$ of a memory in the telephone controller 14. No description will be given of the method for verifying the digital signature, because it is disclosed in the afore-noted various digital signature schemes. As described previously, the verification of the digital signature S(M) generally calls for an unsigned full document M and a public key for verification use, but in the following description there are cases where a simplified description, "the digital signature is verified using the public key" or "digital signature is verified" is used.

Incidentally, the management center 4 has set therein its master secret keys pA and qA and has functions of creating a different terminal identification number IDT for each IC card terminal 2 and the terminal public key nT and the terminal secret keys pT and qT corresponding to the terminal identification number IDT.

It is preferable that the terminal secret keys pT and qT be recorded in the terminal information area $2M_1$ in the IC card terminal 2 which is not easily accessible from the outside, for example, in a RAM of a one-chip CPU or battery backup RAM of a construction wherein the power supply from the battery is cut off when the IC card terminal 2 is abused.

In Fig. 4B there is shown the process that is performed by the IC card dispenser 5 when it issues the IC card 6. The IC card 6 receives from the IC card dispenser 5 such pieces of card information listed below that need to be held in the IC card 6. These pieces of information are provided in advance from the management center 4 to the IC card dispenser 5.

(1) Master public key nA for verifying the master digital signature of the management center 4;

(2) Card secret keys pU and qU for the IC card 6 to create it digital signature;

(3) Card public key nU for verifying the digital signature of the IC card 6;

(4) Card identification number IDU for identifying the IC card 6;

(5) Master digital signature SA(nU*IDU) of the management center 4 for the card public key nU and the card identification number IDU.

After receiving these pieces of card information, the IC card 6 verifies the validity of the master digital signature SA(nU*IDU) through use of the

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

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.