(12) PATENT
(19) AUSTRALIAN PATENT OFFICE

(11) Application No. AU 199869230 B2
(10) Patent No. 723525

(54) Title

Rollup certification in a reader

(51)[6] International Patent Classification(s)
G07F 007/10 G07F 009/08

(21) Application No: 199869230 (22) Application Date: 1998.03.11

(87) WIPO No: WO98/44464

(30) Priority Data

(31) Number	(32) Date	(33) Country
97/04090	1997.04.03	FR

(43) Publication Date : 1998.10.22
(43) Publication Journal Date : 1998.12.10
(44) Accepted Journal Date : 2000.08.31

(71) Applicant(s)

Gemplus S.C.A.

(72) Inventor(s)

Mounji Methlouthi; Jean-Louis Valadier

(74) Agent/Attorney

PHILLIPS ORMONDE and FITZPATRICK,367 Collins Street,MELBOURNE VIC 3000

(56) Related Art

EP 0417007
EP 0671712
GB 2287565

OPI DATE 22/10/98 APPLN. ID 69230/98
AOJP DATE 10/12/98 PCT NUMBER PCT/FR98/00511

AU9869230

ETS (PCT)

(51) Classification internationale des brevets 6 : G07F 7/10, 9/08

A1

(11) Numéro de publication internationale: WO 98/44464

(43) Date de publication internationale: 8 octobre 1998 (08.10.98)

(21) Numéro de la demande internationale: PCT/FR98/00511

(22) Date de dépôt international: 11 mars 1998 (11.03.98)

(30) Données relatives à la priorité:
97/04090 3 avril 1997 (03.04.97) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: GEMPLUS S.C.A. [FR/FR]; Parc d'activités de Gémenos, Avenue du Pic de Bertagne, F–13881 Gémenos Cedex (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: METHLOUTHI, Mounji [FR/FR]; Quartier Passe le Temps, F–13114 Puyloubier (FR). VALADIER, Jean–Louis [FR/FR]; 22, impasse Omphale, F–13011 Marseille (FR).

(74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., Z.I. Athelia III, Voie Antiope, F–13705 La Ciotat Cedex (FR).

(81) Etats désignés: AU, BR, CA, CN, JP, KR, MX, RU, SG, US, VN, brevet européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.
Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues.

(54) Title: ROLLUP CERTIFICATION IN A READER

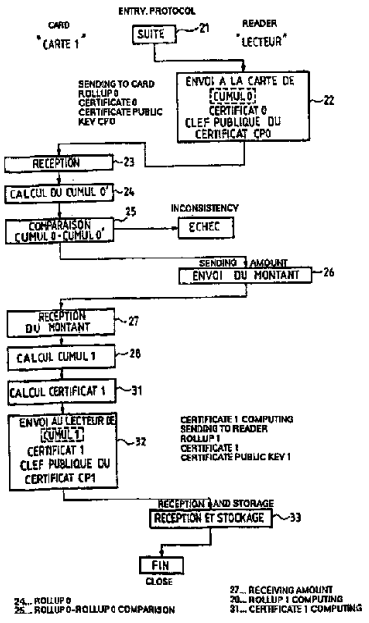
(54) Titre: PROCEDE DE CERTIFICATION D'UN CUMUL DANS UN LECTEUR

(57) Abstract

The invention concerns a method for rollup certification which comprises the following steps: during data exchange between an electronic purse and a reader, transmitting (22) from the reader to the electronic purse the rollup contained in the reader, a certificate associated with said rollup and a cryptographic public key corresponding to an unknown private key, with which the certificate has been produced from the rollup; decrypting (24) in the smart card the certificate from the public key and verifying (25) that the rollup is consistent; for the next transaction, computing (21) a new rollup then a new certificate (31) from a private key pertaining to the receiver card; then sending (33) to the reader the new rollup, the new certificate and the public key corresponding to the card which has just carried out the operation, thereby eliminating the need to store in the reader a security circuit to carry out certification.

(57) Abrégé

Lors de l'échange d'informations entre un porte–monnaie électronique et un lecteur, on transmet (22) du lecteur au porte–monnaie électronique le cumul contenu dans le lecteur, un certificat associé à ce cumul et une clé publique de chiffrement correspondant à une clé privée, inconnue, avec laquelle le certificat a été élaboré à partir du cumul. Dans la carte à puce on déchiffre (24) le certificat à partir de la clé publique et on vérifie (25) que le cumul est cohérent. Pour une transaction suivante, on calcule (21) un nouveau cumul puis un nouveau certificat (31) à partir d'une clé privée propre à la carte réceptrice. On envoie (33) ensuite au lecteur le nouveau cumul, le nouveau certificat et la clé publique correspondant à la carte qui vient d'effectuer l'opération. On montre qu'en agissant ainsi on n'a plus besoin de stocker dans le lecteur un circuit sécurisé pour faire des certifications.



A METHOD FOR CERTIFYING A RUNNING TOTAL IN A READER

The object of the present invention is a method for certifying a running total in a reader, or terminal, when this reader is used with a portable payment medium (for example, preferably a smart card). In the present application, the term smart card covers the term portable electronic circuit medium.

Running total will principally be referring to monetary arithmetic operations (or those concerning units), the certification serving to guard against frauds. But under the term "running total", information of any sort whatsoever can quite just as easily be represented, the certification serving to provide authentication of this information which can be anything. Although subsequently the term running total will always be used, for simplicity of understanding, it is self-evident that the invention can be applied to certifications of any information whatsoever and in

particular simply to certification of the amount of a transaction.

In the prior art, payment by means of a portable object, in practice by smart card, is performed as follows. A purchaser, at the time of paying for his purchase, places his bank payment smart card in a smart card reader which is in the possession of a vendor. The latter then instigates a payment whose presence, for the purchaser, is marked by the appearance, on the screen of the reader, of the amount of his purchase and by an invitation for this purchaser to enter the secret code for his card. When he has entered and validated the secret code for his card, the purchase is complete. In fact, at the time of this completion, the reader performs two types of operation. Firstly, it stores the bank details of the purchaser (it removed them from the card of the purchaser when this was passed through) corresponding to the amount of the purchase as well as to other ancillary data (the date, the time, and the references of the reader or of the vendor). Furthermore, the reader performs a running total operation consisting in adding the amount of the purchase made by this purchaser to a running total of the purchases made by the previous purchasers which have come to the shop, and which have been served by the same reader. The two items of information are therefore on the one hand an item of information necessary for debiting the current account of the purchaser and on the other hand for crediting the current account of the vendor.

The running total thus recorded therefore has a financial value and the integrity of this value should be protected from fraudulent manipulations. To achieve this, equipping the reader with a so-called SAM (Secure Application Module) security circuit, which performs a certification of the running totals, is known. The certification amounts to calculating a certificate, a string of binary characters, which is a result of an operation of encrypting the running total with an encryption algorithm. The encryption algorithm is in general of the DES type, the RSA type, or some other. The special feature of algorithms of this type is the ability to be parameterized by an encryption key. The encryption key is normally secret: it is stored inside the SAM circuit. The complexity of the encryption algorithms cited is such that it is accepted, nowadays, that these algorithms cannot be broken, that is to say it is not possible to recover the encryption key from the knowledge of an amount, which is known, which has been encrypted and of which the result of encryption is known. The result of the encryption is precisely this certificate.

In other words, with this security system, a sensitive information item, the running total information, has been replaced by a pair of protected information items, the running total associated with its certificate.

At the end of the day, when he does his till, the vendor connects his reader to a central service: in general the central service of his bank. He then

transmits, to his bank, the information relating to the purchasers and the information which concerns him: the running total of the purchases made in his shop and the certificate attached to this running total. In the central service, verifications are performed, notably using the certificate, and the amount of the running total is credited to the account of the vendor.

For the central operator, in the course of time, the number of readers which are connected each evening can be very large. It can reach several million.

At present, for well understandable reasons of caution, it is accepted that it is necessary to change the SAM circuits in all the readers periodically. For example, the periodicity is of the order of two or three years. This operation is on the one hand costly and furthermore very difficult to carry out, in view of the fact that it cannot be performed everywhere at the same time, that it is necessary, and that it is not in any case practical.

Yet more generally, if the bank payment cards of the customers are replaced by electronic purse type cards, the problem becomes still more crucial. This is because, in the case of the electronic purse card or portable medium, there is no longer any identification of a customer current account. The purse can be anonymous and it contains monetary units. There is therefore furthermore no possibility of verification for this reason.

In this last case as in the first case, it is envisaged that skilful fraudsters may be tempted to

tamper with or to seek to ascertain, by means of very frequent operations, the secret of the SAM circuit.

The object of the invention is to remedy this drawback by making provision to not equip the readers with security circuits. Therefore the management of these readers will be completely removed. There is no longer any at all. In order nevertheless to retain the comfort of security supplied by the system of a running total associated with a certificate, provision is made to keep such a system. However, in the invention, the parameterization of the encryption algorithms will no longer be performed by a secret private key contained in the security circuit, itself contained in the reader, but by a secret private key contained in a memory of the smart card of the customer. It will thus be shown that total freedom from the necessity of having a SAM circuit in the reader can be gained. In practice, execution of the encryption algorithms will even be carried out in the card. However, this execution could be carried out in the reader, by a microprocessor of this reader, provided that this reader receives, from the card, the secret private encryption key.

According to one aspect of the present invention there is provided a method for certifying an item of information in a reader, characterised in that

- there is stored, in a smart card, a pair of associated encryption keys, a private key of the card and a public key of the card,
- the smart card receives a previous certificate corresponding to a previous information item, and a previous public key,
- the card extracts from the previous certificate an image of the previous information by implementing an algorithm for encrypting this previous certificate using the previous public key,
- the card verifies that the image of the information is consistent,
- a new information item is calculated on the basis of the previous information item and a transaction information item,
- the card signs the new information with its private key by implementing an encryption algorithm in order to obtain a new certificate corresponding to the new information,
- and the new certificate corresponding to the new information, and the public key of the card are stored in the reader.

According to a further aspect of the present invention there is provided a method for certifying an item of information in a reader, characterised in that

- there is stored, in a smart card, a pair of associated encryption keys, a private key of the card and a certified public key of the card,
- there is stored, in the card or in the reader, a public certification key, the public certificate key being associated with a private certification key, the certified public key of the card recorded in the card having been obtained by encrypting this public key of the card by means of an encryption algorithm using this private certification key,
- the smart card receives from the reader, a previous certificate corresponding to a previous information item, and a certified public key of a previous card,
- the card extracts the public key of the previous card by implementing an algorithm for encrypting the received certified public key of the previous card using the public certification key,

- the card extracts an image of the previous information by implementing an algorithm for encrypting the previous certificate using the public key of the previous card extracted previously,
- the card verifies that the image of the information is consistent,
- the card calculates a new information item on the basis of the previous information item and a transaction information item,
- the card signs the new information with its private key by implementing an encryption algorithm using the private key of the card in order to obtain a new certificate corresponding to the new information,
- and the new certificate, and the certified public key of the card, are stored in the reader.

It should be noted that, from two associated keys, data can be signed, that is to say encrypted, with one key (for example a private key) and decrypted with the associated key (for example a public key) or vice versa. Furthermore, associated keys can be found, one from the other, only in a single direction: a private key being able to generate a public key. In the case of DES type algorithms, mother keys and daughter keys are referred to, a mother key being able to have a number of daughters.

A feature of the invention may be to store, in a terminal, a certificate, CERTIFICATE 0, relating to an amount and to a public key CP0. The public key CP0 corresponds to a private key CS0 with which the certificate CERTIFICATE 0 was produced in a secure manner (in the card). This public key CP0 is the public key of a card with which a previous transaction was performed. From one transaction to another, the public key recorded in the terminal can change. In the invention, at each transaction, another public key may be stored in the terminal. The public key stored corresponds to the private key with which the last certificate was calculated. It follows from this solution that a card can verify that the running total, RUNNING TOTAL 0, stored in a terminal, correctly corresponds to the CERTIFICATE 0 stored in this terminal since it can be recovered, in the card preferably, with the public key (the public key of CERTIFICATE 0) itself also stored in the terminal.

The invention will be better understood from a reading of the following description and from an examination of the accompanying figures. These are given solely for information and are in no way limitative of the invention. The figures show:

- Figure 1: a system with a smart card and a reader which can be used for implementing the method of the invention;

- Figure 2 and Figure 3: the main steps of two preferred algorithms, showing the different steps of the method of the invention;

- Figures 4a to 4e: schematic representations of operations performed in the electronic circuits of the card and/or of the reader.

Figure 1 shows a smart card 1 comprising an electronic circuit, a chip 2. The card 1 is intended to communicate with a reader 3. The reader 3 is itself provided with means for communicating with a central service 4, the computer service of a bank for example, periodically. The communications between the reader 3 and the service 4 of the bank are of known type and do not play a part in the invention. The electronic circuit 2 of the smart card has a microprocessor 5 connected by a bus 6 to a program memory 7 and a random access memory 8 having notably a set of registers 9 to 13. The bus 6 is also connected to a non-volatile memory 14 and a connection interface represented by a connector 15. The program memory 7 and the non-volatile memory 14 will be, for example, formed based on memory cells of EPROM or EEPROM type, or the backed-up random access memory type, while the memory 8 will consist of a set of volatile dynamic or static memories. The memory 8 is however not necessarily volatile. The reader 3 has a connector 16 intended to come into contact with the connector 15 of the smart card 1 when the latter is inserted into the reader. The reader 3 also has, preferably, a microprocessor 17 connected by a bus 18 to a program memory 19 and a data memory 20. Preferably, the memory 19 and the memory 20 are non-volatile.

The program memories 7 and 19 include the programs executable by the microprocessors 5 and 17 respectively for performing, among other things, the operations in accordance with the method of the invention on the one hand, and furthermore for periodically providing the transfer of the information contained in the memory 20 to the service 4 of the bank on the other hand. At the initialization of the method, the server centre 4 can have downloaded, to the readers 3, a certificate corresponding to a running total equal to zero and resulting from an encryption algorithm (RSA for example) performed on this zero running total with an initial private key of an imaginary card. The public key corresponding to this zero running total is also downloaded to the readers 3. This private certification key is retained by the server centre 4 (which is the issuer of the card) while the corresponding public certification key is downloaded to the terminals.

The method of the invention necessitates that, in the circuit 2 of the card 1, notably in the non-volatile memory 14, there is stored a pair of associated encryption keys: a private key, CS1, for the card 1, and a public key, CP1, also for the card 1. Furthermore, there is stored in the memory 20 of the reader, preferably in a non-volatile manner in case there should be a power failure, a previous certificate CERTIFICATE 0, and a public key CP0 relating to a previous smart card with which the stored certificate, CERTIFICATE 0, was formed.

A preferred solution will be described in which the RUNNING TOTAL 0 is itself also stored in the reader 3. However, as will be seen subsequently, in view of the certification which is a redundancy of the running total, having to store this running total itself could even be avoided. For the time being, it will be accepted that a running total RUNNING TOTAL 0, relating to a previous transaction, is also stored in the memory 20.

In a first operation, step 21, Figure 2 or 3, a protocol for communication of the card 1 with the reader 3 is implemented. This protocol is preliminary to the invention; it is of known type and, as regards the invention, it requires no special feature. In a usual manner, however, this recognition and communication protocol will oblige the purchaser to enter his secret code on a keypad of the reader so that the secret code can be verified by this reader.

A first step of the method, step 22, Figure 2, consists in the sending, by the reader 3 to the card 1, of the last running total state stored in this reader. In practice, the reader therefore sends the CERTIFICATE 0, the public key CP0 of the CERTIFICATE 0 and, preferably, the RUNNING TOTAL 0 to the card 1. During a step 23, the card 1 receives these elements, and the program contained in the memory 7 causes the storage of the running total RUNNING TOTAL 0 in the running total register 9, of the certificate CERTIFICATE 0 in the certificate register 10 and of the public key CP0 of

the certificate CERTIFICATE 0 in the register 11 of the memory 8.

According to the invention, the card will first engage in an operation of verifying the consistency of the reader. It verifies in fact the consistency of the information: the structure or format of the certificates, after encryption of this certificate using the public key. The card tests as it were the fact that the reader has not been tampered with nor is a fraudulent reader or that the information has not been manipulated. With this aim, in a preferred manner, there is calculated in the card, operation 24, an image of the running total RUNNING TOTAL 0, here referred to as RUNNING TOTAL 0'. Figure 4a shows functionally the principle of step 24. This step consists in encrypting the certificate CERTIFICATE 0 (now available in the register 10) by means of an algorithm of the type held in the system, for example here, in order to be simple, an RSA type algorithm. Implementation of the algorithm is performed using the public key CP0 now available in the register 11.

It should be noted that the public key CP0, relating to a previous card 0, is associated with a private key CS0 which is unknown. This is because the private key CS0 is contained, in a secure manner, in a previous card 0 to which access is not available. The formation of the certificate CERTIFICATE 0 by a previous card consisted of encrypting the RUNNING TOTAL 0 by means of the private key CS0 so as to obtain the certificate CERTIFICATE 0.

According to the principle indicated above of the association of keys, it is possible to recover the running total RUNNING TOTAL 0 using the public key CP0 associated with the private key CS0. It is indicated, in Figure 4a, that it is RUNNING TOTAL 0' because in fact it is not known whether or not the real RUNNING TOTAL 0, preferably stored in the reader 3, is a genuine running total. At the end of the operation 24, there is therefore available, in a random access register 12, RUNNING TOTAL 0'. It is then possible, with the instructions of the program in the memory 7, to achieve the comparison, operation 25, of the running total RUNNING TOTAL 0 and the running total RUNNING TOTAL 0'. If this comparison shows any differences, the program 7 will cause a failure of the transaction and will refuse to go any further. If this comparison is correct, the remainder of the operations takes place.

Preferably, calculation of the running total RUNNING TOTAL 0' (operation 24) and comparison of the two running totals (operation 25) is performed by the microprocessor 5 executing the program in the memory 7. It would be entirely possible however to transmit, by means of the connectors 15 and 16, the elements of the program 7 to the microprocessor 17 and have it execute part of a program which would then not necessarily be contained in the memory 19. In a variant, the verification program is contained in the memory 19, but is executed by the microprocessor 5.

In addition, the verification which is concerned in the operations 24 and 25, which necessitates the storage and transfer of the running total RUNNING TOTAL 0, could be replaced by a verification of the intrinsic integrity of the calculated running total RUNNING TOTAL 0'. This is because, it is known in the algorithms, notably the RSA type algorithms, that the running total result RUNNING TOTAL 0' (Figure 4a) calculated from a certificate CERTIFICATE 0 and from a normal public key CP0, must have a particular conformation of bits. Format verifications can then be performed on this conformation. For example, on a running total RUNNING TOTAL 0', which would be coded in 512 bits, only around ten bits are used for the running total itself. All the others are conformation bits (structure, format, identifier). By way of example, batches of bits, for example 64 bits, can then be taken, the parity of each batch having to be, according to the nature of a key, alternate from one batch to another or all of the same parity or some other arrangement. Other intrinsic type verifications can be envisaged. These intrinsic verifications are such that, if the certificate CERTIFICATE 0 was not produced with a private key CS0 (because in the end a fraudster did not know it and invented a public key CP0), in this case the calculated running total RUNNING TOTAL 0' will have no consistent meaning. With the structure specific to the algorithm, it will be possible to see that this result is fundamentally false, even if, for the satisfaction of

the fraudster, the bits used for the running total indicate a substantial value.

Once the operation of verifying the previous running total has been carried through to completion, the terminal 3 sends the amount of the transaction in progress with the purchaser to the smart card 1. In practice the sending of the amount can have been performed, not at a later step 26, but at the same time as the step 22.

At a following step 27, the card receives an amount and calculates, at a step 28, a new running total: the running total RUNNING TOTAL 1. In practice, the running total RUNNING TOTAL 1 is the sum of the running total RUNNING TOTAL 0 and the amount of the transaction which is in the process of being performed.

The operations 22 to 25 can also take place before the amount appears on a screen 29 of the reader, and before the purchaser has validated his secret code, with a keypad 30.

The method of the invention continues with the step 31 during which, Figure 4b, the microprocessor 5, applying the program in the memory 7, calculates the certificate CERTIFICATE 1 in a step 31. The certificate CERTIFICATE 1 is obtained by encrypting the running total RUNNING TOTAL 1, the new running total, by implementing an encryption algorithm (for example of RSA type) using the private key of the card 1, CS1. Preferably, the running total RUNNING TOTAL 1 is first conformed (format, structure, identifier added) before being encrypted. This allows a step of verification or

intrinsic checking of the consistency of this information. This step can be implemented either by the reader or by a following card.

The card 1 next sends, at a step 32, to the reader 3, the certificate CERTIFICATE 1 which has just been calculated, and the public key CP1 which is associated with the private key CS1 with which the certificate CERTIFICATE 1 was calculated. In a preferred version, the running total RUNNING TOTAL 1 itself is sent to the reader 3.

This information is received, during a step 33, in the memory 20 of the reader 3. Either this information takes the place of previous information, or is recorded in a file, as following recordings 20'. The system is then available for a following transaction; what has been said relating to a card 0 will become true for a card 1.

Figure 3 shows a preferred variant of the invention in which the system has been complicated even further in order to make it even less fragile as regards fraudsters. Until now, it had been seen that there existed, in the card, pairs of associated keys CS1 and CP1. In the card, the key CS1 is accommodated in a secret area; it is inaccessible by reading for display or transmission. In practice, it is known how to end up with sufficient security from this point of view. As for the public key CP1, being intended to be transmitted to a reader 3, this is not stored in an inaccessible area; it is stored in an entirely readable area of the memory 14.

In the variant, this pair of keys will be replaced by another pair or a triplet of keys. The aim of the variant is to prevent a fraudster from acting should this fraudster know a pair of associated private and public keys which are compatible. The triplet of keys includes, as previously, the private key of the card CS1. It has, in the place of the public key CP1, a certified public key CPC1. This certified public key CPC1 was obtained, Figure 4c, by passing the public key CP1 of the card 1 through a certification circuit implementing an encryption algorithm. The certification circuit, and therefore the algorithm, used a private certification key, CS, known to a certification body. In an example, the certification body is the central body; for example it is the bank which manages the service 4. In this case, the private certification key CS is unknown to the whole world (except the service 4). The private key CS is stored neither in the smart cards 1, nor in any of the readers 3. On the other hand, a public certification key CP associated with the private certification key CS, with which the certified public key CPC1 was produced, is itself stored in the cards 1, or in the readers 3, perhaps even in both.

Preferably, it is stored in the cards 1 only. This has the advantage, as the cards are changed, of being able to change the private certification key/public certification key pair itself, while allowing the system to operate with old private certification key/public certification key pairs.

Figure 3 shows, following the step 21, as previously, a step 33 during which the reader 3 sends, to the card, the running total RUNNING TOTAL 0 (as previously this is not necessary but is preferred), the certificate CERTIFICATE 0 and the certified public key CPC0 of the card with which the certificate CERTIFICATE 0 was produced. During an operation 35, the card 1 receives these elements and starts by extracting, during an operation 36, the public key CP0 of the card 0. This operation is shown furthermore in Figure 4d. This operation 36 amounts to encrypting the certified public key CPC0 of the certificate CERTIFICATE 0 by implementing an encryption algorithm (RSA) using the public certification key CP. The key CP is the key associated with the private certification key. During the operation 36, the capability then exists of producing the public key CP0 of the card with which the certificate CERTIFICATE 0 was (theoretically) produced. This is depicted in Figure 4d. During an optional, but preferred, operation 37 (shown in dashes), there is carried out an intrinsic consistency verification of the key CP0 obtained. This consistency verification is in accordance with what has been seen previously. If consistency is not obtained there is a rejection and the operation is not executed. If this operation has taken place correctly, during a following step 38, the running total RUNNING TOTAL 0' is calculated, as at the step 24 (Figure 4e). Next, the comparison of the running totals RUNNING TOTAL 0 and RUNNING TOTAL 0' is performed at the step 39 as at the step 25. In the

event of failure of this comparison, there is a rejection operation as previously. Otherwise, at the step 40, as at the step 26, the amount is sent by the reader to the card.

The amount is received at the step 41 in the card, the new running total, RUNNING TOTAL 1, is calculated at the step 42, the new certificate, CERTIFICATE 1, is calculated at the step 43 (Figure 4b), and at the step 44 the card sends, to the reader, the calculated elements, i.e. essentially the CERTIFICATE 1, preferably in the preferred variant the RUNNING TOTAL 1, and furthermore, the certified public key of the card 1: CPC1. Where, on the one hand, the public certification keys are contained in the cards and where, furthermore, it is planned to change them regularly, during a possible operation 45, the card 1 sends in addition, to the reader, the public certification key CP which it contains. In this way, easy rotation of the public certification keys CP is provided when the certification body decides to change them. It is sufficient for it to distribute to its customers, purchasers, smart cards equipped with the new public certification key CP corresponding to the private key CS with which the public key CP1 of the card was itself certified.

During the operation 46, this information is received in the reader and stored in the memory 20 as previously. Preferably, the reader then engages in an operation 47 of verifying the consistency of the certified public key of the card 1 which has just been

given to it. This consistency verification is of the same type as those seen previously. The operation 47, depicted in part in Figure 4f, amounts first to calculating this public key CP1 by encrypting the certified public key CPC1 by means of an RSA encryption algorithm which uses for this encryption the public certification key CP also received. In the event of failure of verification of this consistency, the following step 48 of storing the running total is not undertaken.

In the event of rejection, the reader 3 remains in its initial state with, as the last input data, the running total RUNNING TOTAL 0 and the certificate CERTIFICATE 0.

A key is a long string of bits. In an example, a key has a length of 512 or 1024 bits.

The running totals can be of a number of types. They can be payment transaction running totals, or refund transaction running totals, or even running totals of transfers between two electronic purses by means of a reader. Furthermore, as was indicated previously, rather than running totals of monetary units, any authenticated information whatsoever may be concerned. In this case, and notably when the information is simply a transaction amount, it is not necessary for the method of the invention to comprise a step consisting of calculating the new information on the basis of the previous information and a transaction information item. The new information can be received,

deduced or read by a card before being signed with the private key of this card.

Rather than encrypting the information, Figures 4a to 4f, only by means of keys, it is possible to encrypt them by means of keys and variable information known otherwise. This variable information is for example dates, card serial numbers, or counter states of the integrated circuit on these cards. In this case, these elements can also be transmitted by the smart card to the reader so that the latter can store them and retransmit them, during a following operation, to a following card so that it can decrypt the running total from the certificate. They are also transmitted to the server centre at the time of the remote collection.

At the time of the remote collection from the reader, the set of the electronic transactions and/or the total of the amounts of the transactions and the associated certificate can be transferred to the acquisition centre. The acquisition centre can then perform following checks:

- verification of the validity of the electronic signature of each transaction thus making sure that it has not been modified,

- verification of the consistency of the total received from the terminal and of the associated certificate,

- verification that the total received from the terminal corresponds to the running total of the

electronic transactions, in order to make sure that no transaction has been added or deleted.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A method for certifying an item of information in a reader, characterised in that

- there is stored, in a smart card, a pair of associated encryption keys, a private key of the card and a public key of the card,
- the smart card receives a previous certificate corresponding to a previous information item, and a previous public key,
- the card extracts from the previous certificate an image of the previous information by implementing an algorithm for encrypting this previous certificate using the previous public key,
- the card verifies that the image of the information is consistent,
- a new information item is calculated on the basis of the previous information item and a transaction information item,
- the card signs the new information with its private key by implementing an encryption algorithm in order to obtain a new certificate corresponding to the new information,
- and the new certificate corresponding to the new information, and the public key of the card are stored in the reader.

2. A method for certifying an item of information in a reader, characterised in that

- there is stored, in a smart card, a pair of associated encryption keys, a private key of the card and a certified public key of the card,
- there is stored, in the card or in the reader, a public certification key, the public certificate key being associated with a private certification key, the certified public key of the card recorded in the card having been obtained by encrypting this public key of the card by means of an encryption algorithm using this private certification key,
- the smart card receives from the reader, a previous certificate corresponding to a previous information item, and a certified public key of a previous card,

- the card extracts the public key of the previous card by implementing an algorithm for encrypting the received certified public key of the previous card using the public certification key,

- the card extracts an image of the previous information by implementing an algorithm for encrypting the previous certificate using the public key of the previous card extracted previously,

- the card verifies that the image of the information is consistent,

- the card calculates a new information item on the basis of the previous information item and a transaction information item,

- the card signs the new information with its private key by implementing an encryption algorithm using the private key of the card in order to obtain a new certificate corresponding to the new information,

- and the new certificate, and the certified public key of the card, are stored in the reader.

3. A method according to Claim 2, characterised in that

- the consistency of the certified public key of the card is verified in the reader.

4. A method according to Claim 1, characterised in that

- the consistency of the new certificate is verified in the reader.

5. A method according to Claim 2 or Claim 3, characterised in that

- the card verifies the consistency of the extracted public key.

6. A method according to any one of Claims 1 to 5, characterised in that

- the consistency is verified by an intrinsic verification, specific to the encryption algorithm.

7. A method according to any one of Claims 1 to 6, characterised in that

- the previous information is transmitted to the card,

- it is verified that the image of the previous information is consistent with this previous information, and

- the new information is transmitted to the reader.

8. A method according to any one of Claims 1 to 7, characterised in that

- the public key for certifying keys is stored in the card.

9. A method according to any one of Claims 1 to 8, characterised in that

- the successive information items, certificates and public keys are stored in the reader.

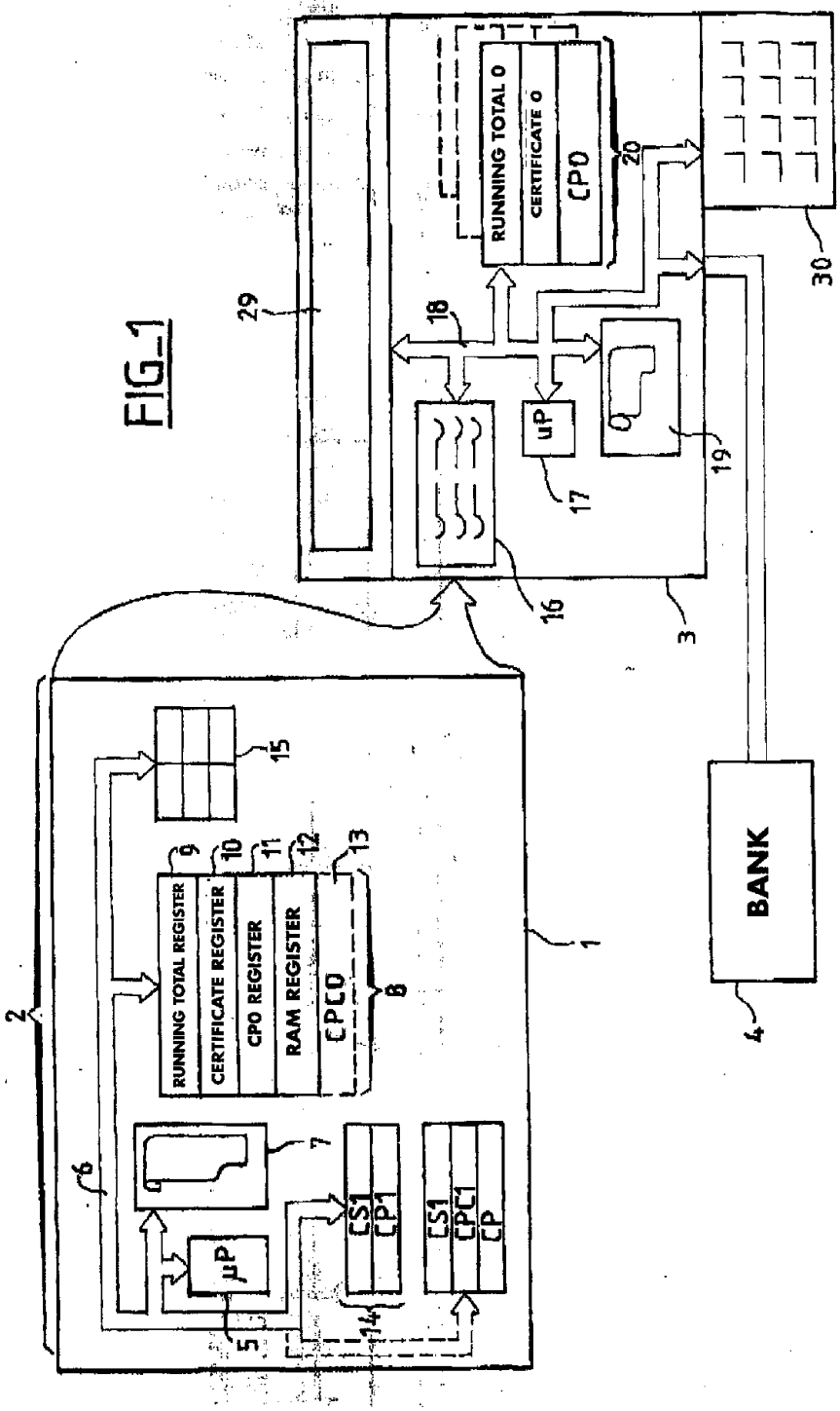
10. A method according to any one of Claims 1 to 9, characterised in that the information represents a running total and the transaction information transaction represents an amount of a transaction.

11. A method for certifying an item of information in a reader substantially as herein described with reference to the accompanying drawings.

DATED: 21 March, 2000

PHILLIPS ORMONDE & FITZPATRICK
Attorneys for:
GEMPLUS S.C.A.

FIG_1


RUNNING TOTAL 0
CERTIFICATE 0
CP0
20
30
29
18
uP
19
17
16
3
15
9
10
11
12
13
RUNNING TOTAL REGISTER
CERTIFICATE REGISTER
CPO REGISTER
RAM REGISTER
CPC0
8
1
2
6
7
CS1
CP1
CS1
CPC1
CP
μP
5
14
BANK
4

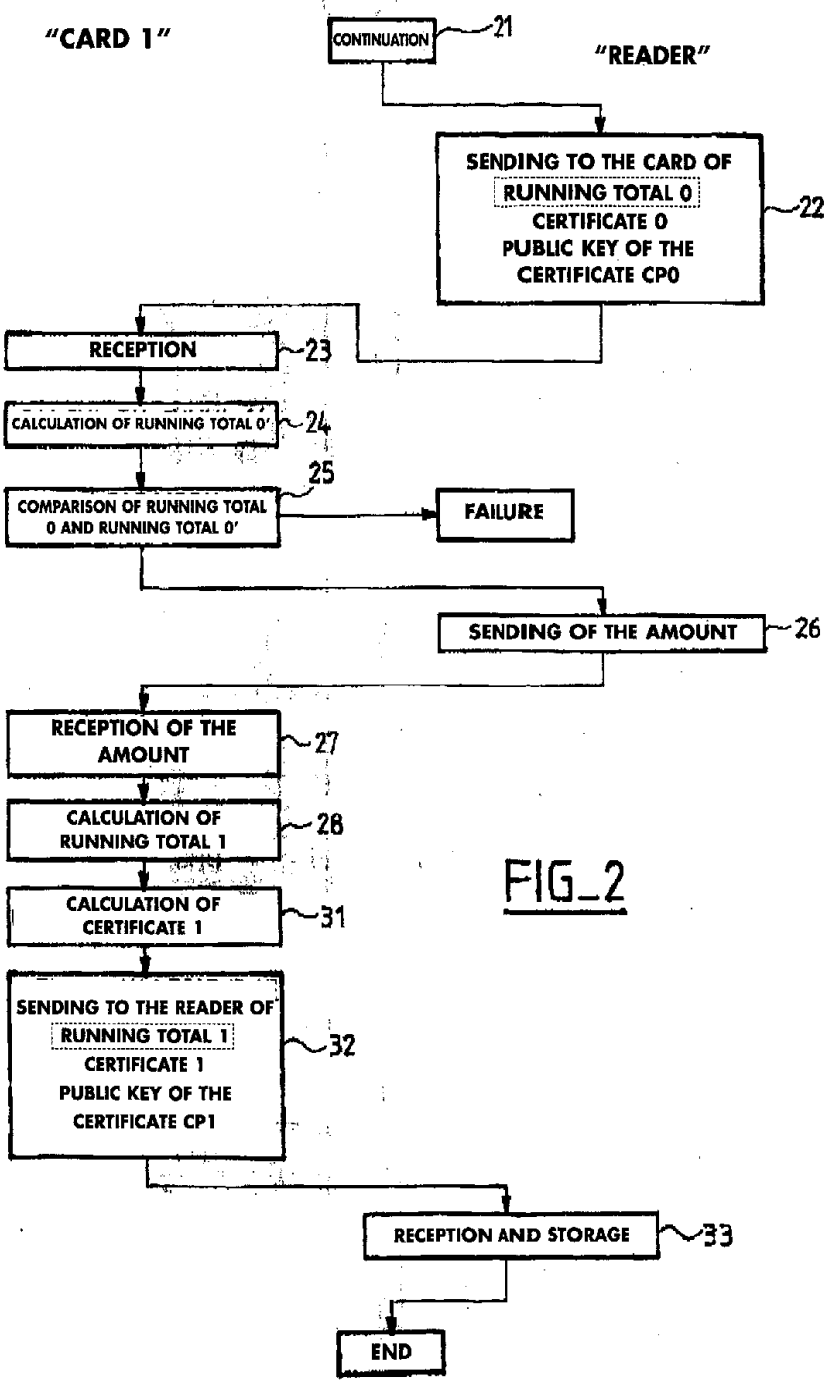
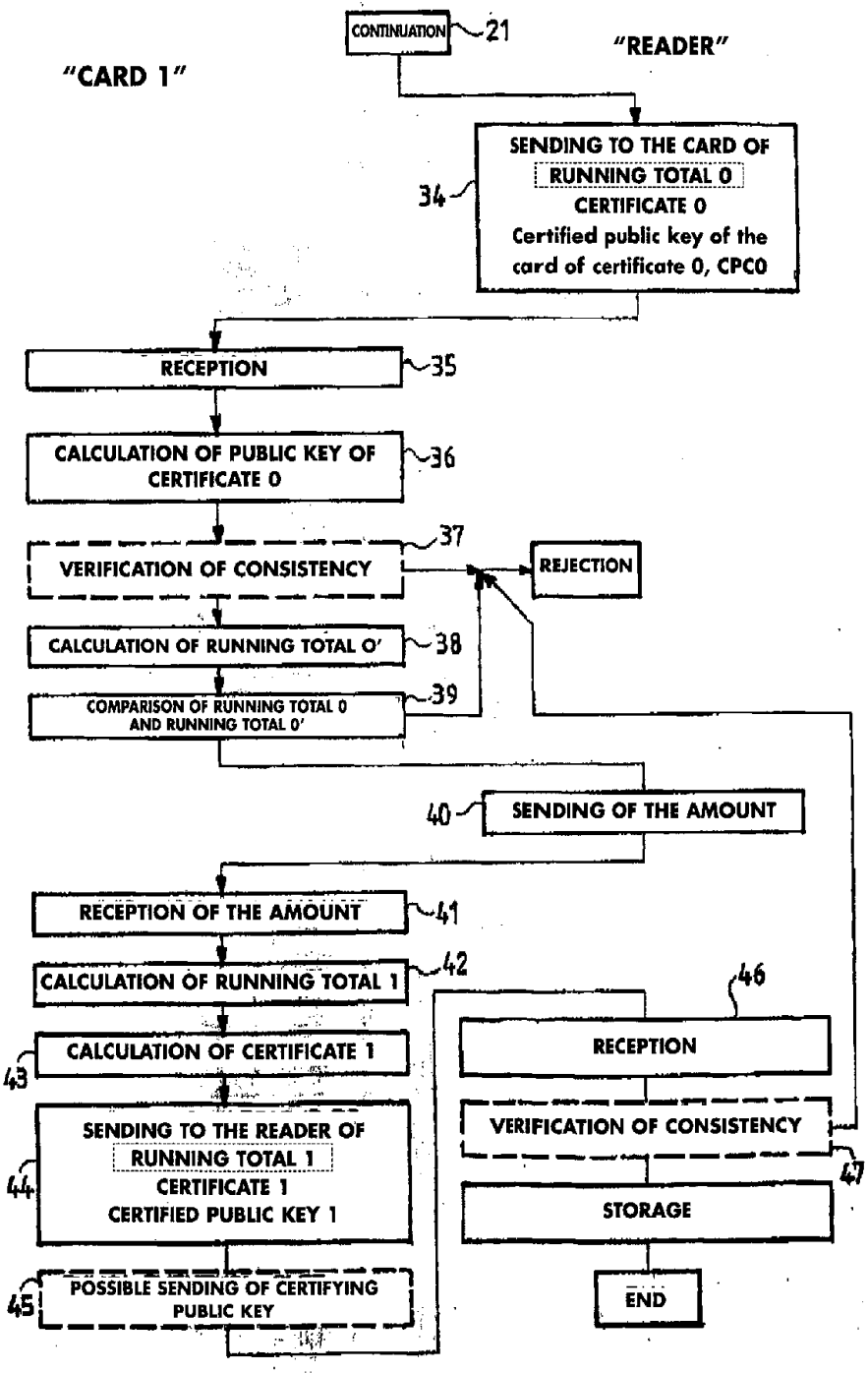

"CARD 1"
"READER"
CONTINUATION
21
SENDING TO THE CARD OF
RUNNING TOTAL 0
CERTIFICATE 0
PUBLIC KEY OF THE
CERTIFICATE CP0
22
RECEPTION
23
CALCULATION OF RUNNING TOTAL 0'
24
25
COMPARISON OF RUNNING TOTAL
0 AND RUNNING TOTAL 0'
FAILURE
SENDING OF THE AMOUNT
26
RECEPTION OF THE
AMOUNT
27
CALCULATION OF
RUNNING TOTAL 1
28
CALCULATION OF
CERTIFICATE 1
31
SENDING TO THE READER OF
RUNNING TOTAL 1
CERTIFICATE 1
PUBLIC KEY OF THE
CERTIFICATE CP1
32
RECEPTION AND STORAGE
33
END

FIG_2


"CARD 1"
"READER"
CONTINUATION
21
SENDING TO THE CARD OF
RUNNING TOTAL 0
CERTIFICATE 0
Certified public key of the card of certificate 0, CPC0
34
RECEPTION
35
CALCULATION OF PUBLIC KEY OF CERTIFICATE 0
36
VERIFICATION OF CONSISTENCY
37
REJECTION
CALCULATION OF RUNNING TOTAL O'
38
COMPARISON OF RUNNING TOTAL 0 AND RUNNING TOTAL 0'
39
40
SENDING OF THE AMOUNT
RECEPTION OF THE AMOUNT
41
CALCULATION OF RUNNING TOTAL 1
42
CALCULATION OF CERTIFICATE 1
43
SENDING TO THE READER OF
RUNNING TOTAL 1
CERTIFICATE 1
CERTIFIED PUBLIC KEY 1
44
POSSIBLE SENDING OF CERTIFYING PUBLIC KEY
45
46
RECEPTION
VERIFICATION OF CONSISTENCY
47
STORAGE
END

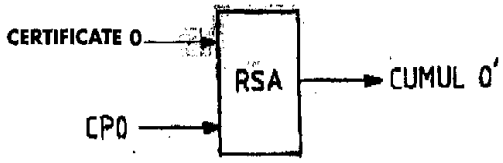


FIG_4a

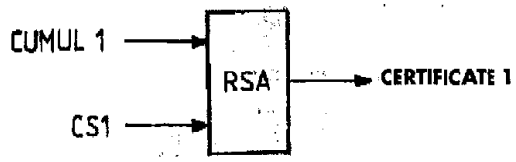


FIG_4b

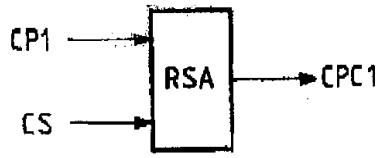


FIG_4c

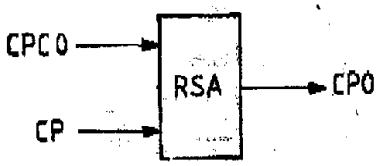


FIG_4d

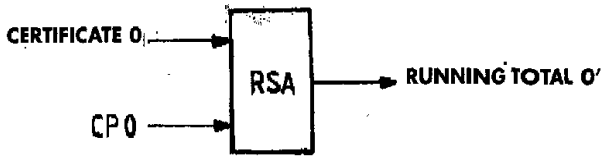


FIG_4e

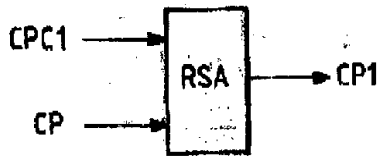


FIG_4f