SYSTEM OF PAYMENT OR TRANSFER OF INFORMATION USING AN ELECTRONIC MEMORY CARD AS A WALLET

The present invention concerns a system of payment by electronic memory card. It relates in particular to money handling systems in which, in order to avoid the theft of money and also, above all, to simplify banking operations, payment systems of the electronic type with the use of memory cards are adopted. It may nevertheless be applied in other spheres, particularly when numerical information has to be transferred and it is desired to avoid or at all events to know whether these items of information have been transformed between the place where they were emitted by an emitter and the moment when they are received by their genuine addressee.

Payment systems of the electronic type are known in which use is made of a microchip card. Systems of this kind are described, for example, in FR-A-2386080 or in DE-A-3211568. The microchip card is essentially characterized by the presence of a microprocessor. In this card the said microprocessor performs an obvious security function. The fact is that in a card of this kind a microprocessor of this type is capable of operating a complex algorithm for calculating or verifying a secret code from an item of identification data indicated to it. After this microchip card has been inserted into a reader, and if the secret code calculated is not equivalent to a secret code already contained in the card, it becomes impossible to operate with this card, so that in this case the item of identification data is known to be false. In one improved version the number of possible operations or attempts to reach the correct code is actually limited. For example, after three operations the microchip card drops into a trap forming a rear outlet of the microchip card reader. It is not even restored to its user.

This system proves satisfactory, particularly in view of the use of algorithms of the D E S type (Standard

Inscription Data in the English-language literature on the subject) which is so complex that an illicit user would require several years of work to dismantle its mechanism. These microchip cards, however, suffer from the drawback that they have to include the microprocessor and that after all they then prove very costly.

In the invention these problems are solved by the use of a memory card not necessarily comprising a microprocessor. Essentially, the memory card includes different types of zones, at least four in number. These zones may be of different technologies (EPROM, EEPROM....) since they are not volatile. More simply, the memory card to which the invention relates even includes zones which are all completely readable, only one of them not being reinscribable. This is a zone known as the identity zone, specific to the card, in order to make it impossible for two cards to be totally identical: one is a clone of the other by duplication. The principle of the invention is as follows:

It is considered that when a card holder uses his card and effects a banking operation, for example, it is possible to count these operations. It is also known that the card, being "personalized", comprises specific details relating to its holder's identity. The card may also comprise a secret access code known to the user. Under these circumstances the invention provides that each time the card is used a numerical signature is calculated which is a function of the identity, of the balance and of the number of the banking operation effected. This identity, balance and number are also recorded in three different zones of the card. This signature, taking the form of a binary sequence of logical states, is also recorded in a particular zone of the memory card in the form of a certificate.

In a subsequent operation, after any possible conventional operations to identify the holder (his indiction of his secret code and verification by a reader

that this code duly corresponds to a secret code entered in the card) the reader is caused to calculate a signature from the balance, the identity and from the number of the operation recorded in the card. This calculation of the signature is the same as that which had to be effected at the time when the signature was entered as a certificate. It is therefore possible to verify that the new signature prepared is in actual fact the same as or at least corresponds to that recorded in the card.

If this is the case a supplementary banking operation is enabled to take place on the basis of the new balance, the identity and the new operation number, which in the meantime has been incremented by one unit in order to take account of the operation which has just been carried out. This new signature is then recorded as a new certificate in the memory card, preferably in the place of the old certificate. Needless to say, the reader calculating the signature is supplied with an undecipherable calculation algorithm, preferably of the DES type. The result is that one does not achieve the same level of security as with cards having a microprocessor, but the only memory cards having to be used are now those only containing memory zones and not necessarily including the microprocessor. They are far less expensive.

The object of the invention is thus a payment system using an electronic memory card as a wallet, comprising memory cards as wallets, and one or more interaction terminals to interact on financial balances recorded in these cards, the said memory cards comprising an identity memory zone and a balance memory zone, the system comprising means for modifying, in the course of the interaction, the balance recorded in the balance zone, characterized

- in that these memory cards comprise at least two other different memory zones: an interaction counter zone and a certificate zone,
- in that the terminals comprise means before each

interaction, for

- preparing a signature from the balance recorded in the balance zone, on the basis of the contents of the counter and on the basis of the identity recorded in the identity zone,
- verifying that this signature corresponds to a certificate recorded in the certificate zone,
- and in that this system also comprises means for, at each interaction,
- incrementing the contents of the interaction counter,
- preparing a new signature as a function of the modified balance of the new contents of the interaction counter and of the identity,
- and recording the new signature as a new certificate in the certificate zone.

In an application which no longer involves financial transactions and which is now aimed at the transfer of information, the system will be a transfer system, its security characteristics remaining unchanged. In this latter case the terminals may be differentiated from one another according to whether they are simply readers or simply recorders.

The invention will be understood more clearly from a study of the description which now follows and from an examination of the diagrams by which it is accompanied. These are provided solely by way of information, the invention being in no way limited thereto. The drawings are as follows:

Figure 1 - schematic diagram of the system of the invention,

Figure 2 - a diagram showing the different verification and recording stages effected by a reader on the memory card to which the invention relates.

Figure 1 shows a system for payment by a memory card as a wallet in accordance with the invention. Although it is the banking operation that is described in the present case it will be easily understood that the

invention can be applied for transfers of information in general, a financial balance being a particular item of information in itself. This system comprises memory cards as wallets, such as the card 1. The card 1 is designed to be introduced into a reader 2 or interaction terminal. This interaction terminal is designed to interact on financial balances recorded in the card 1. Where operations effected on traders' premises are concerned, in principle at the time of the purchases, the financial balance must decrease. On the other hand, when the owner of the card goes to his bank he may have his purse filled with the total amount of his bank balance or with a sum on which he can decide in advance.

The memory cards according to the invention essentially comprise four zones. A first zone 3 serves to record an identity. This identity may correspond to the name and address of the owner. It is specific to the card. No card can have the same identity as another. Zone 3 can only be read. As it therefore cannot be written, the duplication of an already known identity is thus prevented. This identity is recorded in memory cells of the memory zone 3. The memory cells of the first zone 3 are preferably of the EPROM type, non-erasable. The cells of the other zones are preferably of the EEPROM type, electrically erasable.

The second memory zone 4 comprises a pre-recorded certificate. The zone 4 can be read and written as many times as desired. A third zone 5 concerns an interaction counter. The information content of zone 5 indicates the number of operations effected with the card since the beginning of the latter's "life". The count indicated cannot be re-zeroed or de-incremented. When the counter reaches its maximum the card can no longer be used and has to be exchanged for another. The de-incrementation is prevented by the safety mechanism of the component itself. Preferably for example the counter zone 5 is of the token type: only tokens can be used up. In this case it is in

the EPROM category. It may nevertheless be in the EEPROM category, electrically erasable, but it is then associated with a counter for counting the number of erasures, and this counter itself is then of the EPROM type. The zone 5 likewise may be read and written when desired. Finally, the card 1 comprises at least a fourth zone 6 which relates to the financial balance, the money, available to the owner.

These four zones may in practice each consist of a limited number of single memory cells. The complete system may correspond to some hundreds of bits. The secret identity code may be accommodated by a few tens of bits. The signature and the balance may even be of a lower logical magnitude. As regards the counter, this will preferably be replaced by a counting indicator. The counting and incrementation operations are then effected by the microprocessor of the reader. The zone for the balance may be a zone operated by tokens but will preferably include an indication of the balance "in - clear" in a zone of the EEPROM type. The card 1 may optionally comprise a fifth zone 11 containing a secret access code known to the owner of the card.

A description will now be given, by reference to Figure 2, of the operations performed with the memory card when an owner effects a purchase from a trader having a reader such as 2 designed for the control of these new memory cards. The operations are controlled in a known manner by a microprocessor contained in the terminal 2. When the purchase has been determined the card owner introduces his card into a reading slit 7 of the recorder reader terminal 2. In a first operation the reader 2 tries to recognize the owner. The reader 2 then emits on a display screen 8, in a known manner, questions by which the owner is requested to key in his secret code. He may do this by means of a keyboard 9 connected to the reader. The code keyed in by the owner is compared with the secret code contained in the zone 11 of the card. When they have been

compared successfully a subsequent verification is performed.

In this latter, the reader 2 uses the numerical data which is representative to the identity (contained in the zone 3), of the state of the interaction counter (contained in the zone 5) and of the state of the balance (contained in zone 6) in order to prepare a signature. This signature is mae up by the reader with the use of an algorithm of the DES type, performed by a DES operator (Figure 1). As soon as the reader 2 has prepared this signature it is compared with the signature which has already been recorded previously as a certificate in the card and which is now stored in the zone 4 of the card 1. In order to do this the reader reads the contents of the zone 4 and compares them in its logic comparator with the signature which it has just calculated. If the comparison shows the two signatures to be identical the actual purchase operation can then be carried out.

In this case the trader or possibly the customer himself may program the operation of the deduction of the balance on the reader 2. As this is a purchase operation the balance can only decrease. The reader 2 is then capable of calculating a new balance taking into account the old balance and the purchase price of the article purchased. This new balance is then recorded to replace the old balance in the zone 6 by a re-entry operation. Similarly, in view of the fact that a fresh financial banking operation has just been effected, the contents of the counter 5 are incremented by one unit. Where a visit to the bank is concerned the same action is taken. A supplementary unit is nevertheless counted in the counter, even though the balance has been increased. In practice it may even be decided to modify the contents of the counter each time something has been entered as a new balance. Once the new balance and the new value of the counter have been established the reader again prepares a new signature, with the use of the same algorithm. This new signature is

obviously different from the preceding one owing to the fact that the conditions for calculation have changed. This new signature is then recorded as a new certificate in the zone 4. As may be seen, the four zones can be read at will. The last three can even be modified at will, although the counter can only be incremented.

An algorithm of the DES type is an algorithm of the same type as those published in the "Federal Information Processing Standards Publication" on January 15th 1977 and updated on September 13th 1983 by the "American National Bureau of Standards", Pages 41009-41140. This algorithm is penetrable by a key of 64 bits. In the application considered all the readers used would be equipped with one and the same parametered version of this algorithm. Other algorithms are nevertheless possible.

The invention imparts an intrinsic integrity to the recordings, somewhat in the manner of the error corrector codes for numerical processing. This means that the system is likewise usable for the transport of any items of information, other than a balance, making it possible to verify that they have not been illicitly modified between their emission and their reception. The security is due to the complexity signature of the calculation algorithm, known elsewhere. The simplification provided by the invention is due to the fact that the card does not necessarily include a microprocessor. When we say that the card is not necessarily provided with a microprocessor we are also envisaging the applications in which microchip cards with a microprocessor are employed but in which the security level of the transaction is further improved by the adoption of the system to which the invention relates.

The operations thus described enable a high degree of security to be obtained, since a user wishing to use his card fraudulently would be unable to calculate any coherent certificate from any counter content and from a balance which this offender had naturally increased

artificially. It is thus possible to ensure that in the event of a failure in the verification of whether the new signature corresponds to the certificate the specific identity of the card will be noted in a memory of the reader 2. It may even be decided to block the card itself with a self-locking mechanism for a secret code. This self-locking mechanism comprises both a counter for counting false card presentations and a locking system of which the principle is based on the non-transmission of the secret code or of the identity beyond the counting threshold of the counter for the false presentations.

The payment system to which the invention relates thus preferably comprises a server 10 which periodically operates in conjunction with all the readers 2 of its network. For example, a reading is taken every night. In the course of this reading each reader transmits to the server 10 the amounts of the transactions with the accounts of each of the card owners. It also transmits, in a black list, the specific identities of the memory cards which have caused a failure in the verification of the signature with their certificate. A concatenated black list is then sent, with the same periodicity every night, to all the interaction terminals 2, in such a way that the next morning each of them knows, in its own memory, the list of the identities of the cards to be rejected. It then becomes impossible for the owners of these cards to use them for any operation. For this purpose the identity of the card is compared, at the time of the first verification, with all the "prohibited identities" contained in the black list.

For cases in which a reader 2 is stolen it is possible to secure it by using a memory card 12 known as a security card. This security card 12, this time with a microprocessor, has to be inserted into the reader. It comprises the DES algorithm with a parametered secret key associated with the system of the invention. The use of this card, which enables the certificates of the wallets to

be calculated, is subordinate, each time the terminal 2 is rendered live, to the presentation of the carrier code of this card. This carrier code is a code known by the person authorized to use the terminal. It may also be keyed in with the keyboard 9. This card 12 must be permanently present in the reader 2 to render is valid.

Furthermore, in view of the fact that the list of operations effected is communicated to the server each evening, any card of which the balance has been increased may be regarded as a falsified card if its carrier cannot present the mark and the proof of the recharging.

Since a reader, if it is to remain authorized by the network, has to be periodically connected to the server 10, it is naturally easy for this server 10 to verify that during each period the reader 2 has not effected any operations of a prohibited type. For example, a trader cannot effect any balance increases on the cards introduced into his reader.

CLAIMS

1. Payment system using an electronic memory card as a wallet, comprising memory cards (1) as wallets and one or more interaction terminals (2) to interact on financial balances recorded in these cards, the said memory cards comprising an identity memory zone (3) and a balance memory zone (6), the system comprising means for modifying, in the course of the interaction, the balance recorded in the balance zone, characterised

- in that these memory cards comprise at least two other different memory zones: an interaction counter zone (5) and a certificate zone (4),
- in that the terminals comprise means before each interaction, for
- preparing a signature from the balance recorded in the balance zone, on the basis of the contents of the counter and on the basis of the identity recorded in the identity zone,
- verifying that this signature corresponds to a certificate recorded in the certificate zone,
- and in that this system also comprises means for, each interaction,
- incrementing the contents of the interaction counter,
- preparing a new signature as a function of the modified balance of the new contents of the interaction counter and of the identity,
- and recording the new signature as a new certificate in the memory card.

2. System according to claim 1, characterised in that the interaction terminal, comprise means for preparing a new signature with the application of an algorithm of the type DES.

3. System according to claim 1, characterised in that the terminals (2) comprise means for transmitting to a server (10) an identity of the memory cards for which the verification of the signature has not corresponded to a certificate recorded beforehand in the certificate zone.

4. System according to any one of claims 1 to 3, characterised in that the terminals (2) comprise memories for recording and permanently verifying that the identity entered in a card which has been introduced does not appear on a black list.

5. System according to claims 1 to 4, characterised in that the memory zone allocated to the counting of the interactions cannot be de-incremented.

6. System for transfer of information by electronic memory card, comprising memory cards and one or more interaction terminals designed to interact on items of information recorded in these cards, these memory cards comprising an identity zone and an information storage zone, this system comprising means for modifying, in the course of each interaction, the items of information (1) stored in the information storage zone, characterised

- in that the memory cards comprise at least two other memory zones: an interaction counter zone and a certificate zone,
- in that the terminals comprise means for, prior to each interaction,
- preparing a signature from the items of information stored in the information storage zone, from the contents of the counter and from the identity recorded in the identity zone,
- and verifying that this signature corresponds to a certificate recorded in the certificate zone,
- and in that this system likewise comprises means for, at each interaction,
- incrementing the contents of the interaction counter,
- preparing a new signature as a function of the modified items of information, of the new contents of the interaction counter, and of the identity,
- and recording the new signature as a new certificate in the memory card.