Method of debiting an electronic payment means.

BACKGROUND OF THE INVENTION

The invention relates to a method of debiting an electronic payment means, such as an electronic payment card provided with an intergrated circuit ("chip card"). In particular, though not exclusively, the invention relates to a method for protectedly debiting prepaid electronic payment cards ("prepaid cards") as these are applied, e.g., for telephone booths. In the present text, the term payment means will be used irrespective of the form or the type of the specific payment means. A payment means may therefore be formed by, e.g., a revaluable payment card (i.e. a payment card whose balance may be increased) or a non-card-shaped electronic payment means.

In recent years, electronic payment means are being applied ever more frequently, not only for paying for the use of public telephone sets, but also for many other payment purposes. Since such a payment means generally comprises a (credit) balance which represents a monetary value, it is necessary to have the exchange of data between such a payment means and a payment station (such as a telephone set designed for electronic payment or an electronic cash register) run according to a protected method (payment protocol). Here, it should be ensured, e.g., that an amount (monetary value or number of calculation units) debited to the payment means correspond to an amount (monetary value or calculation units) credited elsewhere: the amount paid by a customer should correspond to the amount to be received by a supplier. The credited amount may be stored, e.g., in a protected module present in the payment station.

Prior Art payment methods, as disclosed in e.g. European Patent Application EP 0,637,004, comprise: a first step, in which the balance of the payment means is retrieved by the payment station; a second step, in which the balance of the payment means is lowered (debiting the payment means); and a third step, in which the balance of the payment means is retrieved again. From the difference between the balances of the first and third steps the debited amount may be determined and therewith the amount to be credited in the payment station. In order to prevent fraud here, in the first step use is made of a random number which is generated by the payment station and is transferred to the payment means. On the basis of the first random number, the payment means generates, as a first response, an

authentication code which may comprise an (e.g., cryptographic) processed form of, inter alia, the random number and the balance. By using a different random number for each transaction, it is prevented that a transaction may be imitated by replay. In addition, in the third step use is made of a second random number, which is also generated by the payment station and transferred to the payment means. On the basis of the second random number the payment means generates, as a second response, a second and new authentication code which may comprise a processed form of, inter alia, the second random number and the new balance. On the basis of the difference between the two transferred balances, the payment station (or a protected module of the payment station) determines by which amount the balance of the payment station should be credited.

Said known method is basically very resistant to fraud as long as a payment means communicates with one payment station (or protected module). The drawback of the known method, however, lies in the fact that the first and second authentication codes are independent. If a second or third payment station (or protected module) communicates with the payment means, it is possible, due to said independence, to separate the first step from the second and third steps. As a result, an apparently complete transaction may be achieved without the payment means in question being debited. It will be understood that such is undesirable.

US Patent US 5,495,098 and corresponding European Patent Application EP 0,621,570 disclose a method in which the identity of the security module of the payment station is used to ensure that a data exchange takes place between the card and one terminal only. The protection of the data exchange between the security module, the station and the card is relatively complicated and requires extensive cryptographic calculations.

Other Prior Art methods are disclosed in e.g. European Patent Applications EP 0,223,213 and EP 0,570,924, but these documents do not offer a solution to the above-mentioned problems.

SUMMARY OF THE INVENTION

It is an object of the invention to eliminate the above and other drawbacks of the Prior Art, and to provide a method which offers an even greater degree of protection of debiting transactions. In

THIS SHEET HAS BEEN REPLACED

particular, it is an object of the invention to provide a method which ensures that during a transaction only one payment station is credited.

Accordingly, the present invention provides a method of performing a transaction using an electronic payment means and a payment station, the method comprising the repeated execution of an interrogation step in which the payment station interrogates the payment means and receives payment means data in response, the payment means data comprising an authentication code produced by a predetermined process, a subsequent authentication code being linked to a preceding authentication code of the same transaction by states of said process.

By providing a link between the authentication codes, it can be ensured that the data received by the payment station are unique to that station. In order to link the authentication codes of the different steps the process, in an interrogation step, preferably uses an initial value derived from the final state of the process in the preceding interrogation step.

More specifically, the present invention provides a method of protectedly debiting an electronic payment means using a payment station, the method comprising:

- a first step, in which:
  - the payment station transfers a first random value to the payment means,
  - the payment means, in response to said first random value, transfers a first authentication code to the payment station, which authentication code is determined on the basis of at least a first start value, the first random value and the current balance of the payment means using a predetermined process, the process further producing a first end value,
- an optional second step, in which:
  - the payment station transfers a debiting command to the payment means, and the balance of the payment means is lowered on the basis of the debiting command, and
- a third step, in which:
  - the payment means transfers a second random value to the payment means, and the payment means, in response to said second random value, transfers a second authentication code to the payment

This Sheet Has Been Replaced



THIS SHEET HAS BEEN REPLACED

station, which authentication code is determined on the basis of at least a second start value, the second random value and the current balance of the payment means using said process, the second start value being based on the first end value.

The method according to the invention is thus characterised in that the second start value is based on the first end value.

By basing the second start value on the first end value, i.e. on the state of the process after completion of the first authentication code, a direct coupling between the first step and the remaining steps is obtained and it is no longer possible to interrupt the method, or to exchange data with other payment stations, without such being noticed. Here, the second start value, which may form, e.g., the initialisation vector of a cryptographic process, may be identical to the first end value or be derived from the first end value. In the first case the first end value may be stored, in the second case the second start value may be, e.g., the state of a (cryptographic) process which, starting from the first end value, has been executed a number of times. In either case, the second start value may be reproduced from the first end value, as a result of which a check on the authenticity is offered, and thereby on the continuity of the method.

The process may, in the third step, produce a second end value which may be used for deriving start values for possible additional steps.

The invention is therefore based on the insight that the application of multiple independent start values on authentications in consecutive steps of a debiting transaction under certain circumstances creates the possibility that not all steps of the transaction are carried out between the same pair of a payment means and a payment station.

The invention further provides an advantageous implementation of the said method in existing electronic payment means.

In the above reference is made to a payment station with which the payment means (card) communicates. A payment station may have an integrated storage of transaction data or a separate module. It will be understood that the payment means may in practice communicate with the protected module ("Security Module") via the payment station in case the payment station uses such a module for the secure storage of

This Sheet Has Been Replaced

transaction data.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be explained in greater detail below by reference to the Figures.

Fig. 1 schematically shows a payment system in which the invention may be applied.

Fig. 2 schematically shows a method in which the invention is applied.

Fig. 3 schematically shows further details of a method in which the invention is applied.

Fig. 4 schematically shows an alternative embodiment of the method of Fig. 3.

Fig. 5 schematically shows the integrated circuit of a payment means with which the invention may be applied.

PREFERRED EMBODIMENTS

The system 10 for electronic payment schematically shown in Fig. 1, by way of example comprises an electronic payment means, such as a so-called chip card or smart card 11, a payment station 12, a first payment institution 13, and a second payment institution 14. The payment station (terminal) 12 is shown in Fig. 1 as a cash register, but may also comprise, e.g., a (public) telephone set. The payment institutions 13 and 14, both denoted as bank in Fig. 1, may not only be banks but also further institutions having at their disposal means (computers) for settling payments. In practise, the payment institutions 13 and 14 may form one payment institution. In the example shown, the payment means 11 comprises a substrate and an integrated circuit having contacts 15, which circuit is designed for processing (payment) transactions. The payment means may also comprise an electronic wallet.

Between the payment means 11 and the payment station 12 there takes place, during a transaction, an exchange of payment data PD1. The payment means 11 is associated with the payment institution 13, while the payment station 12 is associated with the payment institution 14. Between the payment institutions 13 and 14 there takes place, after a transaction, a settlement by exchanging payment data PD2, which is derived from the payment data PD1. During a transaction

there basically does not take place communication between the payment station 12 and the payment institution 14 in question (so-called off-line system). Transactions must therefore occur under controlled conditions to ensure that there can take place no abuse of the system. Such an abuse may be, e.g., increasing a balance of the payment means (card) 11 which is not matched by a balance change of a counterpart account at the payment institution 13.

The diagram of Fig. 2 shows the exchange of data between (the integrated circuit of) a payment means denoted as "Card" (11 in Fig. 1) and (the security module of) a payment station denoted as "Terminal" (12 in Fig. 1), with consecutive occurrences being shown one below the other.

In the first step, denoted by I, the terminal produces a first random number R1 and transfers this number to the card (substep Ia). On the basis of the random number R1 and other data, preferably including the card balance S1, the card produces an authentication code MAC1 = F(R1, S1, ...), where F may be a cryptographic function known per se. This will later be further explained with reference to Figs. 3 and 4. The code MAC1 ("Message Authentication Code") is transferred to the terminal along with at least the balance S1 (substep Ib). After checking the authentication code MAC1, the terminal records the balance S1.

In the second step, denoted by II, the terminal produces a debiting command D, which comprises the value (amount) to be debited to the card. The debiting command D is transferred to the card, whereafter the balance S1 of the card is lowered by the amount to be debited, resulting in a new balance S2. The carrying out of step II is not essential to the invention. In practice, step II may be carried out an arbitrary number of times, including zero.

In the third step, denoted by III, the terminal produces a second random number R2 and transfers this to the card (substep IIIa). On the basis of the random number R2 and other data, including the new balance S2 of the card, the card produces an authentication code MAC2 = F(R2, S2, ...), where F may be a cryptographic function known per se. The new balance S2 and the authentication code MAC2 are transferred to the terminal (substep IIIb). The terminal checks the authentication code MAC2, e.g., by regenerating the code using R2 and S2, and comparing the regenerated and received codes. Alternatively,

the terminal may decipher the code MAC2 to obtain R2 and S2. Said deciphering may take place, e.g., by carrying out the inverse of the function F.

After a positive check of the code MAC2, the new balance S2 is recorded in the terminal. It will be understood that the repeated transfer of balances to the terminal is not essential to the present invention. In this respect, the transfer of the card balance may be omitted and be replaced by e.g. a decrease acknowledgement in the third step, after which the amount of the decrease (as transferred to the card in step II) is recorded in the terminal. A card identification may be transferred to the terminal in the first and third steps, in addition to, or instead of, a card balance.

In a fourth step, denoted by IV, the difference of the balances S1 and S2 is determined in the terminal and recorded there. In this connection, such difference may either be stored separately or be added to an existing value (balance of the payment station) to be settled later. Said fourth step, as well as possible following steps, is not essential for the invention. The steps shown in Fig. 2 may be preceded by an authentication or verification step in which the key is identified which is to be used for producing the authentication codes. Preferably, a different key is used for each batch of cards or even for each individual card. This may for example be accomplished by means of key diversification on the basis of a card identity number, a technique well known in the art.

In the diagram discussed above, the random values R1 and R2 are different. The random values R1 and R2 may be identical (R1 = R2 = R), however, so that in step III it may be checked whether in the authentication code MAC2 use is still being made of the same random number R (= R1).

According to the prior art, the authentication values MAC1 and MAC2 are basically independent. This is to say that, if the random numbers R1 and R2 differ, there is no direct or indirect relationship between the values of MAC1 and MAC2 since the process (function F) with which the authentication code is determined, always assumes the same start value, namely, the start value zero. Due to this independence, there is basically no guarantee that the steps I and III are carried out between the same pair of a card and a payment station.

According to the invention, however, when determining the second

authentication code (MAC2) there is assumed a start value which is the result of the determination of the first authentication code (MAC1). As second start value there may be used, e.g., the state of the (cryptographic) process after the determination of the first authentication code. In this connection it is not essential whether the process, after the determination of the first authentication code, has still gone through a number of process steps, since the dependence and the reproducibility of the second start value will be guaranteed.

The said dependence of the start values in accordance with the invention ensures that all steps of the transaction, in which the method according to the invention is applied, take place between the same card and the same payment station.

The relationship between the start values will now be explained with reference to Fig. 3, in which the steps I and III may be identical to the steps I and III in Fig. 2. In step I, the first authentication code MAC1 is generated using a function F, which may be a cryptographic function known per se, such as a DES ("Data Encryption Standard") function, or a relatively simple combinatorial function (see also Fig. 5) or "hash" function. This function F has the first random value R1, the first (old) balance S1, a key K and a first start value Q1 as input parameters. Optionally, an identification of a debiting command (as used in step II) may be used as input parameter. A clock pulse α, which may be identical to the clock α of Fig. 5, is shown to control the processing.

The first start value (initialization vector) Q1 may be equal to zero or to another preset iritial value if no previous processing involving the function F has taken place before activation of the card (activation may take place by inserting the card in the terminal).

The function F produces an authentication code MAC1. Additionally, the state ("residue") of the function F is saved as first end value Y1. This first end value Y1 will later be used in step III as second start value Q2 (Q2 = Y1), thus linking the first and third steps.

In step III, the second authentication code MAC2 is generated using the function F, which preferably is identical to the function F of step I. Here, the function F has the second random value R2, the second (new) balance S2, the key K and the second start value Q2 as input parameters. The function F produces the second authentication

code MAC2 and, additionally, the second end value Y2 which is the state of the function F after the processing. The second end value Y2 may be saved to be used as third start value (Q3) in case a third authentication code (MAC3) involving the same card and security module (terminal) is required. Generally, the deactivation of the card (e.g. by removing the card from the terminal) will result in the current end value (e.g. Y2) being lost. This guarantees the uniqueness of the transaction.

Fig. 4 shows the case in which the processing of the function F continues between the steps I and III under control of the clock α. Step I results in a code MAC1 and a first end value Y1, as in Fig. 3. This end value Y1 is "input" into the function F' as starting value. As stated above, the end value Y1 is the state of the function F after completion of the code MAC1, so if the function continues processing said state may be considered as start value. In Fig. 4, the function F is in step II denoted as F' as the function may not receive the input parameters R1, S1 and K.

In step III, the state (end value) of the function F' is used as start value Q2. Subsequently, MAC2 is produced using F and the input parameters R2, S2 and K.

In the example of Fig. 4, the start value Q2 is not identical to the end value Y1. However, the values Q2 and Y1 are related through the function F'. This still allows a check on the correspondence between the steps I and III.

It will be understood that the steps of Figs. 3 and 4 are carried out both in the card and in the (security module of the) terminal. That is, both the card and the terminal produce the codes MAC1 and MAC2 as shown in Fig. 3 or Fig. 4. By comparing the received code with its counterpart produced in the terminal, it is possible for the terminal to determine the authenticity of the data received and to ascertain that only a single card is involved in the transaction.

On the basis of Fig. 5, it will be further explained how the method according to the invention may be applied with commercially available payment cards.

The integrated circuit 100 schematically shown in Fig. 5, which basically corresponds to the integrated circuit 15 in the payment means 11 of Fig. 1, comprises a first memory 101 and an address register 102. The memory 101 comprises multiple memory locations,

which are addressed with the help of the address register 102, which is constructed as a counter. In response to a clock pulse α, which is generated outside the payment means, the address register 102 runs through a range of addresses. The memory 101 is constructed as a so-called EPROM or EEPROM memory and may, in response to (external) read/write signals R/W, be optionally written or read. Data, i.e., balances S1, S2 etc., are exchanged, by means of a data bus 103, with other parts of the integrated circuit 100.

A second memory 104 is constructed as a shift register having feedback. In many cases, said memory is formed by a dynamic memory, as a result of which the information stored in the memory is lost if said information is not regularly "refreshed". This point will be elaborated later. The random number R may be (temporarily) stored in an (optional) register 105. To the second memory 104 there are fed, by way of an (optional) combination circuit 106, both the random number R and a balance S from the register 105 and the memory 101, respectively. Possibly, still further parameters may be involved in the combination, such as a key K stored in the memory 101. At the (fed-back) output of the memory (shift register) 104 there originates the authentication code MAC (i.e., MAC1, MAC2, ...), which has therefore originated from the enciphered combination of the balance S, the random number R and possible other parameters, such as an identification code (e.g., a card number), a key K and the like. The feedback takes place by way of a number of modulo-2 adders and the combination circuit 106. The circuits 104, 106 and the adders connected thereto constitute the functions F and F' of Figs. 3 and 4.

In practice, the integrated circuit 100 may comprise many other parts which are not essential, however, for the present invention.

In the event of existing methods and their implementations, the problem arises that for writing data (in this case balances) to the EEPROM memory 101 there is required a relatively long write time of, e.g., at least 5 ms. During the writing, there are supplied clock and write signals to the memory (shown as the signals a and R/W). In the event of existing payment cards, it is not possible during the writing to the EEPROM memory to supply another clock pulse to other parts of the integrated circuit 100. As a result, the contents of the dynamic memory 104 is lost, since said memory must regularly and within brief

time intervals of, e.g., at least 0.1 ms, receive a clock pulse for "refreshing" the memory contents. After the writing of a balance to the EEPROM memory 101 (step II in Fig. 2), therefore, the contents of the dynamic memory 104 are lost and said memory should therefore be reset in order to achieve a defined initial state of the memory. Said reset may take place by feeding a series of zeros (or ones) to the input of the memory 104. For this purpose, the combination circuit 106 may be constructed in such a manner that on the basis of a certain control signal it issues only zeros (or ones) to its output.

Resetting the memory 104 has the drawback, however, that information which is related to the earlier steps of the method (step I in Fig. 2) is thereby lost. According to the invention, therefore, the information in the memory 104 is maintained. This is preferably achieved by having the writing of the data to the EEPROM memory 101 take place in such a manner that the refreshing of the dynamic memory 104 and possible other dynamic-memory elements, e.g., the register 105, is not disturbed. For this purpose, the frequency of the clock pulse α is always maintained at such a value that the refreshing of the dynamic memories is not endangered. Depending on the dynamic memory elements used, the clock frequency may amount to, e.g., at least 10 kHz. Since the (clock) pulse duration during the writing at such a clock frequency is too low (e.g., 0.05 ms at 10 kHz, while with a certain EEPROM memory there is required a pulse duration of at least 5 ms), the writing is carried out repeatedly. In other words, the same value (balance) is written to the same address of the memory 101 several times, until at least the total prescribed duration has been achieved. In the given example of a clock frequency of 10 kHz and a minimum write time of 5 ms, this means that a total of at least 100 times should be written to the same address.

The repeated write referred to above may be made difficult, however, by the fact that with each clock pulse in many existing payment cards the address register is raised (or lowered) by one. The actual write may therefore take place on only one of the many addresses, so that the entire address range should always be run through to write during one (relatively brief) clock pulse. As a result, the duration required for the writing is extended.

According to a further aspect of the invention, a solution for this is offered by varying the frequency of the clock α in such a

manner that, during the running through of the address register and therefore in the absence of the write signal, the frequency of the clock α is raised in order to speed up running, and immediately before or during the writing the clock frequency is lowered in order to have the write pulse continue longer. It will be understood that the clock frequency can be lowered only to the extent permitted by the required refreshing of the dynamic memory.

Also, the shape of the clock pulse may advantageously be adjusted, so that the 1/0 ratio amounts not to 50/50 but, e.g., to 70/30 or 90/10. This results in a longer write pulse (if writing takes place with a clock pulse equal to 1) and therefore in a shorter total write time without, however, disturbing the refreshing of the dynamic memory.

Adjusting the shape of the clock pulse may advantageously be combined with varying the clock frequency. In addition, the address register may advantageously be constructed in such a manner that it does not generate more different addresses than strictly necessary. By restricting the number of possible addresses, the time required for running through the address register may be effectively restricted.

As explained above, the invention is based on the fact that no authentication information is lost between the various steps of the method. For this purpose, it is ensured that dynamic registers and memories maintain their contents, even during a write to a memory requiring a relatively long write time, such as an EEPROM memory.

In practice, the method may be implemented in the form of software in the payment station, particularly in a so-called card reader of the payment station.

It will be understood by those skilled in the art that the invention is not limited to the embodiments shown, and that many modifications and amendments are possible without departing from the scope of the invention. Thus, the principle of the invention is described above on the basis of debiting a payment means, but such principle may also be applied to crediting a payment means.

THIS SHEET HAS BEEN REPLACED

13 THIS SHEET HAS BEEN REPLACED

CLAIMS

1. Method of performing a transaction using an electronic payment means (11) and a payment station (12), the method comprising the repeated execution of an interrogation step (I; III) in which the payment station (12) interrogates the payment means (11) and receives payment means data (e.g. S1; S2) in response, the payment means data comprising an authentication code (MAC1; MAC2) produced by a predetermined process (F), a subsequent authentication code (e.g. MAC2) being linked to a preceding authentication code (MAC1) of the same transaction by states of said process (F).

2. Method according to claim 1, wherein the process (F), in an interrogation step (e.g. III), uses an initial value (Q2) derived from the final state (Y1) of the process (F) in the preceding interrogation step (I).

3. Method according to claim 1 or 2, wherein the process (F) involves a key (K).

4. Method according to claim 1, 2 or 3, wherein the process (F) involves a random value (e.g. R2) produced by the payment station (12) and a payment means balance (e.g. S2).

5. Method of protectedly debiting an electronic payment means (11) using a payment station (12), the method comprising:

- a first step (I), in which:
  - the payment station (12) transfers a first random value (R1) to the payment means (11),
  - the payment means (11), in response to said first random value (R1), transfers a first authentication code (MAC1) to the payment station (12), which authentication code is determined on the basis of at least a first start value (Q1), the first random value (R1) and the current balance (S1) of the payment means (11) using a predetermined process (F), the process further producing a first end value (Y1),
- an optional second step (II), in which:
  - the payment station (12) transfers a debiting command (D) to the payment means (11), and the balance (S1) of the payment means (11) is lowered on the basis of the debiting command (D), and
- a third step (III), in which:
  - the payment means (11) transfers a second random value (R2) to the payment means (11), and the payment means, in response to

This Sheet Has Been Replaced

* C L M S *

THIS SHEET HAS BEEN REPLACED

said second random value (R2), transfers a second authentication code (MAC2) to the payment station (12), which authentication code is determined on the basis of at least a second start value (Q2), the second random value (R2) and the current balance (S2) of the payment means (11) using said process (F), the second start value (Q2) being based on the first end value (Y1).

6. Method according to claim 5, wherein the second start value (Q2) is identical to the first end value (Y1).

7. Method according to claim 5 or 6, wherein an authentication code (e.g. MAC1) is also determined on the basis of a key (K) and an identification code.

8. Method according to claim 5, 6 or 7, wherein the process (F) involves a cryptographic function.

9. Method according to claim 5, 6, 7 or 8, further comprising a fourth step (IV), in which:

- the payment station (12) records the difference (S1-S2) between the balances of the first and third steps.

10. Method according to any of the claims 5 through 9, wherein the first random value (R1) and the second random value (R2) are identical.

11. Method according to any of the claims 5 through 10, wherein the third step (III) is carried out repeatedly.

12. Method according to any of the claims 5 through 11, wherein the payment station (12) comprises a module for protectedly recording data.

13. Method according to any of the claims 5 through 12, for application with a payment means (11) which comprises an integrated circuit having a first, rewritable memory (101) for storing balances and a second, dynamic memory (104) for, as a function of a random number (R), generating an authentication code (MAC), with the writing of a balance (S) to the first memory (101) taking place with repeated write actions and such clock pulses (α) that the contents of the second, dynamic memory (104) is maintained.

14. Method according to claim 13, wherein the number of write actions per written balance amounts to between 50 and 150.

15. Method according to claim 13 or 14, wherein the frequency of the clock pulses (α) is increased between write actions.

16. Method according to claim 13, 14 or 15, wherein the clock pulses

This Sheet Has Been Replaced

(α) have an asymmetric 1/0 ratio.

17. Smart card (11) comprising an integrated circuit, the circuit comprising memory means (101) for storing a key and data to be encrypted, fed-back shift register means (104) for storing encryption data and for producing encrypted data (MAC), and logic means (106) operatively connected to the memory means (101) and the shift register means (104) for combining data from the memory means with fed-back data from the shift register means and for feeding combined data into the shift register means (104), the circuit being arranged for maintaining the contents of the shift register means.

18. Smart card according to claim 17, further comprising means for varying the clock pulse rate and the clock pulse ratio.

19. Smart card according to claim 18, further comprising a register (105) connected to the logic means (106) for storing a random value (R).

20. Financial transaction, carried out by application of the method according to any of the claims 1 through 16.

21. Payment station (12), designed for applying the method according to any of the claims 1 through 16.

PART OF THIS SHEET HAS BEEN REPLACED

This Sheet Has Been Replaced

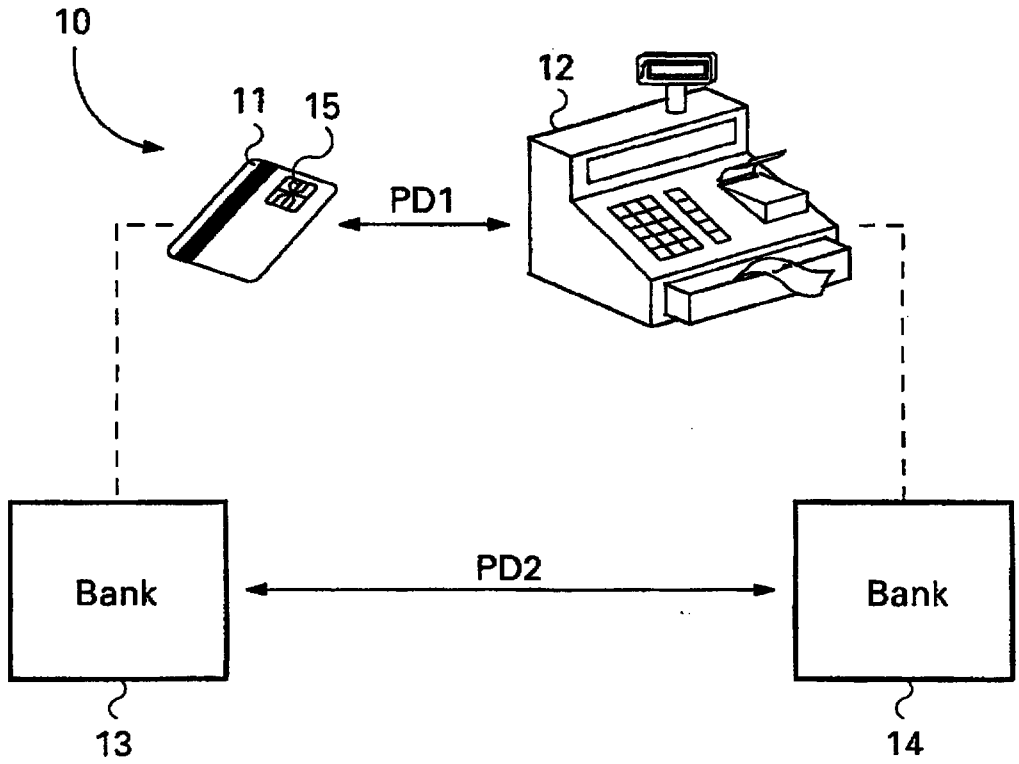


Fig.1

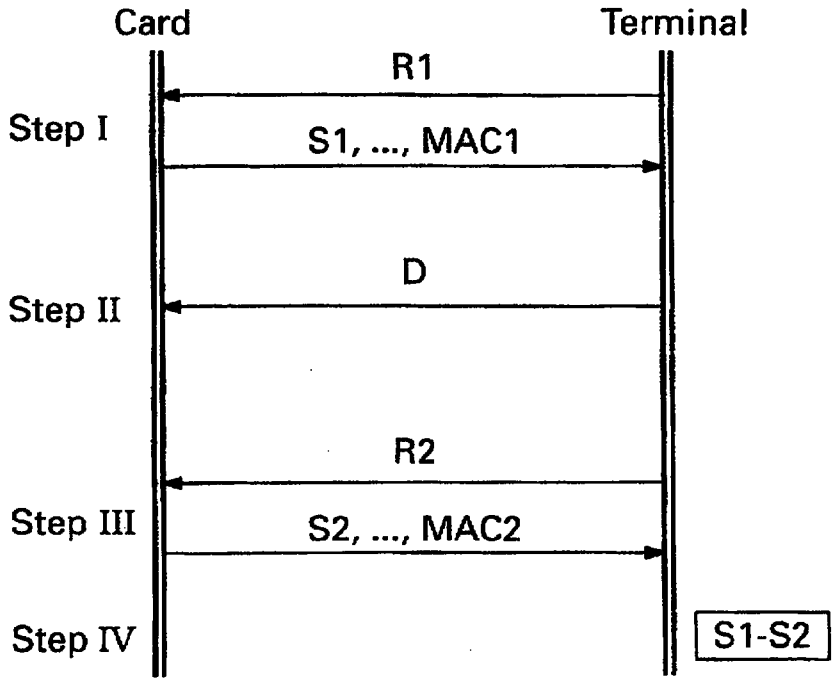

Card
Terminal
R1
Step I
S1, ..., MAC1
D
Step II
R2
Step III
S2, ..., MAC2
Step IV
S1-S2

Fig.2

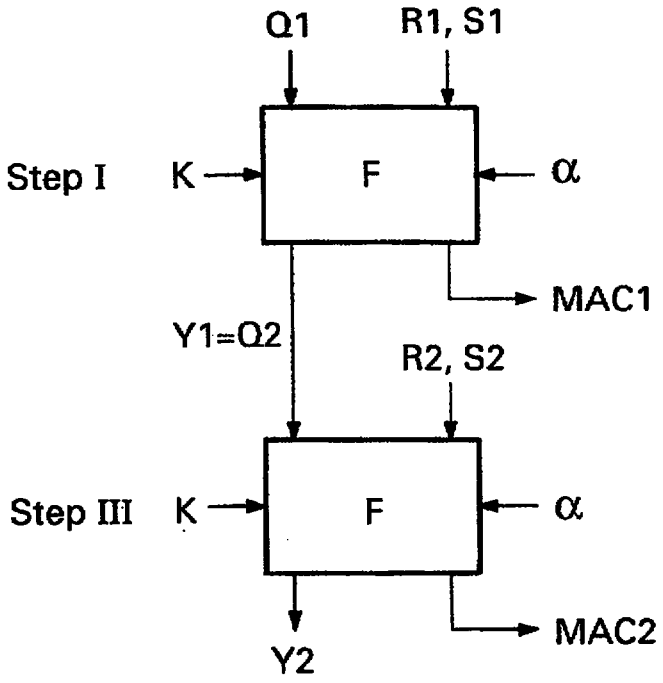


Fig. 3

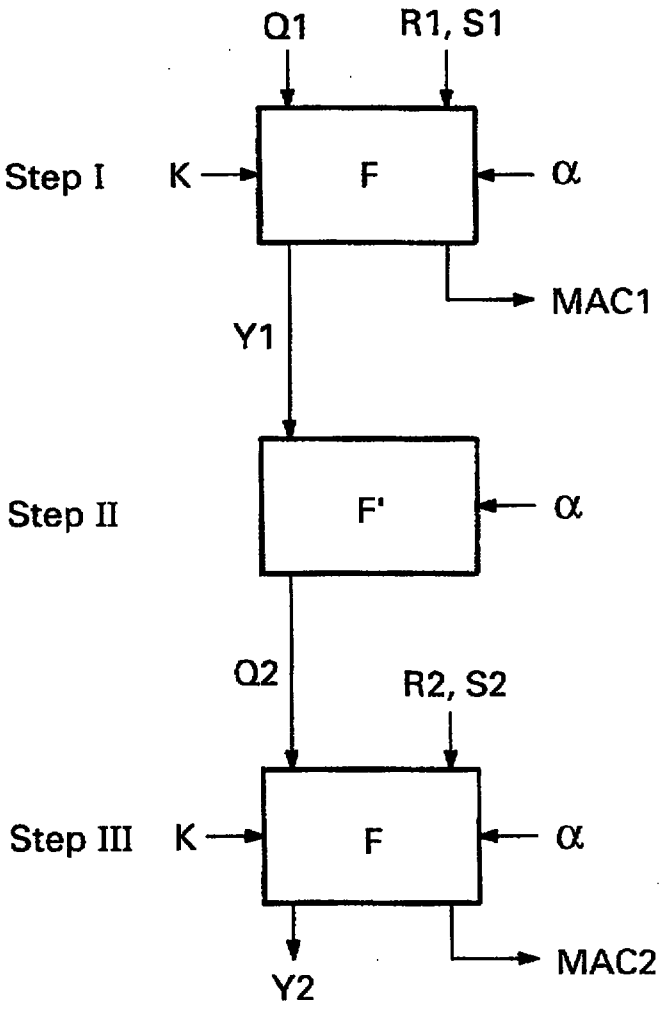

Q1
R1, S1
Step I
K
F
α
MAC1
Y1
Step II
F'
α
Q2
R2, S2
Step III
K
F
α
MAC2
Y2

Fig. 4

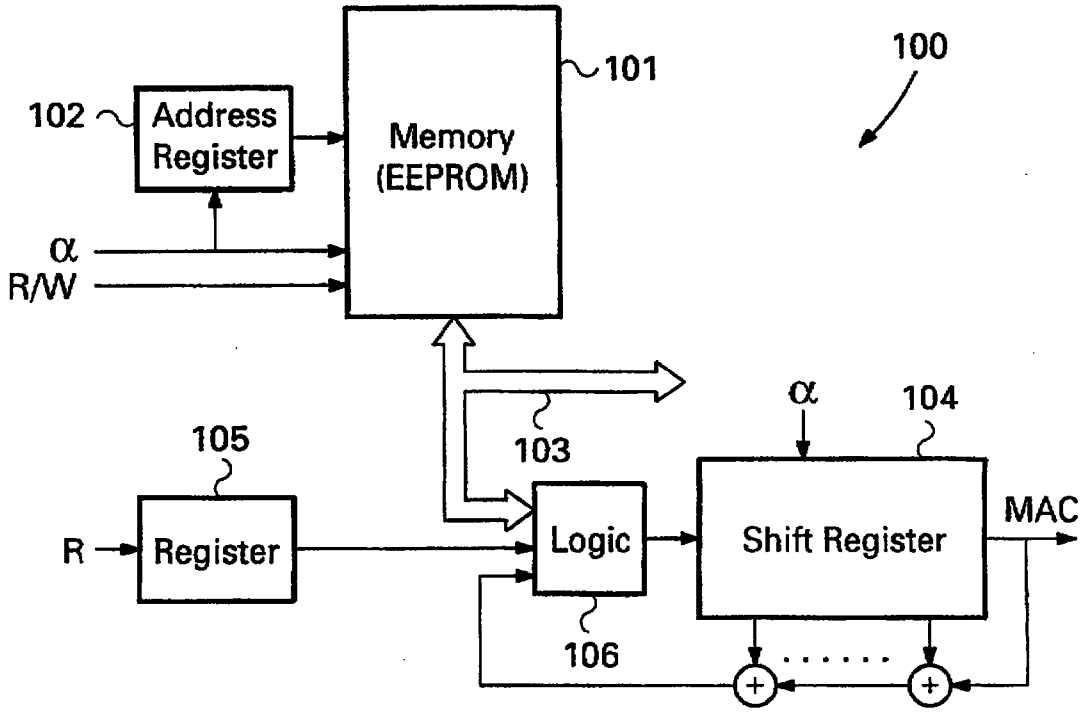

100
101
102
Address Register
Memory (EEPROM)
α
R/W
103
104
105
R
Register
Logic
Shift Register
MAC
106

Fig. 5

to a preceding authentication code of the same transaction by states of said process.

By providing a link between the authentication codes, it can be ensured that the data received by the payment station are unique to that station. In order to link the authentication codes of the different steps the process, in an interrogation step, preferably uses an initial value derived from the final state of the process in the preceding interrogation step.

More specifically, the present invention provides a method of protectedly performing a transaction using an electronic payment means and a payment station, the method comprising:

- an initial step, in which:
  - the payment station transfers a first random value to the payment means,
  - the payment means, in response to the first random value, transfers a first authentication code to the payment station, which authentication code is determined on the basis of at least a first start value, the first random value and first transaction data of the payment means using a predetermined process, the process further producing a first end value,
- a further step, in which:
  - the payment station transfers a second random value to the payment means,
  - the payment means transfers a second authentication code to the payment station, which authentication code is determined on the basis of at least a second start value, the second random value and second transaction data of the payment means using said process, the second start value being based on the first end value.

The method according to the invention is thus characterised in that the second start value is based on the first end value.

By basing the second start value on the first end value, i.e. on the state of the process after completion of the first authentication code, a direct coupling between the initial (first) step and the remaining steps is obtained and it is no longer possible to interrupt the method, or to exchange data with other payment stations, without such being noticed. Here, the second start value, which may form, e.g., the initialisation vector of a cryptographic process, may be

AMENDED SHEET

identical to the first end value or be derived from the first end value. In the first case the first end value may be stored, in the second case the second start value may be, e.g., the state of a (cryptographic) process which, starting from the first end value, has been executed a number of times. In either case, the second start value may be reproduced from the first end value, as a result of which a check on the authenticity is offered, and thereby on the continuity of the method.

The process may, in the further (third) step, produce a second end value which may be used for deriving start values for possible additional steps. The method optionally comprises an intermediate step carried out between the initial and further step, in which the payment station transfers a command to the payment means, and a balance of the payment means is changed on the basis of the command.

The invention is thus based on the insight that the application of multiple independent start values on authentications in consecutive steps of a debiting transaction under certain circumstances creates the possibility that not all steps of the transaction are carried out between the same pair of a payment means and a payment station.

The invention further provides an advantageous implementation of the said method in existing electronic payment means.

In the above reference is made to a payment station with which the payment means (card) communicates. A payment station may have an integrated storage of transaction data or a separate module. It will be understood that the payment means may in practice communicate with the protected module ("Security Module") via the payment station in case the payment station uses such a module for the secure storage of

AMENDED SHEET

CLAIMS

1. Method of protectedly performing a transaction using an electronic payment means (11) and a payment station (12), the method comprising:

- an initial step (I), in which:
  - the payment station (12) transfers a first random value (R1) to the payment means (11),
  - the payment means (11), in response to said first random value (R1), transfers a first authentication code (MAC1) to the payment station (12), which authentication code is determined on the basis of at least a first start value (Q1), a first random value (R1) and first transaction data (S1) of the payment means (11) using a predetermined process (F), the process further producing a first end value (Y1),
- a further step (III), in which:
  - the payment station (12) transfers a second random value (R2) to the payment means (11),
  - the payment means (11) transfers a second authentication code (MAC2) to the payment station (12), which authentication code is determined on the basis of at least a second start value (Q2), the second random value (R2) and second transaction data (S2) of the payment means (11) using said process (F), the second start value (Q2) being based on the first end value (Y1).

2. Method according to claim 1, wherein the second start value (Q2) is identical to the first end value (Y1).

3. Method according to claim 1 or 2, wherein an authentication code (e.g. MAC1) is also determined on the basis of a key (K) and/or an identification code.

4. Method according to claim 1, 2 or 3, comprising an optional intermediate step (II) carried out between the initial (I) and further (III) steps, in which:

- the payment station (12) transfers a command (D) to the payment means (11), and a balance of the payment means (11) is changed on the basis of the command (D).

5. Method according to any of the preceding claims, wherein the first random value (R1) and the second random value (R2) are identical, the substep of the payment station (12) transferring the second random value (R2) to the payment means (11) being omitted.

AMENDED SHEET

6. Method according to any of the preceding claims, wherein the process (F) involves a cryptographic function.

7. Method according to any of the preceding claims, further comprising a fourth step (IV), in which:

- the payment station (12) records the difference (S1-S2) between the balances of the first and third steps.

8. Method according to any of the preceding claims, wherein the third step (III) is carried out repeatedly.

9. Method according to any of the preceding claims, wherein the payment station (12) comprises a module for protectedly recording data.

10. Payment means (11) for application of the method according to any of the preceding claims, the payment means (11) comprising an integrated circuit (100) having a first, rewritable memory (101) for storing balances and a second, dynamic memory (104) for, as a function of a random number (R), generating an authentication code (MAC), the integrated circuit (100) being arranged for writing a balance (S) to the first memory (101) using repeated write actions and such clock pulses (α) that the contents of the second, dynamic memory (104) are maintained.

11. Payment means according to claim 10, wherein the number of write actions per written balance amounts to between 50 and 150.

12. Payment means according to claim 10 or 11, wherein the frequency of the clock pulses (α) is increased between write actions.

13. Payment means according to claim 10, 11 or 12, wherein the clock pulses (α) have an asymmetric 1/0 ratio.

14. Payment means according to any of claims 10-14, further comprising means for varying the clock pulse ratio.

15. Payment means according to any of claims 10-14, further comprising logic means (106) operatively connected to the first memory (101) and the second memory (104) for combining data from the first memory with fed-back data from the second memory and for feeding combined data into the second memory (104).

16. Payment means according to any of claims 10-15, further comprising a register (105) connected to the logic means (106) for storing a random value (R).

AMENDED SHEET

* NO COVER LETTER

9802756-8
IPOS copy.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F 7/10 — A1

(11) International Publication Number: WO 97/18537

(43) International Publication Date: 22 May 1997 (22.05.97)

(21) International Application Number: PCT/EP96/05028

(22) International Filing Date: 14 November 1996 (14.11.96)

(30) Priority Data:
1001659 15 November 1995 (15.11.95) NL

(71) Applicant: KONINKLIJKE PTT NEDERLAND N.V. [NL/NL]; P.O. Box 95321, NL-2509 CH The Hague (NL).

(72) Inventors: PIETERSE, Rob; Verbenalaán 7, NL-2111 ZL Aerdenhout (NL). ROMBAUT, Willem; G.A. van Beverenplein 11, NL-2552 HT The Hague (NL).

(74) Agent: BEITSMA, Gerhard, Romano; Koninklijke PTT Nederland N.V., P.O. Box 95321, NL-2509 CH The Hague (NL).

(81) Designated States: AU, BG, BR, CA, CN, CZ, EE, HU, IL, JP, KR, MX, NO, PL, RO, SG, SK, Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD OF DEBITING AN ELECTRONIC PAYMENT MEANS

(57) Abstract

The invention provides a method for protectedly debiting an electronic payment means (11), such as a telephone card. In the communication protocol between a payment means (11) and a payment station (12), an authentication is used to identify the payment means during various steps of the protocol. According to the invention, the authentications are mutually related by states (Y1, Q2) of a cryptographic process (F) in order to be capable of detecting an interference in the protocol. The method may be applied to existing payment cards having a dynamic memory, it being guaranteed that the contents of the dynamic memory, in which there is located information related to the authentication, is not lost during the protocol.

