(12) PATENT
(19) AUSTRALIAN PATENT OFFICE

(11) Application No. AU 199914379 B2
(10) Patent No. 740143

(54) Title

Method for managing data in a smart card

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

(21) Application No: 199914379

(22) Application Date: 1998.11.24

(87) WIPO No: WO99/27504

(30) Priority Data

(31) Number	(32) Date	(33) Country
97/14802	1997.11.25	FR

(43) Publication Date : 1999.06.15
(43) Publication Journal Date : 1999.08.12
(44) Accepted Journal Date : 2001.11.01

(71) Applicant(s)

Gemplus S.C.A.

(72) Inventor(s)

Gilles Lisimaque

(74) Agent/Attorney

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

(56) Related Art

US 5162638
US 5867577
WO 94/16415

14379/99

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 : G07F 7/08 — A1

(11) Numéro de publication internationale: **WO 99/27504**

(43) Date de publication internationale: 3 juin 1999 (03.06.99)

(21) Numéro de la demande internationale: PCT/FR98/02510

(22) Date de dépôt international: 24 novembre 1998 (24.11.98)

(30) Données relatives à la priorité:
97/14802 25 novembre 1997 (25.11.97) 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) Inventeur; et
(75) Inventeur/Déposant *(US seulement)*: LISIMAQUE, Gilles [US/US]; 1508 Blue Meadow Road, Potomac, MD 20854 (US).

(74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., Parc d'Activités de Gémenos, Avenue du Pic de Bertagne, F-13881 Gémenos Cedex (FR).

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

Publiée
Avec rapport de recherche internationale.

(54) Title: METHOD FOR MANAGING DATA IN A SMART CARD

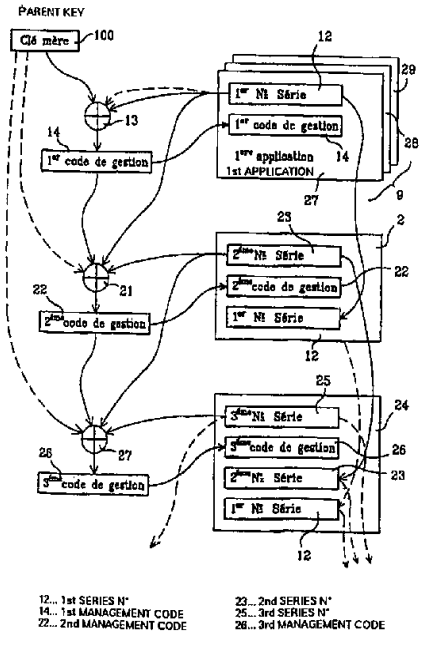
(54) Titre: PROCEDE DE GESTION DES DONNEES DANS UNE CARTE A PUCE

(57) Abstract

The invention concerns a method for duplicating data contained a smart card (9) memory in the memory of another smart card (2), which consists in producing for said other card another management code (22), another secret code. Said other management code is produced on the basis of identification data particular to the first card (12) and also particular to the second card (23). For the system to operate, identification data (12) concerning the first card are also recorded in the second card.

(57) Abrégé

Pour permettre la duplication de données contenues dans une mémoire d'une carte (9) à puce dans une autre mémoire d'une autre carte (2) à puce, on prévoit de créer pour cette autre carte à puce un autre code (22) de gestion, un autre code secret. Cet autre code de gestion est produit sur la base d'informations d'identification propres à la première (12) carte et également propres à la deuxième (23) carte. Pour que le système fonctionne, on enregistre également les informations (12) d'identification relatives à la première carte dans la deuxième carte.



PROCESS TO MANAGE DATA IN A CHIP CARD

The aim of this invention is a process to manage data stored in a chip card. The invention concerns the transfer of data from one card to another, particularly in the case where the original card is on the point of expiry and has to be replaced by a card with extended duration and also having similar system options, the same data recorded in the electronic circuit.

Thus for example electronic purses are already known in the field of chip cards, or more generally portable equipment with a computer chip. In such uses monetary units stored in the memory of a chip card are transferred to another and withdrawn from the first. There is on the face of it no limit to validity. Also in the banking sector chip cards, the card body of which is clearly embossed with the expiry date of the card, are known. This precaution of limiting the validity of the card has two objectives. On the one hand it allows the age of the electronic circuits to be taken into account and to facilitate its replacement. On the other hand it gives rise to the return of the cards in circulation to the supervisory body in such a way that this body can totally control the means which it makes available to carry out transactions.

With the exponential development of applications controlled by uses of the chip card, expired chip cards may no longer need to be replaced by a supervisory body: it ought to be possible to do this on site, if necessary with common chip card readers/recorders.

The principles of using chip cards include the requirement to compose a secret code or personal identity number (PIN) and comparison of this code with a code stored in the memory of the chip. If this comparison is successful, the application i.e. in practical terms goods or services corresponding to the transaction can be obtained, or even a payment can be effected with the card. If not the case a reject situation is indicated to the carrier. This comparison is implemented in a fail-safe manner.

The problem which occurs when the requirement is to transfer data fom one card to another is a problem of managing these secret codes or, more generally, management codes which allow management under the control of

data stored in the memory of the cards. In fact these codes stored in one form or another in the memory of the chip card are produced by the supervisory body according to data capable of identifying the card and particular to this body. As a result it is impossible to arrange the automatic extension of the validity of the cards by replacing expired cards with cards with longer memory without the intervention of this body. Indeed such an operation would amount to disclosing all the secrets concerning the formulation of the secret codes and particular to this body to all the other organisations or even all the readers capable of arranging this extension.

The present invention may alleviate this future problem by instituting a recording procedure for the management codes. The procedure may take into account the previous management codes or at least data relating to the old cards from which the data are to be recorded into the new originates.

A cryptographic algorithm may be used to produce a new management code which on the one hand takes into account identification data of the new card and on the other hand information relating to the old card. In a particular case the data relating to the old card may be the identification data of the old card. In another case the management code of the old card itself may be used. Any other data relating to the old card can be used.

At the moment of use the user can be asked to compose a secret code which corresponds to the management code of the second card. In certain cases of special verification he can also be asked to compose, in a second stage or first stage, a secret code corresponding to the management code of the first card in order to check the coherence of the formulation of the second management code.

According to one aspect of the present invention there is provided a process to manage data stored in a first memory of a first chip of a first chip card in which

- a first management code is produced with a first cryptographic algorithm based on a mother key and a first set of identification data of the first chip card,
- the first management code is recorded in the first memory,
- the first card is linked to a chip card reader,
- editing of data stored in the first memory is authorised if a secret code presented to the reader is compatible with the first management code recorded, wherein

- a second management code is produced with a second cryptographic algorithm based on data relating to the first card and a second set of identification data of a second chip card
- the data relating to the first card and the second management code is recorded in a second memory of a second chip of the second chip card

editing the data stored in the second memory is authorised if a secret code presented to the reader is compatible with the second management code recorded.

The invention will be better understood after reading the description below and after examining the figures which accompany it. The latter are only given as a guide and in no way limit the invention. The figures are detailed as follows:

- Figure 1: a diagramatic illustration of a device which can be used to implement the process of the invention;
- Figure 2: essential stages for implementing the process of the invention;
- Figure 3: preferred method to check the legality of the holding of a chip card by a carrier;
- Figure 4: diagramatic illustration of a symmetric-type algorithm enabling a management code to be found from a previous management code.

Figure 1 shows a device which can be used to implement the process of managing data according to the invention. This figure shows a reader 1 to read portable equipment 2 with a chip card or a chip card inserted in a slot 3 of the reader. This reader, in a conventional way, has a screen 4 to display messages written by the reader and a key-pad 5 to allow an operator, the carrier of the card, to arrange a transaction between reader 1 and chip card 2. In an example the reader can be linked by various means to a master system 6, either in real or delayed time. In an example these means can include a radio

link using two antennas 7 and 8 and their associated transmission/reception system, linked to the reader and master system respectively.

The invention concerns more particularly the transfer of data contained in an expired chip card 9 (its expiry date being for example 1996, already out-of-date) and a new chip card 2 with a much later expiry date (2007). Card 9 as well as card 2 each contain a computer chip, such as that referenced 10, and means of linking up with reader 1. In an example these means of linking up with the reader are quite simply a connector 11. Other solutions of linking up are known.

On Figure 2 the stages of the process of the invention are shown in a more detailed way. The old chip card 9 and the new chip card 2 are both illustrated. The chip card contains data 12 recorded in a memory of the chip, representing a serial number of the card or chip. In a banking application this serial number can also be or correspond to a bank account number.

The principle of formulating a management code consists of using a mother key 100. A mother key is thus a chain of binary characters: in an example a mother key has a length of 1024 bits. The serial number of the card or the chip can also be presented in binary form. The two chains of corresponding binary characters are then presented to a cryptographic algorithm represented symbolically by reference 13. Cryptographic algorithm 13 results in the production of a first management code. In an example cryptographic algorithm 13 is implemented by the master system, available at an issuer of the card, before this issuer decides to send the chip card to its user. In the course of a procedure known as personalisation, the issuer reads the serial number of the card with a special chip card reader and produces a first management code 14 with an algorithm 13 and a mother key 100 known by the issuer alone. The master system records the first management code 14 in the memory of the chip of the card. In a known way this can be recorded in a place of the chip of card 9. This place can also depend for its position on the application, first application 27, controllable with the card. Preferably the management codes are therefore secret and stored in places which cannot be violated.

Figure 3 shows a preferred method for using a chip card or portable equipment with a chip equipped for an application such as a management code 14. When an operator, a user, inserts his chip card into reader 1, the latter produces a random chain of bits 15. This random chain of bits 15 is sent especially by means of connector 11 to chip card 9. The latter then starts to encrypt the random chain of bits15 by the management code 14 and produces a management code 16 encrypted by the random chain of bits. At the same time the operator composes a secret code on keypad 5. This secret code is sent to reader 1. Reader 1, in the same way as card 9, produces the encryption 17 of the secret code by the value of the random chain of bits 15 which this reader knows. A comparison circuit 18 of the reader unless the latter is a comparison circuit 19 of the card, compares the management code 16 encrypted by the random chain of bits with secret code 17 encrypted by the random chain of bits. If this is identical the result of the comparison circuit 18 or 19 will be positive and the progress of the transaction planned with card 9 can continue.

Notably this progress of transactions will include editing the data stored in the first memory of the first card 9 if the secret code presented to the reader is compatible with the first management code 14 recorded.

In fact the reader will on the one hand often produce a ticket 20 representing the transaction or on the other hand in a non-obvious way make a record in its memory to represent this transaction. This record is itself intended to be transmitted to the master system in delayed mode or in real time.

Ticket 20 as well as the record will include details of the transaction, notably at least a way of identifying chip card 2, for example serial number 12 envisaged up till now, or an account number or any other information recorded in card 9. The sole fact that this information appears on ticket 20 or on the record of reader 1 signifies that it has also been edited. In practical terms an attempt is made in fact with the comparison to prevent or allow such editing and therefore the continuation of the transaction.

In the invention it has been considered that a card 9 was concerned and transferring the contents of chip 10 of this card 9 into a chip of a new card 2

was wanted. According to the invention a second management code 22 is produced with an algorithm 21, based on data relating to card 9 and a set of identification data of the second card 2.

In a particular example the information relating to the first card is rightly the serial number 12 and the information relating to the second card 9 is equally a serial number 23 of this second card. However the first management code 14 or any other information could be used as data relating to the first card.

In the invention algorithm 21 is implemented by a common-type reader 1 but equipped with software for the purpose, during a cession to produce code 22, of reading useful data in card 9, requesting extraction of card 9 and putting into place card 2 as a replacement, reading useful identification data in card 2, calculating code 22 and recording it in card 2. To simplify such production of management codes, the software for implementing the algorithm can, at least partly, be stored in card 9 (or in card 2). It can even be implemented by the micro-processor of the card for greater security.

To simplify the explanation it was considered that algorithm 21 needed to receive three chains of characters. Algorithm 13 preferably will receive the first serial number 12, a second time the first serial number 12 as well as mother key 100. In an example algorithm 21 is the same as algorithm 13. For algorithm 21 the three items of useful data can be serial number 23, serial number 12 and mother key 100. This key 100 can even be replaced by code 14. Therefore according to the invention a second management code 22 is produced with the second cryptographic algorithm 21. The second management code 22 produced in this way is then recorded in the second card 2 at the same time as the data relating to the first card (12 or 14) which has served to formulate this second management code. In the example serial number 12 of the first card 9 is also recorded in the second card 2.

Figure 2 shows again that the mechanism can be extended from the time when a third chip card 24 equipped with a third serial number 25 is used. Then it will be posible with this third card 24 to produce a third management code 26 under the same conditions with an algorithm 27 similar to algorithm 21. In this case

the data relating to the second card 2: serial number 23 will be stored in the memory of the third card 24. However it is also possible to want to store data relating to the first card 9, i.e. serial number 12 in the third card 24.

A first application 27 has been illustrated for card 9. This application is an initial way to use card 9. This card 9 according to the invention can preferaby be a multi-application card. In this case management code 14 is a management code intended for one application. For other applications 28 or 29 the same items will be found. Nevertheless while the same serial number 12 (common to the whole card or whole chip) can be used, the other management codes will benefit from being different. This can easily be achieved by using algorithms 13 programmed by different mother keys 100, depending on the applications concerned. Mother key 100 can also be stored in card 9 in the place of the memory zone reserved for applications 27, 28 or 29. Algorithm 13 is then programmed by a key 100 which depends on the application.

As soon as it is confirmed that the carrier of card 2 is a good carrier, reader 1 and chip card 2 exchange information as shown in Figure 2. In this case however the management code concerned is now code 22 relating to the second card and no longer code 14 relating to the first. The operator must therefore compose a secret code corresponding to code 22.

It is possible according to the invention to check that the second card 2 is a legitimate successor for the contents of the first card 9. This check can be made on request by having reader 1, or alternatively chip card 2, execute corresponding encryption operations, on the one hand, by algorithm 13 and on the other hand by algorithms 16 and 17. The operator must therefore compose a secret code corresponding to code 22. In other words, based on the first serial number 14 available in the second card 2, it is possible - conforming to the information given for the top of Figure 2 - to again find the first management code 14. Then, provided with this management code 14, card 2 can implement algorithm 16 from the random chain of bits. In this case the carrier can be asked to compose not the new secret code but the old secret code. In an example the request to carry out this more complex check could be requested

at random, for example on average once every hundred times. Clearly if the check fails the same consequences on the continuation of the transaction will occur.

Algorithm 21 will preferably be different from algorithm 13, although it could be the same. If it is different algorithm 21 will preferably be an algorithm known as symmetric. A symmetric algorithm 31 is shown on Figure 4. The peculiarity of a symmetric algorithm is the use of CPu public keys paired with CPt private keys.The symmetrical character of algorithm 31 then results in the fact that data 30 ciphered in symmetric algorithm 31 by mother key 32 produce encrypted data 33. If these data 33 are themselves encrypted by the same programmed algorithm 31, then by daughter key 34, then the second implementation of algorithm 31 produces source data 30. In an example it is possible to have several different CPt private daughter keys for the same CPu public mother key. Diversification of the keys involves the intervention of the serial number of the cards so that each card possesses a key, a different management code 14. It is clear that if algorithm 13 or algorithm 21 are symmetric algorithms and if data 30 are replaced by serial number 12 then the daughter key 34 itself is obtained as encrypted data.

According to the invention in addition to the data stored in the memory of card 9, a transmission attribute is associated. And editing of these data is authorised notably to allow them to be copied into the second memory, depending on the value of this attribute. If this is the case these data are copied into the second chip card 2 at the same time as this attribute. In practice this attribute gives information about a need to produce a second management code or not when the data are copied. In certain cases the mechanism implemented by algorithms 13 and 21 will be required; in other cases it will not be executed.

In another case the transmission attribute gives information about the need to control data copying by the master system. In this case when the data to be copied is edited, the attribute concerning these is read. If intervention by the master system is required, a connection to master system 6 is made. This data

copying can then take place in real or delayed time with or without the data being transmitted to the master system.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. Process to manage data stored in a first memory of a first chip of a first chip card in which
a first management code is produced with a first cryptographic algorithm based on a mother key and a first set of identification data of the first chip card,
the first management code is recorded in the first memory,
the first card is linked to a chip card reader,
editing of data stored in the first memory is authorised if a secret code presented to the reader is compatible with the first management code recorded, wherein
a second management code is produced with a second cryptographic algorithm based on data relating to the first card and a second set of identification data of a second chip card
the data relating to the first card and the second management code is recorded in a second memory of a second chip of the second chip card
editing the data stored in the second memory is authorised if a secret code presented to the reader is compatible with the second management code recorded

2. Process according to Claim 1 wherein:
the first and second management codes are secret codes.

3. Process according to Claim 1 or 2 wherein:
the second algorithm is implemented in the chip of the card.

4. Process according to one of Claims 1 to 3, wherein:
the first cryptographic algorithm is different from the second cryptographic algorithm and
the second cryptographic algorithm is symmetric.

5. Process according to one of Claims 1 to 3, wherein:
the first cryptographic algorithm is the same as the second cryptographic algorithm.

6. Process according to one of Claims 1 to 5, wherein:

the data relating to the first card is the first set of identification data of the first card or the first chip.

7. Process according to one of Claims 1 to 6, wherein:
the data relating to the first card is the first management code of the first card or the first chip.

8. Process according to one of Claims 1 to 7, wherein:
a management code word is produced in reader on the basis of the data relating to the first card and
it is checked that the card is authentic if this second management code word is compatible with a secret word.

9. Process according to one of Claims 1 to 8, wherein:
a transmission attribute is associated with the data stored in the first memory,
editing of the data is authorised so that it can be copied into the second memory depending on the value of the attribute,
the data and the attribute are copied into the second memory,
this attribute gives information about a need to produce a second secret code when copying the data.

10. Process according to Claim 9 wherein in order to authorise editing of data contained in the first memory only under the control of a master system:
a transmission attribute which gives information about a need for this control by a master system is associated,
the attribute is read prior to editing,
and an editing programme is started if the attribute having been read allows this.

11. Process according to Claim 9 or 10, wherein:
the transmission attribute forbids editing with a view to the data concerned being copied.

12. Process according to one of Claims 1 to 5, wherein:
the data is copied into the memory in delayed time.

13. Process according to one of Claims 1 to 12, wherein:

the card is a multi-application card, the data being associated with respective management codes.

14. Process for managing data stored in a chip card substantially as herein described with reference to the accompanying drawings.

DATED: 23 October 2000
PHILLIPS ORMONDE & FITZPATRICK
Attorneys for:
GEMPLUS SCA

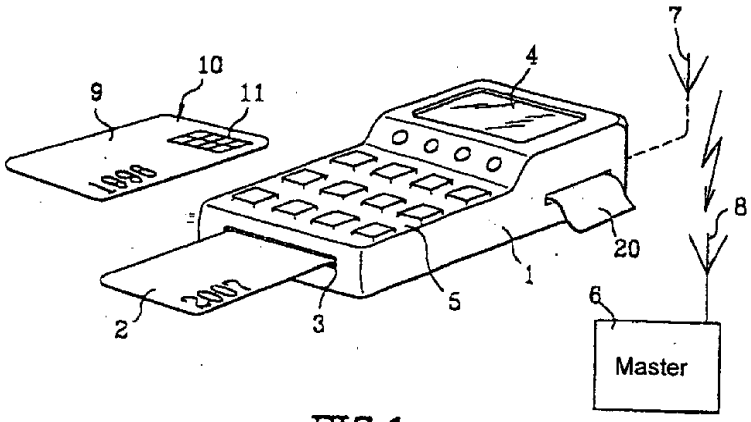

7
10
9
11
4
8
20
1
5
2
3
6
Master

FIG.1

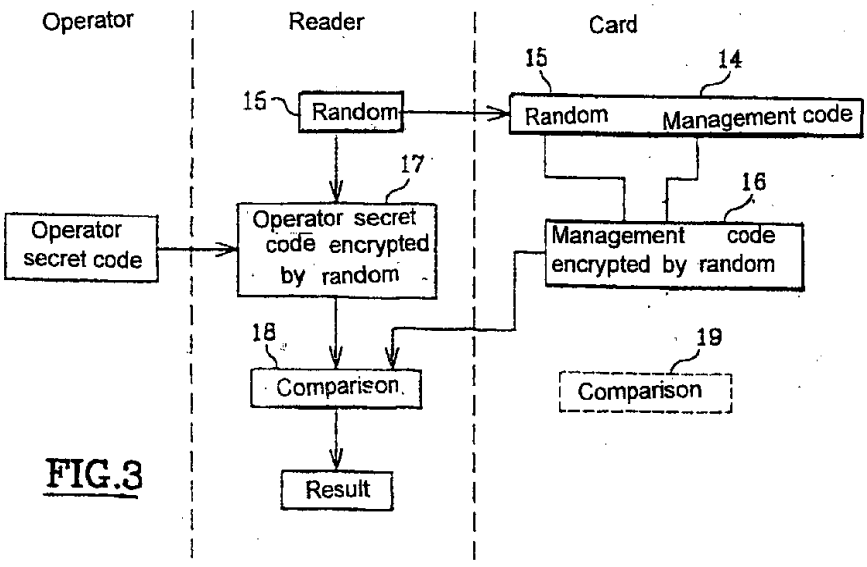

Operator
Reader
Card
15
14
15
Random
Random
Management code
17
16
Operator secret code
Operator secret code encrypted by random
Management code encrypted by random
18
19
Comparison
Comparison
Result

FIG.3

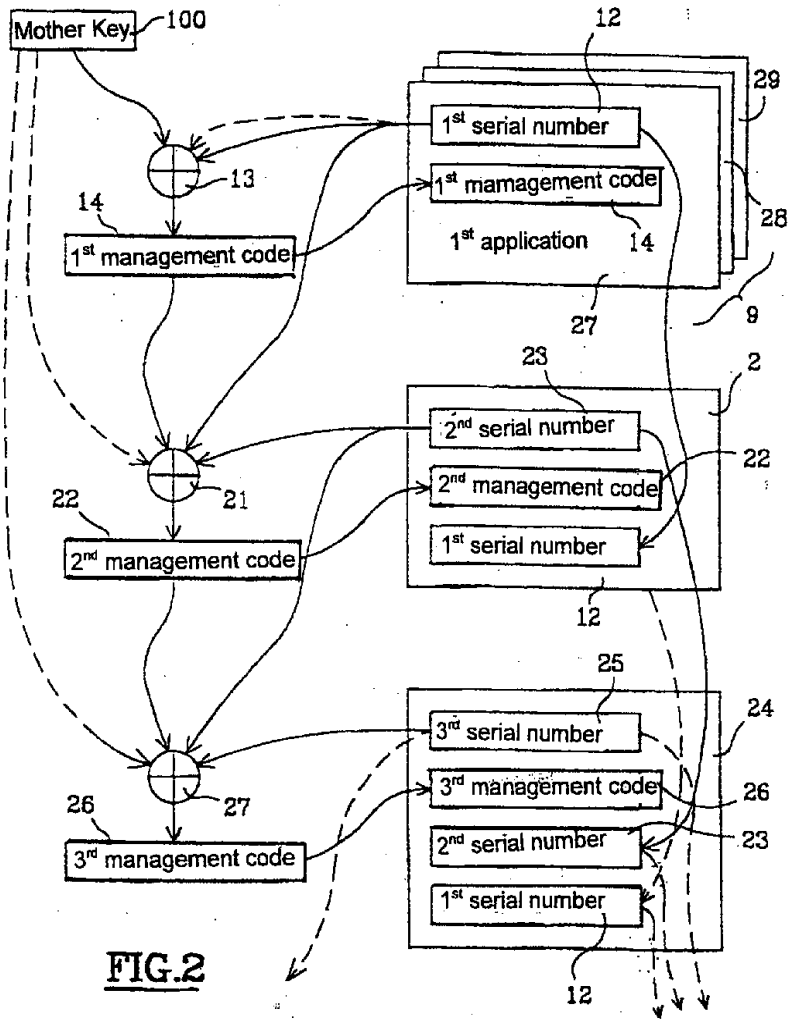

Mother Key
100
12
29
1st serial number
13
1st management code
14
1st application
14
28
27
9
23
2
2nd serial number
22
2nd management code
21
22
2nd management code
1st serial number
12
25
24
3rd serial number
3rd management code
26
27
26
3rd management code
2nd serial number
23
1st serial number
12

FIG.2

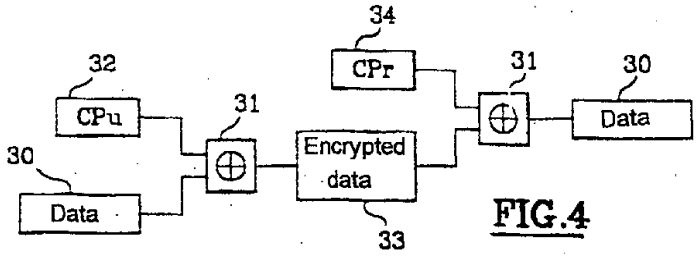

34
CPr
32
31
30
CPu
31
Data
Encrypted data
30
Data
33

FIG.4