

**EUROPEAN PATENT SPECIFICATION**

Date of publication of patent specification: **15.03.89**

Int. Cl.<sup>4</sup>: **H 04 L 9/02**, G 06 F 15/30,  
G 07 F 7/10

Application number: **84305480.0**

Date of filing: **10.08.84**

**Cryptographic key management system.**

Priority: **02.09.83 US 529161**

Date of publication of application:  
**24.04.85 Bulletin 85/17**

Publication of the grant of the patent:  
**15.03.89 Bulletin 89/11**

Designated Contracting States:  
**DE FR GB SE**

References cited:  
**EP-A-0 003 756**  
**EP-A-0 068 805**  
**WO-A-81/02655**

Proprietor: **VISA U.S.A. Inc.**  
**101 California Street**  
**San Francisco California 94111 (US)**

Inventor: **Campbell, Carl Merritt**  
**809 Malin Road**  
**Newtown Square Pennsylvania 19073 (US)**

Representative: **Jackson, David Spence et al**  
**REDDIE & GROSE 16, Theobalds Road**  
**London, WC1X 8PL (GB)**

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European patent convention).

## Description

The invention relates to a method for distributing cryptographic keys in a system having a plurality of issuing institutions and a plurality of transaction terminals and a central host, said method allowing the off-line verification of the authenticity of a financial transaction card at a terminal on the basis of authorisation information placed on the card by the issuing institution, said authorisation information being encrypted using an encrypting key.

In recent years, there has been a clear trend in society to eliminate the use of cash in financial transactions. Financial transaction cards are commonly used as a replacement for cash. These cards, which can either be credit cards or debit cards, can be used instead of cash to purchase goods or services from a merchant. Many cards can also be utilized to obtain cash or traveller's checks from financial institutions or merchants, including through the use of automatic teller machines (ATM's).

The widespread use of transaction cards has produced a concomitant increase in associated fraud. There are many types of transaction card fraud. For example, criminals have used lost or stolen cards to purchase goods or services. Criminals have also duplicated or counterfeited cards using valid account numbers.

A number of systems have been implemented in order to reduce these fraud losses. One approach is to distribute a list of lost or stolen cards to merchants. This list must be checked at the time of purchase to see if a card, which has been presented, is valid. Unfortunately, there are difficulties with this approach. For example, it takes time to distribute the bad card list after the card has been reported lost or stolen. Furthermore, card numbers remain on the list for only a certain period of time and when the numbers are removed, active fraud can resume. Finally, it is quite difficult to insure that all clerks in a merchant establishment will religiously refer to the card list.

Another approach, which overcomes many of the shortcomings of card lists, includes on-line authorization terminals. In this scenario, merchants are provided with electronic terminals that are connected to the issuer of the cards, possibly through a central processor. When a customer presents a card, information encoded on the card is read into the terminal. The terminal communicates this information over transmission lines to a host computer having information on the card holder. If the card is valid and the transaction does not exceed a specified limit, the host computer will return an approval to the merchant.

While this approach is an improvement over the use of bad card lists, it also has drawbacks. For example, counterfeit cards can be generated with valid account numbers which will not be screened by the system. In addition, because of high communication costs, not all transactions

are typically authorized. Thus, a lost or, stolen card can often be used in a remote geographical area to purchase goods.

Because of these latter shortcomings, other systems have been recently proposed to increase security. One method, which the applicant has developed, includes placing a secret, encrypted code on the card to guard against counterfeiting. Preferably, anticounterfeiting check digits are derived by encrypting the personal account number (PAN) associated with the card. These cryptographic check digits are encoded onto the magnetic stripe of the card. When the card is presented to the merchant, the information on the magnetic stripe, which includes the PAN and the check digits, is read and transmitted to the central processor. At the central processor, the transmitted PAN is encrypted in a manner similar to the generation of the cryptographic check digits. If the two results compare favorably, the card can be authorized. As can be appreciated, without knowledge of the encryption technique used to generate the check digits, the counterfeiter merely having a valid personal account number, could not generate valid check digits.

Another approach to reducing fraud losses is to require the use of personal identification numbers (PIN's). In this technique, a particular PIN is assigned to each card holder. The PIN may be either selected by the card holder or issued by the financial institution. This approach is utilized today in many banks having automatic teller machines. When a transaction is to take place, the cardholder will enter his PIN into the terminal. The PIN is transmitted, along with the account number on the card, to the central host. The central host compares the transmitted PIN with the associated PIN stored at the central location. If these numbers match, the card holder is identified as the authorized user of the card. The latter approach is effective to reduce the unauthorized use of lost or stolen credit cards.

The above techniques, however, also have certain shortcomings. These shortcomings are becoming more severe as the geographical reach of the card systems increase. More specifically, both of the above discussed security techniques require that information be transmitted from the merchant to a remote issuer. The communication costs involved in these situations is directly related to the distance between the merchant and the card issuer. Furthermore, as the number of card holders increases, the burdens on computer time also become significant. Therefore, it would be desirable to provide improved security system which can be utilized without having to incur communication costs. This goal can be met through the use of offline approval techniques.

There have been some off-line approaches suggested in the prior art. One example includes the comparison of at least a portion of a cardholder's PIN, at the terminal. In this approach, a portion of the PIN is encrypted and encoded onto the magnetic stripe of the card. The key which is used to encrypt the partial PIN values is supplied

to the transaction terminals. When the card is used in a transaction, the encrypted information is read from the magnetic stripe and compared with the PIN entered by the card holder, utilizing the secret key stored at the terminal. By this arrangement, a degree of security can be provided without incurring any communication costs. The partial PIN check can be used to authorize low value transactions. If a higher level transaction needs to be authorized, the remainder of the PIN can be verified through the communication network in an on-line manner. The offline approach can also be adapted for use with the anticounterfeiting scheme outlined above.

The basic drawback to the off-line approach suggested in the prior art is that there has been no suitable method designed for distributing the encrypting keys throughout the system. Thus, while the latter system can be implemented on a small scale, difficulties arise where there are thousands of transaction terminals and hundreds of institutions issuing cards. Obviously, the simplest answer is to use a single encrypting key for all the institutions, which is then provided to all the terminals. While the keys stored in terminals can be controlled, it is difficult to provide for key security at a large number of issuing institutions. More specifically, terminals can be safely loaded with an encrypting key during manufacture. Furthermore, these terminals can be secured to prevent tampering. However, where a large number of banks are involved, the security of the entire system would be dependent on the security of the weakest link in the group. For example, dishonest employees at one bank could conspire to uncover the key which controls the system. If the key were discovered, the entire off-line system would be compromised. Therefore, in this system, each issuing institution would be forced to rely on the security of all other issuers to guard against fraud.

To overcome the latter problem, each of the institutions could be provided with their own encrypting key. Thus, if the security at any institution were compromised, the rest of the institutions in the system could still operate. The latter approach, however, would require that each terminal be provided with the encrypting keys of each and every institution. Because of the number of institutions, this approach is deemed unfeasible as a long term solution. Therefore, it would be desirable to provide a key management system which would overcome the shortcomings described above.

An alternative, compromise approach would include supplying the terminals with a portion of the encrypting keys used by the card issuers. In this manner, some of the transactions could be approved in an off-line manner. Such a system is disclosed in EP-A- 0 003 756. In the latter system, authorisation information is encoded on each card by the card issuer. The authorisation information is enciphered under a key used by that issuer. Each of the remote terminals is provided with a partial list of the keys used by the various issuers.

In operation, the user initiates a transaction request by inserting his card into the terminal. The issuer identification number is read from the card and used to search the table in the terminal for the proper encryption key data. If the encryption key data is found, the card can be authorised off-line. If the data is not found in the table, the card data is sent to the central host which accesses the key data from a master table. This information is communicated back to the terminal.

This system has some obvious drawbacks. First, it is necessary to distribute keys from each of the issuers to the remote terminals. This process is very inefficient and requires significant storage capabilities at the local terminal. Moreover, since only a fraction of the keys are distributed, many transactions still must be authorised in an on-line manner, that, is by connection to the host which has the master table of key data.

The present invention overcomes these disadvantages by allowing the terminal to derive the encrypting key from information found on the card. This result is achieved by having the central host supply key data to the various issuers which is related to a system master key. Only the system master key is stored in the local terminals. The system master key is used by the terminals to derive the encrypting key permitting full off-line authentication.

According to the present invention a method of distributing cryptographic keys as defined hereinbefore is characterised by the steps of:

generating a system master key at the central host;

supplying the master key to each terminal;

deriving, at the central host, a secondary key for each issuing institution by encrypting data identifying the issuing institution using the master key;

supplying the secondary keys to the associated issuing institutions;

placing said data identifying the issuing institution on said cards; and

placing, by the issuing institutions, authorisation information on each said card, said authorisation information having been encrypted using the secondary key associated with the institution issuing, whereby a card can be authorised in an off-line manner at any terminal by deriving said secondary key utilizing the master key stored at the terminal to encrypt said information identifying said issuing institution placed on said card thereby permitting analysis of said encrypted authorisation information placed on said card.

The invention also provides a corresponding system which is defined in claim 11 hereinafter.

Typically, the issuing institutions are connected by communication lines to the host, and the terminals are also connected by communication lines to the host. By this arrangement, some transactions may be authorized in a typical on-line manner utilizing the communication lines. The system also permits security and fraud analysis to take place in an off-line manner.

Preferably the terminals are designed such that if someone tampers with the terminal, the master

key is erased or destroyed.

Each issuing institution will typically have some form of identification number (i.e. Bank Identification Number, BIN). The encryption key sent to the institution is derived by encrypting the BIN, associated with the bank, under the master key. For the remainder of the specification, the terms issuing institution and bank will be used interchangeably. It should be understood that the scope of the present invention includes any institution which issues financial transaction cards. When the institution issues the card, a set of data is placed on the card. Among this data is the institution's identification number (BIN). The institution also places the authorisation information on the card and, as discussed more fully hereinbelow, this authorisation information can include anticounterfeiting data, personal identification numbers or even dynamic signature information. In any case the authorisation information is placed on the card in encrypted form. Furthermore, the authorisation information is encrypted under the secondary key associated with the institution.

When a card holder initiates a transaction, the information from the card is read by the terminal. In order to authorise the transaction, the secondary key must be derived by the terminal. The secondary key is derived by utilizing the master key stored in the terminal to encrypt, in this example, the BIN placed on the card. Once the secondary key has been derived, it can be used to permit the analysis of the encrypted authorisation information placed on the card.

The methods for analyzing the encrypted information on the card will vary depending on the particular authorisation technique implemented. A number of comparison schemes are set forth in the detailed description. It is intended that the scope of the invention cover any of these comparisons schemes.

The above approach solves the shortcomings found in the prior art. More specifically, it permits off-line authorisation of transaction cards at a terminal. Furthermore, since each individual issuing institution is provided with unique encrypting keys, the compromise of any single issuer's secondary key will not affect the security of the entire system. From a commercial standpoint, it is necessary to have each individual institution responsible for its own security. This result is achieved with the key management approach of the invention. In addition, while each individual bank is given its own unique key, there is no requirement for each terminal to be provided with all of the keys. Rather, the terminal derives the necessary secondary key utilizing the master key supplied by the central host and the bank identification number. Thus, the terminal does not require large storage capacity but only needs to be provided with one secure master key.

The invention will now be described by way of example with reference to the accompanying drawings in which:

Figure 1 is a diagram of a typical electronic

funds transfer system in an interchange network.

Figure 2 is a composite flow chart illustrating the steps to implement a key management system embodying the invention.

Figure 3 is a composite flow chart illustrating the steps necessary to implement a key management system embodying the invention and incorporating an anticounterfeiting technique.

Figure 4 is a composite flow chart, similar to Figure 3, including another embodiment of an anticounterfeiting technique.

Figure 5 is a composite flow chart illustrating the key management system of the subject invention for use with the distribution of personal identification numbers (PIN's).

Figure 6 is a composite flow chart of the key management system of the subject invention showing another embodiment for use in conjunction with the distribution of PIN's.

#### Best Mode For Carrying Out The Invention

Referring to Figure 1, there is shown a typical configuration for an electronics funds transfer system. More specifically, a central host 20 is shown which acts as a network switch, routing information between a plurality of transaction terminals 22 and issuing institutions 24. The issuing institutions can be banks or other service organizations which distribute transaction cards, such as credit cards or debit cards. These cards may be used at various merchants or institutions to purchase goods or services or to obtain cash.

Each merchant is provided with one or more terminals 22. As shown at 22A, a terminal typically includes a reader for receiving information encoded on the magnetic stripe of the card. In addition, the terminal may include a PIN pad to permit a customer to enter their personal identification number (PIN). In accordance with the subject invention, the terminal will also include an encryption apparatus which may be provided in the main portion of the terminal or separately in the PIN pad. The location of the encryption apparatus will depend on the particular technique being selected.

Each of the terminals is connected to the host along communication lines 30. The host is also connected to the issuers along communications lines 32. In many transactions, information about the card holder and the purchase are transmitted from the terminal, along communication lines 30, to the host. Frequently, the central host will make the approval or denial decision. In other cases, the information is routed along lines 32, to the institution which issued the card. The authorization decision made by the institution is retransmitted to the merchant along the same communication lines.

As can be appreciated, as the use of bank cards increases in scope and geographical area, these communication costs will escalate. Therefore, it is desirable to provide some form of security through off-line analysis. In the subject specification, the term off-line is defined to mean operations which can be performed at the terminal

without any communication to the host. These objectives are achieved with the key management system of the subject invention.

Referring now to Figure 2, the general key management system of the subject invention is illustrated. This approach can be utilized to provide both an off-line anticounterfeit check and PIN verification. The flow chart is broken into three segments where Figure 2A shows the operations performed at the central host, Figure 2B shows the operations performed by the issuer and Figure 2C shows the actions taken at the terminal.

Referring to Figure 2A, the central host or control 20 initially generates a system master key 40. This master key is supplied to all of the terminals 42. Since the security of the master key is of utmost importance, this distribution should be handled in a highly secure manner. There have been a number of approaches designed in the prior art for distributing keys to terminals in a secure manner. In one approach, the terminals are physically connected to the host permitting initial loading of the master key. After this time, the terminals are kept under high security until they are installed at merchant locations. In another approach, a key loading device is connected to the host and has the master key loaded therein. The key loading device is then brought to each terminal and physically connected to load the key. In either approach, the terminal should be designed such that any tampering will erase or otherwise destroy the master key, such that it can never be extracted from the terminal.

The host then generates a plurality of secondary keys 44. These secondary keys are derived utilizing the bank identification number (BIN). As pointed out above, each institution is generally associated with a unique identification number. This identification number is encrypted using the master key. The resulting secondary keys are then distributed to the associated issuers. Again, a number of methods can be used to distribute the keys. Typically, secure encrypted communication lines are already established between the issuers and the host and therefore it is possible to transmit these keys over communication lines. The key may also be physically delivered using a key loading device as discussed above.

Referring to Figure 2B, the issuer is now capable of generating transaction cards. Initially, the issuer will place its BIN number on each card 50. Typically, this information is placed on the card by encoding the information on a magnetic stripe. While this approach is fairly common, there many other ways of encoding data on the cards, all of which are within the scope of the subject invention.

The issuer will then generate authorization information 52. As discussed below, this authorization information can be anticounterfeiting digits, PIN information or any other suitable identifier. The authorization information is then encrypted, using the secondary key supplied by the host 54. The encrypted authorization information

is then placed on the card 56 in the manner described above.

The card can now be authorized in an off-line manner at the terminals. Referring to Figure 2C, the card is initially read by the terminal at 60. The terminal will typically have a card reader capable of deciphering the encoded information on the magnetic stripe. As can be appreciated, if the information is placed on the card in another manner, the terminal should have compatible reading equipment. The information which is read includes the BIN number of the institution, as well as the encrypted authorization information.

In accordance with the subject invention, the terminal will then derive the secondary key, utilizing the master key stored at the terminal to encrypt the BIN number of the institution 62. Once the secondary key has been derived, it can be used to analyze encrypted authorization information on the card 64.

Since the encrypted information had been originally encrypted under the secondary key, the analysis can be handled in a number of ways. The particular approach will depend on the system design and a few examples will be discussed in detail hereinbelow. When the information is compared, if similarity is detected, the transaction can be authorized. If the information does not match, the transaction can be denied.

Referring now to Figure 3, a more specific approach is shown for use in an anticounterfeiting scheme. Figure 3A illustrates the actions taken at the issuer, while Figure 3B describes the events at the terminal. In Figures 3 through 6, the activities of the central host are identical with those described in Figure 2 and will not be further discussed.

In applicant's anticounterfeiting technique, the issuer will again place the BIN number on the card 70. The issuer will also generate a personal account number (PAN) which is unique for each card. This account number or (PAN) is placed on the card 72. The issuer will then encrypt the PAN with the secondary key 74. The result of this encryption is placed on the card 76. While the above discussion is limited to the use of a PAN, this number may be combined with any other information normally on the card, such as the card expiration date. Further, the entire encrypted information need not be placed on the card but only a subset thereof. By choosing only a specific subset, the information which must fit on the card can be economized.

Referring to Figure 3B, the card will be read at the terminal 80. Thus, both the BIN number and the encrypted PAN information will be received. The terminal will then derive the secondary key, utilizing the master key to encrypt the BIN 82. The secondary key is then used to encrypt the account number placed on the card at 84. The result of this encryption (or at least a portion thereof) can then be compared with the encrypted account information on the card. If these match, the transaction can be authorized.

Referring now to Figure 4, a more sophisticated

anticounterfeiting approach is shown. More specifically, in the prior art, there have been developed various secure card properties. One such property is a Watermark, manufactured by Malco Plastics. Similar in concept to water marks found on paper currency, an electronic signature can be deeply embedded in the magnetic stripe of a card. This hidden number is very difficult for counterfeiters to reproduce. Other techniques include the precise measurement of certain physical card characteristics. These technologies can be combined with the subject system to provide even further enhancement to the card.

Referring specifically to Figure 4A, the issuer will again place the BIN on the card 90. The PAN is also placed on the card 92. In addition, the secure card property, such as the Watermark is placed on the card. Because of the manufacturing sophistication necessary to implant a secure property, this step will typically be initially handled by an entity other than the issuer. The cards with the secured property placed thereon will then be supplied to the issuer. Thus, it is not intended that the order of the placement of the information on the card restrict the scope of the subject invention. The secure property, which would provide some form of numeric information, is then combined with the account number and encrypted, using a secondary key 96. The result of this encryption is then encoded on the card 98.

Referring to Figure 4B, the information on the card, including the secure property, is read by the terminal 100. The secondary key is derived, utilizing the master key to encrypt the BIN 102. The PAN and secure property are combined and are encrypted using the secondary key 104. The result of this encryption is then compared with the encrypted information encoded on the card 106. As in the previous cases, if the information matches, the transaction can be approved. However, if the information does not match, the transaction can be denied.

Referring now to Figure 5, the use of the key management system is illustrated for use with information particularly associated with the card holder, such as a PIN. The identical system can be used for any other information associated with a specific card holder, such as dynamic signature analysis information. In the latter case, the handwriting analysis information, unique to the cardholder, would be encoded in numeric form and encrypted, using the proper key. For simplicity, the remainder of discussion of Figures 5 and 6 will be restricted to the use of PINs.

Referring specifically to Figure 5A, the issuer will once again place its BIN number on the card 110. A PIN will then be generated to be associated with the customer. Frequently, the bank generates this PIN. The PIN may also be supplied to the issuer by the cardholder. The particular approach taken can be left to the discretion of the issuing institution as there are various advantages and disadvantages with both techniques. The benefits of each technique is discussed in detail in a bulletin by the American National Standards

Committee (ANSI) publication on Pin Management and Security, ANSI-X9.8 (1982). If the PIN has been generated by the institution, it must be supplied to the cardholder.

The PIN which has been selected is then encrypted using the secondary key 114. The result of this encryption is then placed on the card 116. As pointed out above, this system is probably best utilized using only a partial PIN value. For example, where four digits constitute the PIN, only two digits are encrypted and placed on the card. The remaining two digits are utilized for higher value, on-line authorization. The partial PIN digits may also be derived using the full PIN. All or only a portion of these derived digits may be placed on the card. The details of implementing a partial PIN system are known in the prior art and need not be discussed in detail.

Referring to Figure 5B, the card to be used is read by the terminal 120. As in all cases, the secondary key is derived by encrypting the BIN utilizing the master key stored at the terminal 122. The card holder will then enter his PIN. The PIN may be entered through the PIN pad of the terminal 124. The secondary key is then utilized to compare the encrypted PIN information on the card with the PIN entered by the card holder 126. This comparison may be carried out either by encrypting the PIN entered by the card holder or by decrypting the encrypted PIN on the card such that both PINs are in clear text.

The approach laid out in Figure 5 may be used to handle PIN information. Most encryption systems being implemented today utilize the Data encryption standard (DES), approved by the National Bureau of Standards. In this system, 64 bits of information are encrypted to generate 64 bits of enciphered output. If any of these bits are removed, decryption cannot take place. Because of the storage capacity of the magnetic stripe on a transaction card, it is often desirable to minimize the amount of information which needs to be encoded. A variety of techniques have been developed to achieve this result. One of the approaches is known generally as PIN offset generation. The latter approach is indicated in Figure 6 and requires less information to be encoded on the card.

Referring specifically to Figure 6A, the issuer places the BIN number on the card 130. In addition, the PAN is placed on the card 132. A PIN is generated 134 in a manner described above. In this embodiment, rather than encrypting the PIN, the PAN is encrypted 136. The resulting encryption is then combined with the PIN to define a coded value 138. There are a number of ways to combine the encrypted PAN with the PIN. In the preferred embodiment, a portion of the encrypted PAN is added to the PIN using a modulo 10 procedure. Other more sophisticated approaches may be taken. In any case, the coded value is then placed on the card 140.

Referring to Figure 6B, at the initiation of the transaction, the card is read at the terminal 150. The PIN is received from the cardholder 152. The

secondary key is then derived utilizing the master key to encrypt the BIN 154. The PAN is then encrypted under the secondary key 156. The encrypted PAN is then compared with the information placed on the card. This can conveniently be done in two ways, as shown at 158 and 160. More specifically, the encrypted PAN (or a portion thereof) is combined with the coded value and then compared with the PIN entered by the card holder. Where the original combination at 138 was by addition, the encrypted PAN is subtracted from the coded value, which should yield the PIN. Another alternative (160) is to combine the newly encrypted PAN (or a portion thereof) with the PIN entered by the card holder. This result should generate the coded value which has been placed on the card. In either case, if the comparison matches, the transaction can be authorized.

In summary, there has been provided a new and improved key management system, for use in an EFT environment, which permits off-line authorization of a transaction card. In the subject system, a central host generates a master key which is then supplied to all the terminals in the system. The host then derives a secondary key for each issuing institution by encrypting the BIN number of the issuing institution under the master key. The secondary keys are then supplied to the issuing institution.

When the institution issues a card, it places its BIN number on the card. In addition, authorization information is placed on the card in encrypted form. This information is encrypted under the secondary key associated with the institution. This information may include anticounterfeiting digits or PIN information. At the terminal, the information on the card is read. The terminal then derives the secondary key, utilizing the master key stored at the terminal to encrypt the BIN of the institution. The secondary key is then used to permit analysis of the encrypted authorization information which has been placed on the card. By this arrangement, off-line authorization can be carried out to enhance the security of the transaction card network. Furthermore, each of the issuing institutions is given a different cryptographic key, thereby further enhancing overall system security.

The disclosure has included a description of a number of different security approaches which can utilize the subject key management system. These techniques can be used alone or in combination. If used in combination, it could be beneficial to have the issuing institutions use a different secondary key for each technique. This could be accomplished in a number of ways. For example, a different master key could be generated for each technique, or the BIN could be modified in a set way before it is encrypted.

#### Claims

1. A method of distributing cryptographic keys in a system having a plurality of issuing institutions (24) and a plurality of transactions terminals

(22) and a central host (20), the method allowing the off-line verification of the authenticity of a financial transaction card at a terminal (22) on the basis of authorisation information placed on the card by the issuing institution (24), the authorisation information being encrypted using an encrypting key, characterised by the steps of:

generating a system master key at the central host (20);

supplying the master key to each terminal (22); deriving, at the central host (20), a secondary key for each issuing institution by encrypting data identifying the issuing institution using the master key;

supplying the secondary keys to the associated issuing institutions (24);

placing said data identifying the issuing institution on said cards; and

placing, by the issuing institutions (24), authorisation information on each said card, said authorisation information having been encrypted using the secondary key associated with the institution issuing, whereby a card can be authorised in an off-line manner at any terminal (22) by deriving said secondary key utilizing the master key stored at the terminal to encrypt said information identifying said issuing institution placed on said card thereby permitting analysis of said encrypted authorisation information placed on said card.

2. A method according to claim 1, characterised by the steps of:

at each said issuing institution (24):

placing unique account information on each card issued thereby, the authorisation information placed on the card being derived by encrypting the account information; and

comparing, at each terminal (22), the encrypted authorisation information and the account information placed on the presented card.

3. A method according to claim 2, characterised in that the said comparison is carried out by utilizing the secondary key derived at the terminal (22) to encrypt the account information placed on the presented card and comparing the encrypted result with the encrypted authorisation information placed on the presented card.

4. A method according to claim 2, characterised by the step of placing a secure card property on each card issued, and in that the step of deriving authorisation information includes encrypting the secure card property in combination with the account information.

5. A method according to claim 1, characterised in that the said terminals (22) are capable of accepting personal identification information entered by the cardholder, and by the steps of:

encrypting, at each issuing institution (24), the personal identification information of the respective cardholder using the secondary key associated with the issuing institution and placing at least a portion of the encrypted personal identification information on the associated card; and

comparing, at each terminal (22), the encrypted



personal identification information on the presented card with the personal identification information entered into the terminal by the cardholder.

6. A method according to claim 5, characterised in that the said comparison step is carried out by utilizing the secondary key derived at the terminal (22) to decrypt the personal identification information placed on the presented card and comparing the result with the personal identification information entered into the terminal (22) by the card holder.

7. A method according to claim 5, characterised in that the said comparison step is carried out by utilizing the secondary key derived at the terminal (22) to encrypt the personal identification information entered into the terminal (22) by a card holder and comparing the result with the encrypted personal identification information placed on the presented card.

8. A method according to claim 1, characterised in that the said terminals (22) are capable of accepting personal identification information entered by a cardholder and by the steps of:

at each said issuing institution (24):

generating and placing unique account information on each card issued thereby;

generating the authorisation information in the form of a coded message, said coded message being derived by a number of steps which includes combining the associated account information and the associated personal identification information and at least one encryption step using the secondary key;

placing said coded message on said card; and at the terminal (22):

comparing the information on the presented card and the personal identification information entered into the terminal (22) by the cardholder.

9. A method according to claim 8, characterised in that said comparison step is carried out utilizing the secondary key derived at the terminal (22) to encrypt the account information placed on the presented card and combining at least a portion of the result with the coded message placed on the presented card to permit comparison with the personal identification information entered into the terminal (22) by the card holder.

10. A method according to claim 8, characterised in that the said comparison step is carried out by utilizing the secondary key derived at the terminal (22) to encrypt the account information placed on the presented card and combining at least a portion of the result with the personal identification information entered into the terminal (22) by the card holder to permit comparison with the coded message placed on the presented card.

11. A system for distributing cryptographic keys having a plurality of issuing institutions (24) and a plurality of transaction terminals (22) and a central host (20), said system allowing the off-line verification of the authenticity of a financial transaction card at a terminal (22) on the basis of authorisation information placed on the card by

the issuing institution (24) said authorisation information being encrypted using an encrypting key, characterized by:

control means at the central host (20) for generating and supplying a system master key to each of the terminals, and for deriving a secondary key for each issuing institution by encrypting data identifying the issuing institution under the master key and supplying the secondary keys to the associated issuing institutions;

means at the issuing institutions for issuing cards, the card issuing means being capable of placing said data identifying the issuing institution on each card issued thereby, and for generating authorisation information and encrypting said authorisation information in the secondary key supplied by the control means and placing said encrypted authorisation information on said card;

means (22a) at each terminal (22) for reading the information placed on a presented card; and

means (22a) at each terminal (22) to derive said secondary key utilizing the master key stored at the terminal (22) to encrypt said data identifying the issuing institution to derive the secondary key to permit off-line analysis of said authorisation information placed on the presented card.

12. A system according to claim 11, characterised by:

means at each issuing institution (24) for generating unique account information for each card issued thereby and placing said account information on the associated card and means for encrypting the account information under the secondary key and placing at least a portion of the encrypted account information as encrypted authorisation information on the card to be issued; and

means at each terminal (22) for comparing the encrypted authorisation information and the account information placed on the presented card.

13. A system according to claim 12, characterised in that the encrypting means at each terminal (22) utilizes the secondary key derived at the terminal (22) to encrypt the account information placed on the presented card and compares at least a portion of the encrypted result with the encrypted authorisation information placed on the presented card.

14. A system according to claim 12, characterised by a means for placing a secure card property on the card to be issued, in that the encrypting means at each issuing institution (24) encrypts a combination of both the secure card property and the account information and places at least a portion of the result on the card to be issued, and in that each terminal (22) includes a means for reading the secure card property.

15. A system according to claim 12, characterised by:

means at each issuing institution (24) for generating personal identification information for each card and means for generating the authorisation information in the form of a coded



message, said coded message being derived by a number of steps including combining the account information and the personal identification information and at least one encryption step using the secondary key;

means (22a) at each terminal (22) for receiving personal identification information entered by the cardholder; and

means at each terminal (22) for comparing the information on a presented card and the personal identification information entered into the terminal (22) by the cardholder.

16. A system according to claim 15, characterised in that the encrypting means at each terminal (22) utilizes the secondary key derived at the terminal (22) to encrypt the account information placed on the presented card and combines at least a portion of the result with the coded message placed on the presented card to permit comparison with the personal identification information entered into the terminal (22) by the card holder.

17. A system according to claim 15, characterised in that the encrypting means at each terminal (22) utilizes the secondary key derived at the terminal (22) to encrypt the account information placed on the presented card and combines at least a portion of the result with the personal identification information entered into the terminal (22) by the card holder to permit comparison with the coded message on the presented card.

#### Patentansprüche

1. Verfahren zum Verteilen von Cryptographie-schlüsseln in einem System mit einer Vielzahl von Ausgabestellen (24) und einer Vielzahl von Transaktions-Endgeräten (22) und einem zentralen Wirt (20), das off-line die Verifizierung der Authentizität einer Finanztransaktionskarte an einem Endgerät (22) auf der Basis von durch die Ausgabestelle (24) auf die Karte platzierter Autorisationsinformation ermöglicht, wobei die Autorisationsinformation unter Verwendung eines Verschlüsselungs-Schlüssels verschlüsselt ist, gekennzeichnet durch folgende Schritte:

Erzeugen eines System-Hauptschlüssels am zentralen Wirt (20);

Liefern des Hauptschlüssels an jedes Endgeräte (22);

Ableiten eines Sekundärschlüssels für jede Ausgabestelle im zentralen Wirt (20) durch Verschlüsseln von Daten, die die Ausgabestelle identifizieren, unter Verwendung des Hauptschlüssels;

Liefern der Sekundärschlüssel an die angeschlossenen Ausgabestellen (24).

Plazieren der die Ausgabestelle identifizierenden Daten auf die Karten und

Plazieren von Autorisationsinformation auf jede Karte durch die Ausgabestelle (24), wobei die Autorisationsinformation unter Verwendung des Sekundärschlüssels, der mit der Ausgabestelle assoziiert ist, verschlüsselt ist, so daß eine Karte

off-line an jedem Endgerät (22) dadurch autorisiert werden kann, daß der Sekundärschlüssel abgeleitet wird, wobei der am Endgerät gespeicherte Hauptschlüssel dazu verwendet wird, die auf die Karte platzierte Information, die die Ausgabestelle identifiziert, zu verschlüsseln, womit eine Analyse der auf die Karte platzierten verschlüsselten Autorisationsinformation möglich ist.

2. Verfahren nach Anspruch 1, gekennzeichnet durch folgende Schritte:

An jeder der Ausgabestellen (24):

Plazieren eindeutiger Kontoinformation auf jede von dieser Stelle ausgegebene Karte, wobei die auf die Karte platzierte Autorisationsinformation durch Verschlüsseln der Kontoinformation abgeleitet wird; und

an jedem Endgerät (22) Vergleichen der verschlüsselten Autorisationsinformation und der auf die vorgelegte Karte platzierten Kontoinformation.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß der Vergleich durch Verwendung des Sekundärschlüssels durchgeführt wird, der am Endgerät (22) abgeleitet wird, um die Kontoinformation zu verschlüsseln, die auf die vorgelegte Karte platziert ist, und Vergleichen des verschlüsselten Resultates mit der verschlüsselten Autorisationsinformation, die auf die vorgelegte Karte platziert ist.

4. Verfahren nach Anspruch 2, gekennzeichnet durch den Schritt, daß eine Sicherheits-Karteneigenart auf jede ausgegebene Karte platziert wird, und daß der Schritt der Ableitung von Autorisationsinformation eine Verschlüsselung der Sicherheits-Karteneigenart in Kombination mit der Kontoinformation einschließt.

5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Endgeräte (22) fähig sind, vom Kartenhalter eingegebene persönliche Identifikations-Information zu akzeptieren, und durch folgende Schritte:

Verschlüsseln in jeder Ausgabestelle (24) die persönliche Identifikations-Information des betreffenden Kartenhalters unter Verwendung des Sekundärschlüssels, der mit der Ausgabestelle assoziiert ist, und Plazieren wenigstens eines Teils der verschlüsselten persönlichen Identifikations-Information auf die assoziierte Karte; und

Vergleichen, an jedem Endgerät (22), der verschlüsselten persönlichen Identifikations-Information auf der vorgelegten Karte mit der persönlichen Identifikations-Information, die vom Kartenhalter in das Endgerät eingegeben ist.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß der Vergleich dadurch durchgeführt wird, daß der am Endgerät (22) abgeleitete Sekundärschlüssel dazu verwendet wird, die persönliche Identifikations-Information, die auf die vorgelegte Karte platziert ist, zu entschlüsseln, und Vergleichen des Resultates mit der persönlichen Identifikations-Information, die vom Kartenhalter in das Endgerät (22) eingegeben ist.

7. Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß der Vergleich dadurch durchgeführt

wird, daß der am Endgerät (22) abgeleitete Sekundärschlüssel dazu verwendet wird, die persönliche Identifikations-Information, die vom Kartenhalter in das Endgerät (22) eingegeben ist, zu verschlüsseln, und Vergleichen des Resultates mit der persönlichen Identifikations-Information, die auf die vorgelegte Karte plaziert ist.

8. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Endgeräte (22) fähig sind, vom Kartenhalter eingegebene persönliche Identifikations-Information zu akzeptieren, und durch folgende Schritte:

An jeder der Ausgabestellen (24):

Erzeugen und Plazieren eindeutiger Kontoinformation auf jeder von dieser Stelle ausgegebene Karte;

Erzeugen der Autorisationsinformation in Form einer kodierten Nachricht, wobei die kodierte Nachricht durch eine Anzahl von Schritten abgeleitet wird, die die Kombination der assoziierten Kontoinformation und der assoziierten persönlichen Identifikations-Information und wenigstens einen Verschlüsselungsschritt unter Verwendung des Sekundärschlüssels einschließen;

Plazieren der kodierten Nachricht auf der Karte; und

am Endgerät (22):

Vergleichen der Information auf der vorgelegten Karte und der Persönlichen Identifikations-Information, die vom Kartenhalter in das Endgerät (22) eingegeben ist.

9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, daß der Vergleich dadurch durchgeführt wird, daß der am Endgerät (22) abgeleitete Sekundärschlüssel dazu verwendet wird, die Kontoinformation, die auf die vorgelegte Karte plaziert ist, zu verschlüsseln, und Kombinieren wenigstens eines Teils des Resultates mit der kodierten Nachricht, die auf die vorgelegte Karte plaziert ist, um einen Vergleich mit der persönlichen Identifikations-Information, die vom Kartenhalter in das Endgerät (22) eingegeben ist, zu ermöglichen.

10. Verfahren nach Anspruch 8, dadurch gekennzeichnet, daß der Vergleich dadurch durchgeführt wird, daß der am Endgerät (22) abgeleitete Sekundärschlüssel dazu verwendet wird, die Kontoinformation, die auf die vorgelegte Karte plaziert ist, zu verschlüsseln, und Kombinieren wenigstens eines Teils des Resultates mit der persönlichen Identifikations-Information, die vom Kartenhalter in das Endgerät (22) eingegeben ist, um einen Vergleich mit der kodierten Nachricht, die auf die vorgelegte Karte plaziert ist, zu ermöglichen.

11. System zum Verteilen von Cryptographieschlüsseln mit einer Vielzahl von Ausgabestellen (24) und einer Vielzahl von Transaktionsendgeräten (22) und einem zentralen Wirt (22), das die offlin-Verifizierung der Authentizität einer Finanz-Transaktions-Karte an einem Endgerät (22) auf der Basis von von der Ausgabestelle (24) auf die Karte platzierter Autorisationsinformation erlaubt, wobei die Autorisationsinformation unter Verwendung eines Cryptographieschlüssels verschlüsselt ist, gekennzeichnet durch

Kontrollmittel am zentralen Wirt (20) zum Erzeu-

gen und Liefern eines System-Hauptschlüssels an jedes der Endgeräte, und zum Ableiten eines Sekundärschlüssels für jede Ausgabestelle durch Verschlüsseln von die Ausgabestelle identifizierenden Daten unter dem Hauptschlüssel und Liefern der Sekundärschlüssel an die assoziierten Ausgabestellen;

Mitteln an den Ausgabestellen zur Ausgabe von Karten, die in der Lage sind, die Ausgabestelle identifizierende Daten auf jede von dieser Stelle ausgegebene Karte zu plazieren, und zum Erzeugen von Autorisationsinformation und Verschlüsseln dieser Autorisationsinformation mit dem Sekundärschlüssel, der von den Kontrollmitteln geliefert ist, und Plazieren der verschlüsselten Autorisationsinformation auf die Karte;

Mitteln (22a) an jedem Endgerät (22) zum Lesen der auf eine vorgelegte Karte plazierten Information; und

Mitteln (22a) an jedem Endgerät (22) zum Ableiten des Sekundärschlüssels unter Verwendung des im Endgerät (22) gespeicherten Hauptschlüssels, um die die Ausgabestelle identifizierenden Daten zu verschlüsseln, um den Sekundärschlüssel abzuleiten, um eine off-line-Analyse der auf die vorgelegte Karte plazierten Autorisationsinformation zu erlauben.

12. System nach Anspruch 11, gekennzeichnet durch

Mitteln an jeder Ausgabestelle (24) zum Erzeugen von eindeutiger Kontoinformation für jede ausgegebene Karte und Plazieren der Kontoinformation auf die assoziierte Karte und Mitteln zum Verschlüsseln der Kontoinformation unter dem Sekundärschlüssel und Plazieren wenigstens eines Teils der verschlüsselten Kontoinformation als verschlüsselte Autorisationsinformation auf die auszugebene Karte; und

Mitteln an jedem Endgerät (22) zum Vergleich der verschlüsselten Autorisationsinformation und der auf die vorgelegte Karte plazierten Kontoinformation.

13. System nach Anspruch 12, dadurch gekennzeichnet, daß das Verschlüsselungsmittel an jedem Endgerät (22) den Sekundärschlüssel verwendet, der am Endgerät (22) abgeleitet ist, um die Kontoinformation zu verschlüsseln, die auf die vorgelegte Karte plaziert ist, und wenigstens einen Teil des verschlüsselten Resultats mit der verschlüsselten Autorisationsinformation vergleicht, die auf die vorgelegte Karte plaziert ist.

14. System nach Anspruch 12, gekennzeichnet durch ein Mittel zum Plazieren einer Sicherheits-Karteneigenart auf die auszugebene Karte, sowie dadurch, daß das Verschlüsselungsmittel an jeder Ausgabestelle (24) eine Kombination der Sicherheits-Karteneigenart und der Kontoinformation verschlüsselt und wenigstens einen Teil des Resultates auf die auszugebene Karte plaziert, und daß jedes Endgerät (22) ein Mittel zum Lesen der Sicherheits-Karteneigenart aufweist.

15. System nach Anspruch 12, gekennzeichnet durch

Mittel an jeder Ausgabestelle (24) zum Erzeugen von persönlicher Identifikationsinformation für

jede Karte und Mittel zum Erzeugen der Autorisationsinformation in Form einer kodierten Nachricht, wobei die kodierte Nachricht durch eine Anzahl von Schritten abgeleitet wird, einschließlich Kombination der Kontoinformation und der persönlichen Identifikationsinformation und wenigstens einen Verschlüsselungsschritt unter Verwendung des Sekundärschlüssels;

Mittel (22a) an jedem Endgerät (22) zum Empfang von persönlicher Identifikationsinformation, die vom Kartenhalter eingegeben wird; und

Mitteln an jedem Endgerät (22) zum Vergleich der Information auf einer vorgelegten Karte und der persönlichen Identifikationsinformation, die vom Kartenhalter in das Endgerät (22) eingegeben ist.

16. System nach Anspruch 15, dadurch gekennzeichnet, daß das Verschlüsselungsmittel an jedem Endgerät (22) den Sekundärschlüssel verwendet, der am Endgerät (22) abgeleitet ist, um die Kontoinformation zu verschlüsseln, die auf die vorgelegte Karte plaziert ist, und wenigstens einen Teil des Resultates mit der kodierten Nachricht kombiniert, die auf die vorgelegte Karte plaziert ist, um einen Vergleich mit der persönlichen Identifikationsinformation zu erlauben, die vom Kartenhalter in das Endgerät (22) eingegeben ist.

17. System nach Anspruch 15, dadurch gekennzeichnet, daß das Verschlüsselungsmittel an jedem Endgerät (22) den am Endgerät (22) abgeleiteten Sekundärschlüssel dazu benutzt, die Kontoinformation zu verschlüsseln, die auf die vorgelegte Karte plaziert ist, und wenigstens einen Teil des Resultates mit der persönlichen Identifikationsinformation kombiniert, die vom Kartenhalter in das Endgerät (22) eingegeben ist, um einen Vergleich mit der kodierten Nachricht auf der vorgelegten Karte zu erlauben.

## Revendications

1. Procédé de distribution de clés cryptographiques dans un système ayant plusieurs établissements émetteurs (24) et plusieurs terminaux de transactions (22) et un hôte central (20), le procédé permettant la vérification indépendante de l'authenticité d'une carte de transactions financières au niveau d'un terminal (22) d'après une information d'autorisation placée sur la carte par l'établissement émetteur (24), l'information d'autorisation étant chiffrée à l'aide d'une clé de chiffrement, caractérisé par les étapes suivantes:

la création d'une clé maîtresse du système au niveau de l'hôte central (20),

la transmission de la clé maîtresse à chaque terminal (22),

la dérivation, au niveau de l'hôte central (20), d'une clé secondaire pour chaque établissement émetteur par chiffrement de données identifiant l'établissement émetteur à l'aide de la clé maîtresse,

la transmission des clés secondaires aux établissements émetteurs associés (24),

la disposition de données d'identification de l'établissement émetteur sur les cartes, et

la disposition, par les établissements émetteurs (24), d'une information d'autorisation sur chaque carte, l'information d'autorisation ayant été chiffrée avec le clé secondaire associée à l'établissement émetteur, si bien qu'une carte peut être autorisée de manière indépendante au niveau d'un terminal quelconque (22) par dérivation de la clé secondaire à l'aide de la clé maîtresse mémorisée au niveau du terminal afin que l'information identifiant l'établissement émetteur, placée sur la carte, soit chiffrée et permette l'analyse de l'information chiffrée d'autorisation placée sur la carte.

2. Procédé selon la revendication 1, caractérisé par les étapes suivantes:

à chaque établissement émetteur (24):

la disposition d'une information originale de compte sur chaque carte délivrée, l'information d'autorisation placée sur la carte étant dérivée par chiffrement de l'information de compte, et

la comparaison, à chaque terminal (22) de l'information chiffrée d'autorisation et de l'information de compte placée sur la carte présentée.

3. Procédé selon la revendication 2, caractérisé en ce que ladite comparaison est exécutée par utilisation de la clé secondaire dérivée au niveau du terminal (22) pour le chiffrement de l'information de compte placée sur la carte présentée, et par comparaison du résultat chiffré à l'information chiffrée d'autorisation placée sur la carte présentée.

4. Procédé selon la revendication 2, caractérisé par l'étape de disposition d'une propriété de sécurité de carte sur chaque carte délivrée, et en ce que l'étape de dérivation de l'information d'autorisation comprend le chiffrement de la propriété de sécurité de carte en combinaison avec l'information relative au compte.

5. Procédé selon la revendication 1, caractérisé en ce que les terminaux (22) peuvent accepter l'information d'identification personnelle introduite par le porteur de carte, et par les étapes suivantes:

le chiffrement, à chaque établissement émetteur (24), de l'information d'identification personnelle du porteur respectif de carte à l'aide de la clé secondaire associée à l'établissement émetteur et la disposition d'une partie au moins de l'information chiffrée d'identification personnelle sur la carte associée, et

la comparaison, à chaque terminal (22), de l'information chiffrée d'identification personnelle portée par la carte présentée à l'information d'identification personnelle saisie dans le terminal par le porteur de carte.

6. Procédé selon la revendication 5, caractérisé en ce que l'étape de comparaison est exécutée par utilisation de la clé secondaire dérivée au niveau du terminal (22) pour le déchiffrement de l'information d'identification personnelle placée sur la carte présentée, et par comparaison du résultat à l'information d'identification personnelle saisie dans le terminal (22) par le porteur de carte.

7. Procédé selon la revendication 5, caractérisé en ce que l'étape de comparaison est exécutée par utilisation de la clé secondaire dérivée au niveau

du terminal (22) pour le chiffrement de l'information d'identification personnelle saisie dans le terminal (22) par un porteur de carte, et par comparaison du résultat à l'information chiffrée d'identification personnelle placée sur la carte présentée.

8. Procédé selon la revendication 1, caractérisé en ce que les terminaux (22) sont capables d'accepter une information d'identification personnelle saisie par un porteur de carte, et par les étapes suivantes:

a chaque établissement émetteur (24):

la création et la disposition d'une information originale de compte sur chaque carte émise par cet établissement,

la création de l'information d'autorisation sous forme d'un message codé, le message codé étant dérivé au cours d'un certain nombre d'étapes qui comprennent la combinaison de l'information de compte associée et de l'information d'identification personnelle associée et d'au moins une étape de chiffrement utilisant la clé secondaire,

la disposition du message codé sur la carte, et au niveau du terminal (22):

la comparaison de l'information portée par la carte présentée et de l'information d'identification personnelle saisie dans le terminal (22) par le porteur de carte.

9. Procédé selon la revendication 8, caractérisé en ce que l'étape de comparaison est exécutée à l'aide de la clé secondaire dérivée au niveau du terminal (22) pour le chiffrement de l'information de compte placée sur la carte présentée et par combinaison d'une partie au moins du résultat au message codé placé sur la carte présentée afin que la comparaison avec l'information d'identification personnelle saisie dans le terminal (22) par le porteur de carte soit possible.

10. Procédé selon la revendication 8, caractérisé en ce que l'étape de comparaison est exécutée par utilisation de la clé secondaire dérivée au niveau du terminal (22) pour le chiffrement de l'information de compte placée sur la carte présentée, et par combinaison d'une partie au moins du résultat à l'information d'identification personnelle saisie dans le terminal (22) par le porteur de carte afin que la comparaison avec le message codé placé sur la carte présentée soit possible.

11. Système de distribution de clés cryptographiques ayant plusieurs établissements émetteurs (24) et plusieurs terminaux de transactions (22) et un hôte central (20), le système permettant la vérification indépendante de l'authenticité d'une carte de transactions financières à un terminal (22) d'après une information d'autorisation placée sur la carte par l'établissement émetteur (24), l'information d'autorisation étant chiffrée à l'aide d'une clé de chiffrement, caractérisé par:

un dispositif de commande placé au niveau de l'hôte central (20) et destiné à créer et fournir une clé principale du système à chacun des terminaux, et à dériver une clé secondaire pour chaque établissement émetteur par chiffrement de données identifiant l'établissement émetteur avec la clé maîtresse, et à transmettre les clés

secondaires aux établissements émetteurs associés,

un dispositif, placé au niveau des établissements émetteurs, et destiné à émettre des cartes, le dispositif d'émission de cartes pouvant placer les données identifiant l'établissement émetteur sur chaque carte qu'il délivre, et étant destiné à créer une information d'autorisation et à chiffrer l'information d'autorisation avec la clé secondaire transmise par le dispositif de commande, et à placer l'information chiffrée d'autorisation sur la carte,

un dispositif (22a) placé à chaque terminal (22) et destiné à lire l'information placée sur une carte présentée, et

un dispositif (22a) placé à chaque terminal (22) et destiné à dériver la clé secondaire à l'aide de la clé maîtresse conservée au niveau du terminal (22) pour le chiffrement des données identifiant l'établissement émetteur afin qu'il dérive la clé secondaire et permette l'analyse indépendante de l'information d'autorisation placée sur la carte présentée.

12. Système selon la revendication 11, caractérisé par:

un dispositif, placé à chaque établissement émetteur (24) et destiné à créer une information originale de compte sur chaque carte qu'il émet, et à placer l'information de compte sur la carte associée, et un dispositif de chiffrement de l'information de compte, à l'aide de la clé secondaire, et de disposition d'une partie au moins de l'information chiffrée de compte sous forme d'une information chiffrée d'autorisation sur la carte à délivrer, et

un dispositif, placé à chaque terminal (22) et destiné à comparer l'information chiffrée d'autorisation et l'information de compte placée sur la carte présentée.

13. Système selon la revendication 12, caractérisé en ce que le dispositif de chiffrement placé à chaque terminal (22) utilise la clé secondaire dérivée au terminal (22) pour le chiffrement de l'information de compte placée sur la carte présentée et compare une partie au moins du résultat chiffré à l'information chiffrée d'autorisation placée sur la carte présentée.

14. Système selon la revendication 12, caractérisé par un dispositif destiné à placer une propriété de sécurité de carte sur la carte à émettre, en ce que le dispositif de chiffrement de chaque établissement émetteur (24) chiffre une combinaison de la propriété de sécurité de la carte et de l'information de compte et place une partie au moins du résultat sur la carte à délivrer, et en ce que chaque terminal (22) comporte un dispositif de lecture de la propriété de sécurité de la carte.

15. Système selon la revendication 12, caractérisé par:

un dispositif placé à chaque établissement émetteur (24) et destiné à créer une information d'identification personnelle pour chaque carte, et un dispositif destiné à créer l'information d'autorisation sous forme d'un message codé, le mes-

sage codé étant dérivé au cours d'un certain nombre d'étapes comprenant la combinaison de l'information de compte et de l'information d'identification personnelle et au moins une étape de chiffrement mettant en oeuvre la clé secondaire,

un dispositif (22a) placé à chaque terminal (22) et destiné à recevoir l'information d'identification personnelle saisie par le porteur de carte, et

un dispositif placé à chaque terminal (22) et destiné à comparer l'information portée par une carte présentée et l'information d'identification personnelle saisie dans le terminal (22) par le porteur de carte.

16. Système selon la revendication 15, caractérisé en ce que le dispositif de chiffrement placé à chaque terminal (22) utilise la clé secondaire

dérivée au terminal (22) pour le chiffrement de l'information de compte placée sur la carte présentée et combine une partie au moins du résultat au message codé placé sur la carte présentée afin qu'il permette la comparaison à l'information d'identification personnelle saisie dans le terminal (22) par le porteur de carte.

17. Système selon la revendication 15, caractérisé en ce que le dispositif de chiffrement placé à chaque terminal (22) utilise la clé secondaire dérivée au terminal (22) pour le chiffrement de l'information de compte placée sur la carte présentée et combine une partie au moins du résultat à l'information d'identification personnelle saisie dans le terminal (22) par le porteur de carte afin qu'elle puisse être comparée au message codé porté par la carte présentée.

20

25

30

35

40

45

50

55

60

65

13

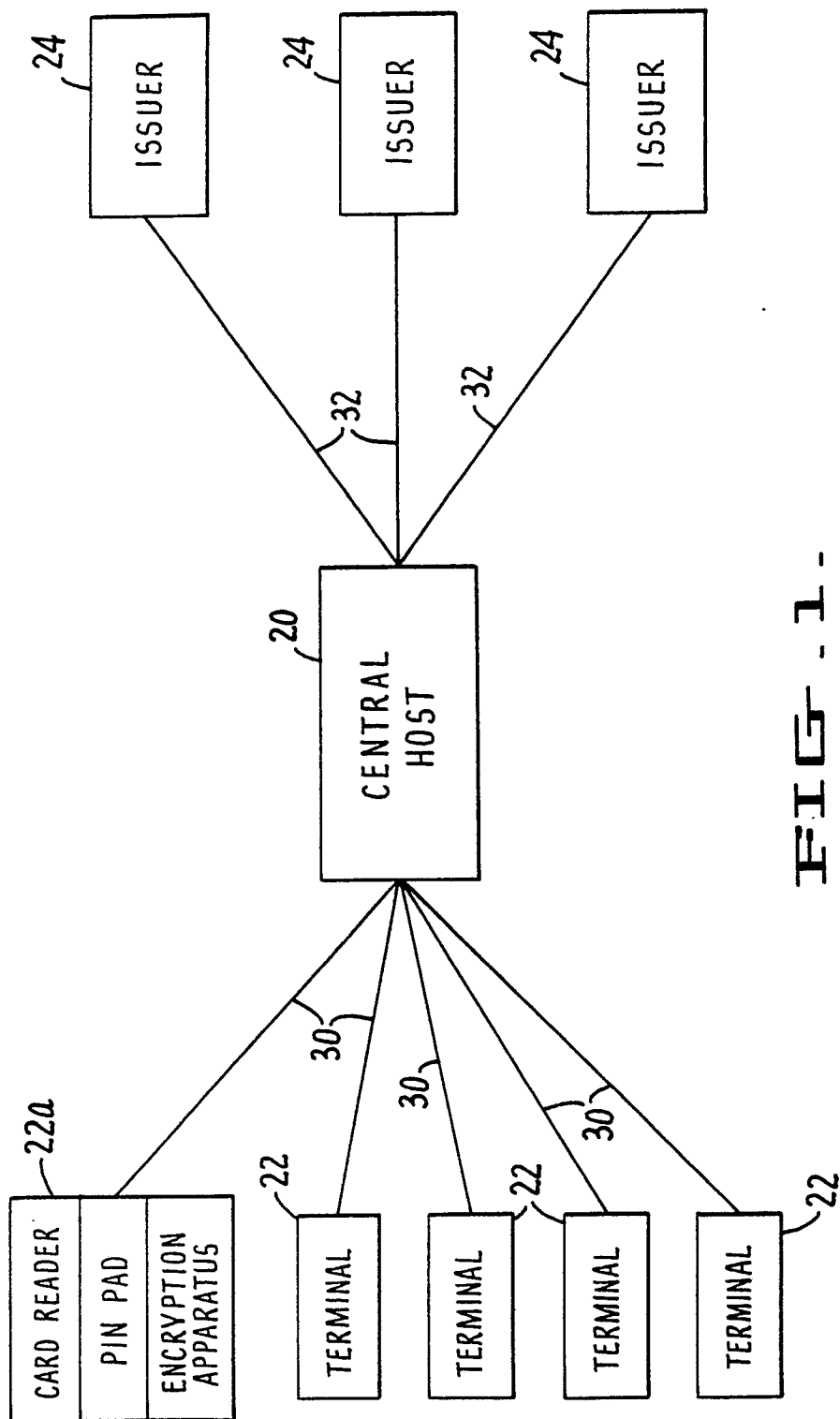
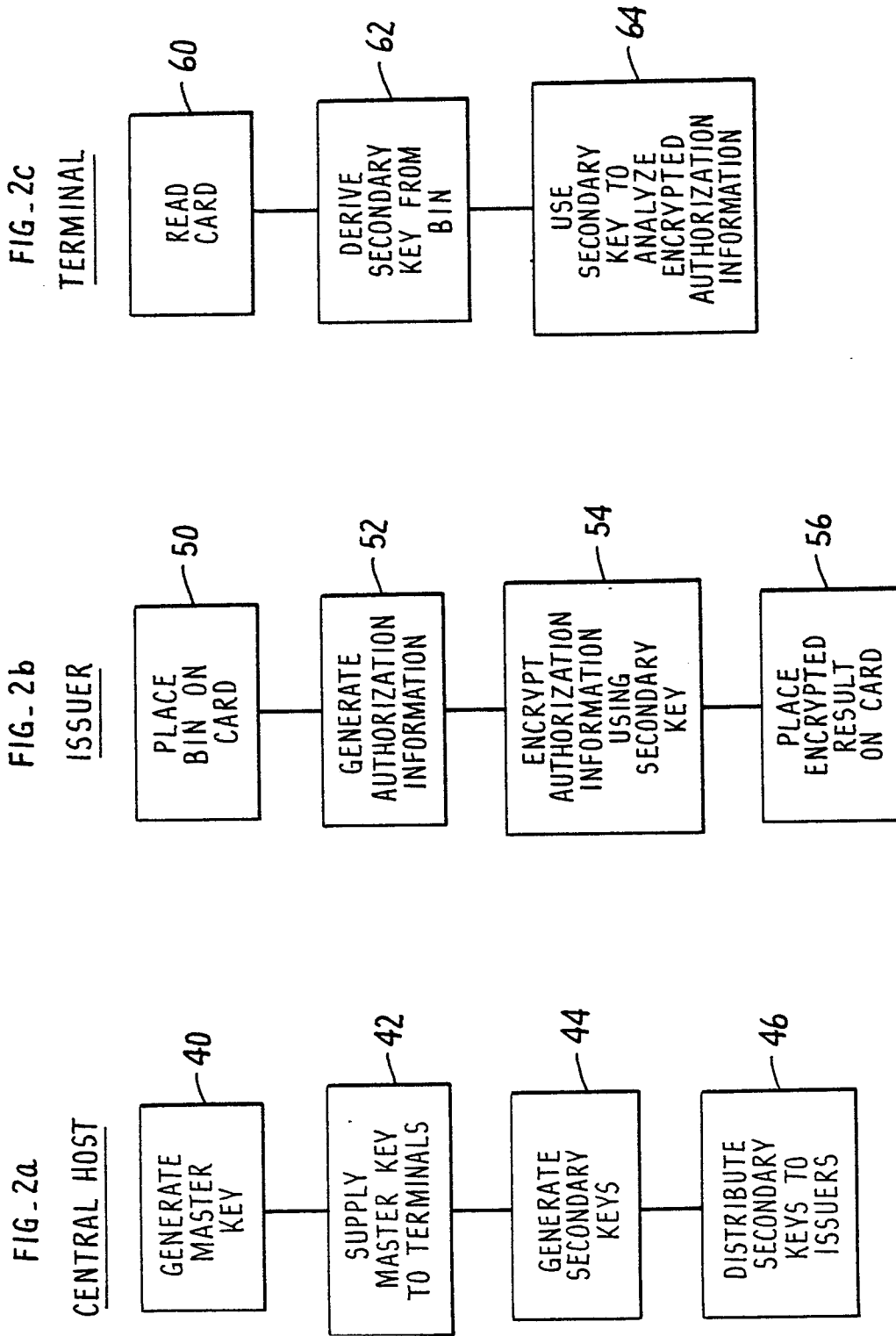


FIG. 1.



**FIG. 2.**



FIG. 3a

ISSUER

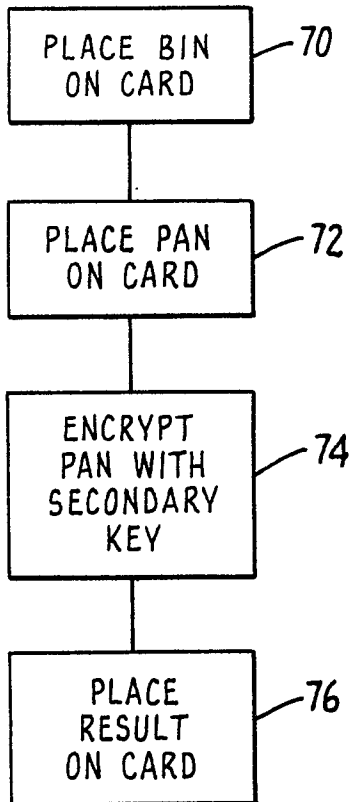


FIG. 3b

TERMINAL

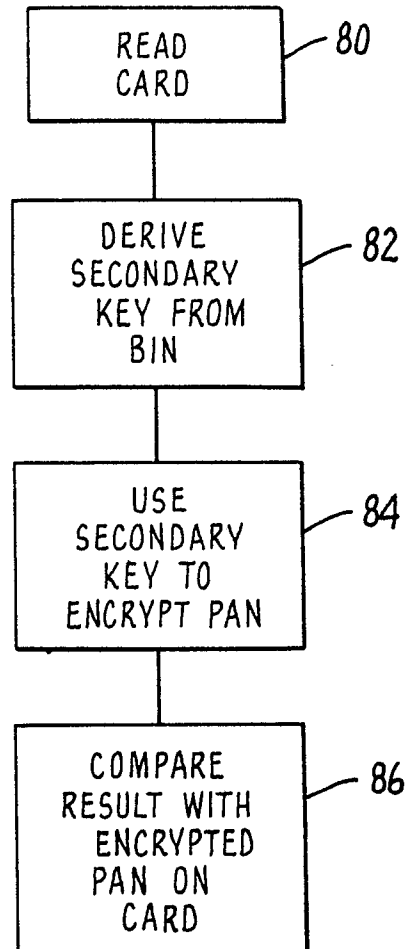


FIG. 3.

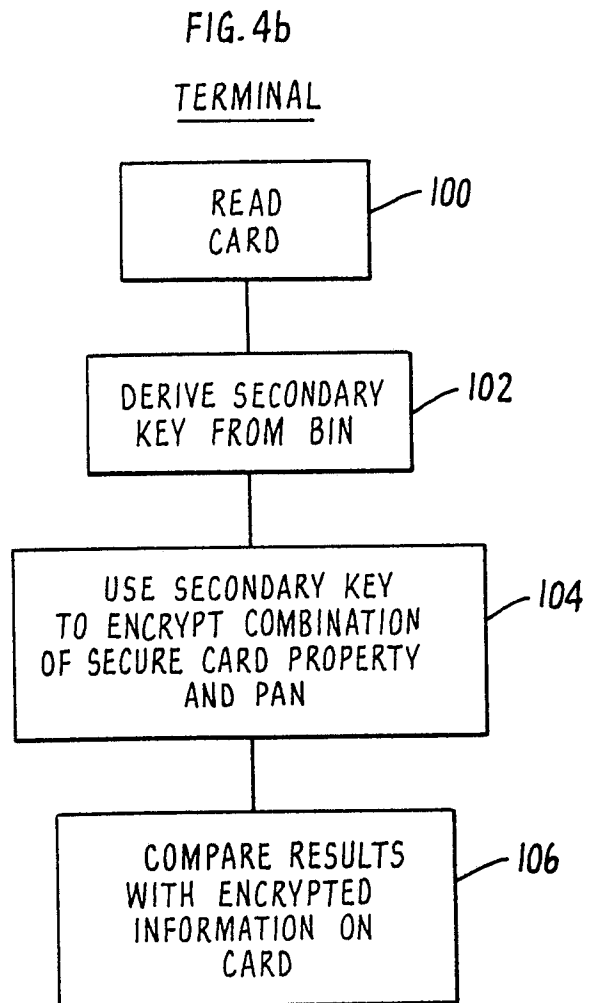
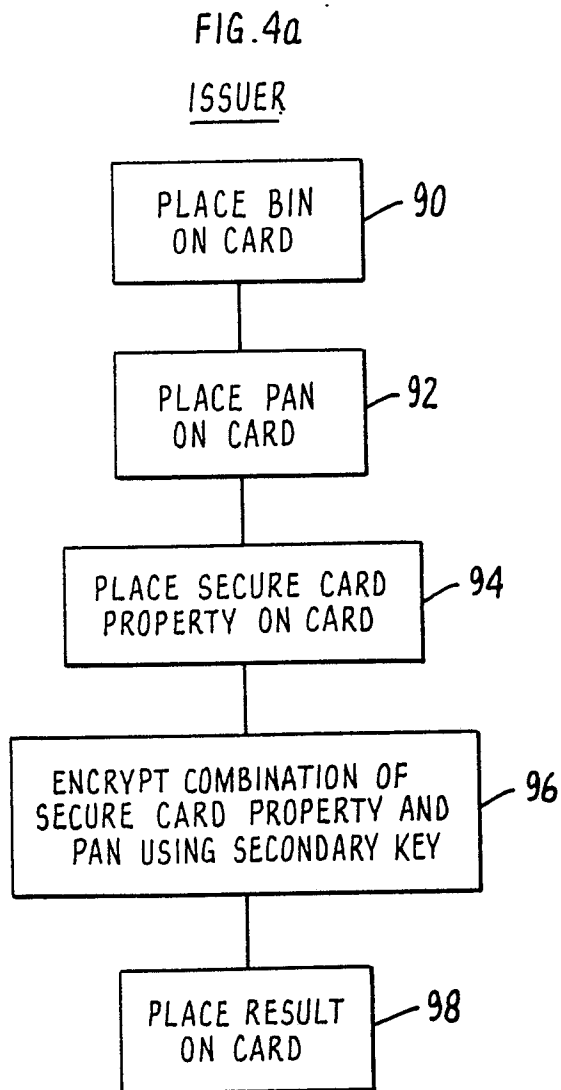


FIG. 4.

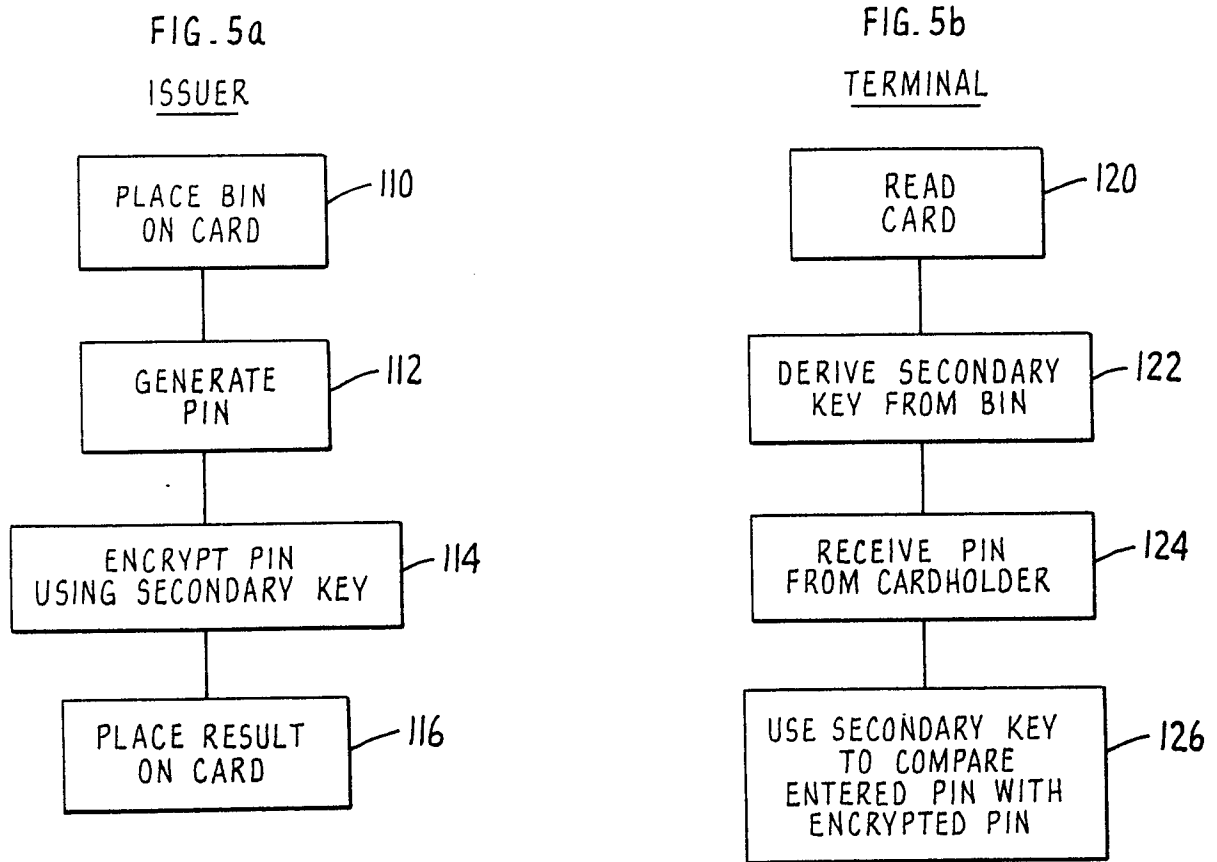


FIG. 5.

