

⑫

EUROPEAN PATENT SPECIFICATION

④⑤ Date of publication of patent specification: **04.03.87**

⑤① Int. Cl.⁴: **G 07 F 7/10**

②① Application number: **82306989.3**

②② Date of filing: **30.12.82**

⑤④ **Testing the validity of identification codes.**

④③ Date of publication of application:
11.07.84 Bulletin 84/28

④⑤ Publication of the grant of the patent:
04.03.87 Bulletin 87/10

⑧④ Designated Contracting States:
DE FR GB IT

⑤⑥ References cited:
EP-A-0 007 002
EP-A-0 028 965
EP-A-0 029 894
WO-A-82/02446
GB-A-2 020 513

IBM TECHNICAL DISCLOSURE BULLETIN, vol.
16, no. 8, January 1974, pages 2539-2540, New
York, USA, C.D. CULLUM et al.: "Cryptographic
password management system"

⑦③ Proprietor: **International Business Machines Corporation**
Old Orchard Road
Armonk, N.Y. 10504 (US)

⑦② Inventor: **Holloway, Christopher**
1 Thorverton Court Thorverton Road
Cricklewood London NW2 1RD (GB)

⑦④ Representative: **Appleton, John Edward**
IBM United Kingdom Limited Intellectual
Property Department Hursley Park
Winchester Hampshire SO21 2JN (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).

Courier Press, Leamington Spa, England.

EP 0 112 944 B1

Description

This invention relates to methods of validating identification codes entered at locations connected in a communication network and in particular to methods of validating personal identification numbers (PIN) in an electronic funds transfer at the retail point of sale (E.F.T.) system.

Electronic Funds Transfer is the name given to a system of directly debiting and crediting customer and service suppliers' accounts at the instant of confirmation of a transaction. The accounts are held at a bank, or credit card company's central processing system, which is connected to a dedicated network of retailers or service suppliers' data processing equipment. In this way no cash or cheque processing is required for the transaction.

In a simple application each bank or credit card company has its own network and each customer of the bank has a credit card which can only be used on that network, such a network is described in European Patent Publication 32193.

European Patent publication 32193 (IBM Corporation) describes a system in which each user and retailer has a key number — retailers key K_r and users key K_p — which is stored together with the user's identity number and retailer's business number in a data store at the host central processing unit (c.p.u.). The retailer's key and the user key are used in the encryption of data sent between the retailer's transaction terminal and the host c.p.u. Obviously only users or customers with their identity numbers and encryption keys stored at the host c.p.u. can make use of the system. As the number of users expands there is an optimum number beyond which the time taken to look up corresponding keys and identity numbers is unacceptable for on-line transaction processing.

European Patent Publication 18 129 (Motorola Inc.) describes a method of providing security of data on a communication path. Privacy and security of a dial-up data communications network are provided by means of either a user or terminal identification code together with a primary cipher key. A list of valid identification codes and primary cipher code pairs is maintained at the central processing unit. Identification code and cipher key pairs, sent to the c.p.u. are compared with the stored code pairs. A correct comparison is required before the c.p.u. will accept encoded data sent from the terminal. All data sent over the network is encrypted to prevent unauthorised access using the relevant user or terminal key.

UK Patent Application 2,020,513A (Atalla Technologies) describes a method and apparatus which avoids the need for transmitting user-identification information such as a personal identification number (PIN) in the clear from station to station in a network such as described in the two European Patent Publications mentioned above. The PIN is encoded using a randomly generated number at a user station and the encoded PIN and the random number are sent to the processing station. At the processing station a

second PIN having generic application is encoded using the received random number and the received encoded PIN and the generic encoded PIN are compared to determine whether the received PIN is valid.

In such a system a generic PIN having an encoded value that will give a valid comparison with many users PINs will be such as to provide valid comparisons with randomly generated PINs and is unlikely to prevent fraudulent use.

The EFT system made possible by the systems described in the above patent applications is limited to a single host c.p.u. holding the accounts of all users both retailers and customers.

An EFT system in which many card issuing organisations (banks, credit card companies, etc.) are connected and many hundreds of retail organisations are connected through switching nodes such as telephone exchanges, brings many more security problems.

PCT publication Wo 81/02655 (Marvin Sendrow) describes a multi-host, multi-user system in which the PIN is encrypted more than once at the entry terminal. The data required to validate and authorise the transactions is transmitted to a host computer which access from its stored data base the data that is required to decrypt and validate the transaction, including the encrypted PIN. A secret terminal master key must be maintained at each terminal. A list of these master keys is also maintained at the host computer.

The maintaining of lists of terminal master keys at each of the card issuing organisation's host computers is obviously a difficult task, when the EFT network may be connecting new retailers terminals on a daily basis.

European Patent publication 55580 (Honeywell Informations systems) seeks to avoid the necessity of transmitting PIN information in the network. This is achieved by issuing each user with a card that has encoded in the magnetic strip the bank identification (BIN) the user's account number (ACCN) and a PIN offset number. The PIN offset is calculated from the PIN, BIN and ACCN. The user enters the PIN at a keyboard attached to the terminal, which also reads the PIN offset, BIN and ACCN from the card. The terminal then recalculates a PIN offset from the user's entered PIN, the BIN and ACCN. If the recalculated PIN offset is the same as the PIN offset read from the card then validation of the PIN is assumed.

This system has the disadvantage in that the card issuer is not involved in the validation and that knowing that the PIN offset is calculated from the PIN, the BIN and ACCN, anyone having illicitly the process can manufacture fraudulent cards with valid PINS.

PCT Application WO 82/02446 (Transac-Alcatel (USA Patent 4,498,000)) describes both a method and the apparatus for exchanging data between a crediting means (smart-card) and a remote data processing centre. The data produced by the smart card includes a secret PIN number and a card identification. An encryption key stored on the card is used to encrypt the data which is then

sent through a suitable terminal to the d.p. centre. Validation takes place at the d.p. centre.

This scheme can only work with a smart-card (i.e. a card with an embedded microprocessor and read only memory) and is not applicable to the majority of credit card schemes that already exist.

IBM Technical Disclosure Bulletin Vol 16 No 8 Jan 1974 at pages 2539 and 2540 includes an article on "Cryptographic password management" by Cullum, Feistel and Smith. The article is directed to securing a users password in a processing network by using cryptographic procedures.

Also relevant prior art is European Patent Application 7002 (IBM) which describes a transaction terminal system provided with potential user authentications.

It is an object of the present invention to avoid the disadvantages inherent in the prior art system discussed above and provide a method for validating an identification code in which the code does not have to be transmitted and the issuer is involved in validation.

According to the present invention there is provided a method of testing the validity of an identification code at a location connected over a communication network to a data processing centre at which valid identification codes are stored, comprising the steps of:

- a) receiving at the location the identification code and an index number,
- b) deriving from the identification code and the index number a derived authorisation parameter, and characterised by including the steps of:
 - c) generating a variable number for each particular validation test,
 - d) storing the variable number in a location store and transmitting the variable number together with the index number to the data processing centre,
 - e) at the data processing centre using the index number to identify or
 - derive a valid authorisation parameter
 - f) encrypting the variable number using the valid authorisation parameter as an encryption key and using the result as a valid message authentication code,
 - g) at the location encrypting the variable number using the derived authorisation parameter as an encryption key and using the result as a derived message authentication code,
 - h) comparing the valid message authentication code with the derived message authentication code and using the result of the comparison as a determination of the validity of the identification code.

An EFT network that is used by several card issuing agencies, banks, credit card companies, etc., and many retail outlets, from large department stores to single unit shops and garages many spread over a large geographical area. It is envisaged that for a country such as Britain then each card issuer's central processing site and each retail outlet will be connected to a telecommunication network such as the telephone net-

work with direct lines to local exchanges. In such a system is it essential that each card issuing agency is involved in the authorisation of transactions and in the authentication of the card user's identity.

The number of retail point of sale locations are numbered in hundreds of thousands and there may be a hundred or more different card issuing agencies. In this situation the use of encryption keys that are known both to all card users and to all the point of sale locations become unmanageable and it is desirable to ensure that PIN's are not transmitted through the network.

In order that the invention may be fully understood a preferred embodiment will now be described with reference to the accompanying drawings in which:

FIG. 1 is a block schematic diagram of the components of a point of sale terminal used in the preferred embodiment.

FIG. 2 is a block schematic diagram of the components of a central processor used in the preferred embodiment.

The essence of the present invention is to generate an authentication parameter that relates to the PIN both from the number entered at the location and the valid number stored at the host and use this authorisation parameter to encode a variable which has no direct relationship with the PIN. The variable can be generated at either or both the initiating location and the host processing centre. The received encoded variable then called a message authentication code is compared with the locally derived encoded variable, a correct comparison indicating that the entered PIN is valid.

In one embodiment the variable is generated in two parts, the first part at the location is transmitted to the central processor and the second part at the central processor, the two parts are logically combined at each location to give the complete variable. In the preferred embodiment the variable parts are the messages sent between the two locations, this can include indexing numbers such as a personal account number (PAN) and the host identification (CIAID) and random numbers generated at each location. As the PAN and CIAID can be deduced from an illicitly obtained user card, the use of random numbers is preferred and adds further to the security of the system.

In its simplest form the variable need only be a truly random number generated at the terminal and sent with index information to the host processing centre. At the host processing centre the variable is encoded using a valid authorisation parameter to derive a valid message authentication code (MAC). The terminal encodes the variable using the locally derived authorisation parameter to generate a derived message authentication code (DMAC), and the DMAC and MAC are compared. The comparison could take place at either the host processing centre or the terminal depending upon processing and security factors built into each location. If the comparison is made

at the host central processing centre then the DMAC is sent as part of the message and it is not necessary to transmit the MAC to the terminal.

Referring now to the drawings the preferred embodiment will be described in more detail. Figure 1 is a block schematic of a point of sale or transaction terminal which includes a keyboard 10, a card reader 11 and display 12, which are connected to a common bus 13. Also connected to the bus 13 is random access memory (RAM) 14, a microprocessor 15, a line adapter 16 and encryption device 17 and a read only memory (ROM) 18. The line adapter is connected to a modem 19 which is connected directly to the EFT network.

Figure 2 shows schematically a card issuing agency's processing system in which a processor 20 is connected to an encryption device 21, a main working store 22 and an input output channel controller 23 through a bus 24. The main work store 22 is connected to a mass backup store 25 which may be a large capacity disc store or a similar device.

When a card issuing agency (CIA) issues a card it encodes on it magnetically the user's account number (PAN) and the agency's identity (CIAID). With the card the customer also receives a secret personal number (PIN) which must be remembered and not associated with the card. The CIA maintains in its data bank 25 a list of all the PANs associated with the relevant valid authorisation parameters (VAPs) and of course the PANs are also used for the relevant financial information, although this aspect is not directly relevant to the present invention.

A transaction is initiated at the terminal when the user, or it may be a shop employee of a retail organisation, enters a card in the card reader 11. The control unit 18 will detect that a card is to be read and control the transfer of the pan and CIAID to the RAM store 14.

The control unit then constructs a message (message A) to be sent through the line adapter 16 and modem 19 to the appropriate host processing unit identified by the CIAID. The message contains the PAN or index number and routing information. It may also contain a random number, which because it does not have to be regenerated can be a truly random number without a known seed. The message A is stored in a message buffer in the RAM store 14. The random number can be generated by a special unit or in the processor 15, by standard techniques.

When the message A is received by the host processing unit the PAN or index number is used to identify the user's PIN held in the store 25. Of course the PIN need not be stored as such, but as a valid authorisation parameter (VAP) which is the combination of PIN and PAN, and other static card data. Using an exclusive or function, the other card data (generically termed a personal key) is combined with the PIN. The resultant data is then used as an encipherment key to encipher the PAN to produce the VAP.

The processor 20 constructs a return message

B, which in the preferred embodiment is regarded as the second half of the variable, as message A this may also contain a truly random number. Messages A and B are then concatenated (Mess A: Mess B) by the processor 20 and the result (VAR) stored in the main store 22. VAR is then encoded by the encryption device 21 using the VAP as the encryption key. The result is a message authentication code (MAC). MAC is then added to message B which is then transmitted to the originating terminal through the I/O channel control 23 and the EFT network.

When the message B together with the MAC are received at the terminal they are stored in a message buffer of RAM 14. The control unit will then cause an instruction to appear on the display 12 telling the card user to enter his or her PIN at the keyboard 10. If the terminal is used by the card user only for cash issuing then the card reader 11, keyboard 10 and display 12 can be close together, however if the terminal is used for point of sale transactions then the keyboard at which PINs are entered must be shielded from the retailers employees. When the user enters the PIN this is then stored in the RAM 14. The next step at the terminal is to generate a locally derived authorisation parameter (DAP). This is done by using the processor 15 to perform the same function as that used to derive the VAP. The DAP is then stored in the RAM 14. The control unit and processor 15 now performs the identical concatenation operation on message A and message B as performed by the host processor. The result should be the same as VAR, the variable generated at the host processor. The encryption device 17 then encrypts VAR using the previously generated DAP as the encryption key, the result is a locally generated MAC (DMAC). The DMAC is stored in the RAM 14 and the processor 15 then compares the received MAC with DMAC. An incorrect comparison indicates that the PIN entered locally and used to generate the DAP was not correct and the transaction is aborted. The control unit 18 will cause an appropriate message to appear on the display. If the comparison is satisfactory then the entered PIN is correct and the control 18 unit will allow the transaction to proceed.

At no point in the above operation is the PIN available on insecure communication lines.

In an EFT system it is not necessary for the transaction terminal to store the PIN. The PIN need only be entered at the keyboard when the MAC is received from the host and the calculation of the DAP can be started at that point.

A random number can be generated by using a continuously running microsecond clock and the timed intervals between key strokes at the keyboard as seed numbers.

In the preferred embodiment the control of the operations of the transaction terminal is by micro-code stored in a read only memory in the control unit. The operations of the terminal could be controlled by a logic switching circuit embodied in a solid state logic device.

Claims

1. A method of testing the validity of an identification code (PIN) at a location (10—19) connected over a communication network to a data processing centre (20—25) at which valid identification codes are stored, comprising the steps of:

a) receiving at the location the identification code (PIN) and an index number (PAN).

b) deriving from the identification code (PIN) and the index number (PAN) a derived authorisation parameter (DAP),

and characterised by including the steps of:

c) generating a variable number unique to each particular validation test,

d) storing the variable number in a location store and transmitting the variable number together with the index number (PAN) to the data processing centre,

e) at the data processing centre using the index number (PAN) to identify or derive a valid authorisation parameter (VAP),

f) encrypting the variable number using the valid authorisation parameter (VAP) as an encryption key and using the result as a valid message authentication code (MAC),

g) at the location encrypting the variable number using the derived authorisation parameter (DAP) as an encryption key and using the result as a derived message authentication code (DMAC),

h) comparing the valid message authentication code (MAC) with the derived message authentication code (DMAC) and using the result of the comparison as a determination of the validity of the identification code (PIN),

2. A method as claimed in claim 1 in which the variable number is a message containing information for each validation test.

3. A method as claimed in claim 2 in which the variable number includes a random number.

4. A method as claimed in any one of claims 1, 2 or 3 in which step (h) is carried out at the location.

5. A method as claimed in any one of claims 1, 2, 3 or 4 in which the variable number includes message information generated by the data processing centre logically combined with message information generated by the location.

6. A method as claimed in claim 5 in which the messages generated by the location and the data processing centre are concatenated.

7. A method of testing as claimed in any one of the preceding claims in which the location is an electronic funds transfer system transaction terminal, the identification code is a personal identification number (PIN) and the index number is a personal account number (PAN).

8. A method as claimed in any one of the preceding claims including the further step of encrypting under a network system key messages sent between the location and the data processing centre.

9. A transaction terminal for connection to a data communication network in which identification numbers (PIN) entered at a remote loca-

tion (10—19) connected to a data processing centre (20—25) are tested for validity, comprising first means to receive and store related identification codes and index numbers, first location processing means operable to derive from the identification code (PIN) and index number (PAN) a derived authorisation parameter (DAP), and characterised by including second means operable to generate a variable number for each particular validation test, third means operable to transmit the index number (PAN) and the variable number to the data processing centre, and to receive from the data processing centre a message authentication code (MAC), second processing means including an encryption device operable to derive a derived message authentication code (DMAC) by using the derived authorisation parameter (DAP) as an encryption key to encode the variable number and comparing means operable to compare the received message authentication code (MAC) with the derived message authentication code (DMAC) and using the result of the comparison to determine the validity of the identification number (PIN).

10. A data communication network including a plurality of transaction terminals as claimed in claim 9 and including at each data processing centre means operable to generate a valid authorisation parameter (VAP) in response to a received index number (PAN) from an originating terminal, means operable to generate a valid message authentication code (MAC) by encrypting the variable number using the valid authorisation parameter (VAP) as an encryption key and producing a message authentication code (MAC) and means to transmit the message authentication code to the originating terminal.

Patentansprüche

1. Verfahren zur Prüfung der Gültigkeit eines Identifikationscodes (PIN) an einem Ort (10—19), welcher über ein Datenübertragungsnetzwerk mit einem Datenverarbeitungszentrum (20—25) verbunden ist, an welchem gültige Identifikationscodes gespeichert sind, mit den Verfahrensschritten des

a) Empfangens des Identifikationscodes (PIN) und einer Indexnummer (PAN) an dem Ort,

b) Herleitens eines hergeleiteten Berechtigungsparameters (DAF) aus dem Identifikationscode (PIN) und der Indexnummer (PAN), und gekennzeichnet dadurch, daß es die folgenden Verfahrensschritte enthält:

c) Erzeugen einer variablen Zahl, die zu jeder einzelnen Gültigkeitsprüfung einzig ist,

d) Speichern der variablen Zahl in einem Ortspeicher und Übertragen der variablen Zahl zusammen mit der Indexnummer (PAN) an das Datenverarbeitungszentrum,

e) Benutzen der Indexnummer (PAN) an dem Datenverarbeitungszentrum zur Identifikation oder Herleitung eines gültigen Berechtigungsparameters (VAP),

f) Verschlüsseln der variablen Zahl unter Verwendung des gültigen Berechtigungsparameters (VAP) als Verschlüsselungsschlüssel und Verwenden des Ergebnisses als gültigen Nachrichtenauthentisierungscode (MAC),

g) Verschlüsseln der variablen Zahl an dem Ort unter Verwendung des hergeleiteten Berechtigungsparameters (DAP) als Verschlüsselungsschlüssel und Verwenden des Ergebnisses als hergeleiteten Nachrichtenauthentisierungscode (DMAC),

h) Vergleichen des gültigen Nachrichtenauthentisierungscode (MAC) mit dem hergeleiteten Nachrichtenauthentisierungscode (DMAC) und Verwenden des Vergleichsergebnisses als Bestimmung der Gültigkeit des Identifikationscodes (PIN).

2. Verfahren nach Anspruch 1, bei welchem die variable Zahl eine Nachricht ist, welche Informationen für eine jede Gültigkeitsprüfung enthält.

3. Verfahren nach Anspruch 2, bei welchem die variable Zahl eine Zufallszahl enthält.

4. Verfahren nach irgendeinem der Ansprüche 1, 2 oder 3, bei welchem der Verfahrensschritt (h) an dem Ort ausgeführt wird.

5. Verfahren nach irgendeinem der Ansprüche 1, 2, 3 oder 4, bei welchem die variable Zahl durch das Datenverarbeitungszentrum erzeugte Nachrichteninformation logisch kombiniert mit durch den Ort erzeugter Nachrichteninformationen enthält.

6. Verfahren nach Anspruch 5, bei welchem die von dem Ort und dem Datenverarbeitungszentrum erzeugten Nachrichten verknüpft werden.

7. Prüfverfahren nach irgendeinem der vorstehenden Ansprüche, bei welchem der Ort ein Transaktionsterminal eines elektronischen Zahlungstransfersystems, der Identifikationscode eine persönliche Identifikationszahl (PIN) und die Indexnummer eine persönliche Kontonummer (PAN) ist.

8. Verfahren nach irgendeinem der vorstehenden Ansprüche mit dem weiteren Verfahrensschritt des Verschlüsseln von zwischen dem Ort und dem Datenverarbeitungszentrum gesendeten Nachrichten mit einem Netzwerkschlüssel.

9. Transaktionsterminal zur Verbindung mit einem Datenübertragungsnetzwerk, bei welchem an einem mit einem Datenverarbeitungszentrum (20—25) verbundenen entfernten Ort (10—19) eingegebene Identifikationszahlen (PIN) auf Gültigkeit geprüft werden, mit ersten Mitteln zum Empfangen und Speichern zugehöriger Identifikationscodes und Indexnummern, ersten Ortverarbeitungsmitteln, welche so betreibbar sind, daß sie aus Identifikationscode (PIN) und Indexnummer (PAN) einen hergeleiteten Berechtigungsparameter (DAP) herleiten, und gekennzeichnet, durch zweite Mittel, welche so betreibbar sind, daß sie eine variable Zahl für jede einzelne Gültigkeitsprüfung erzeugen, dritte Mittel, welche so betreibbar sind, daß sie die Indexnummer (PAN) und die variable Zahl an das Datenverarbeitungszentrum übertragen und vom

Datenverarbeitungszentrum einen Nachrichtenauthentisierungscode (MAC) empfangen, zweite Verarbeitungsmittel, welche eine Verschlüsselungsvorrichtung enthalten, die so betreibbar ist, daß sie einen hergeleiteten Nachrichtenauthentisierungscode (DMAC) unter Verwendung des hergeleiteten Berechtigungsparameters (DAP) als Verschlüsselungsschlüssel zur Codierung der variablen Zahl herleitet, und Vergleichsmittel, welche so betreibbar sind, daß sie den erhaltenen Nachrichtenauthentisierungscode (MAC) mit dem hergeleiteten Nachrichtenauthentisierungscode (DMAC) vergleichen und das Vergleichsergebnis zur Bestimmung der Gültigkeit der Identifikationsnummer (PIN) verwenden.

10. Datenübertragungsnetzwerk mit einer Anzahl von Transaktionsterminals nach Anspruch 9 und mit Mitteln an jedem Datenverarbeitungszentrum, die so betreibbar sind, daß sie einen gültigen Berechtigungsparameter (VAP) ansprechend auf eine von einem verursachenden Terminal erhaltene Indexnummer (PAN) erzeugen, Mitteln, die so betreibbar sind, daß sie einen gültigen Nachrichtenauthentisierungscode (MAC) durch Verschlüsseln der variablen Zahl unter Verwendung des gültigen Berechtigungsparameters (VAP) als Verschlüsselungsschlüssel erzeugen und einen Nachrichtenauthentisierungscode (MAC) erzeugen, und Mitteln zur Übertragung des Nachrichtenauthentisierungscode an den verursachenden Terminal.

Revendications

1. Procédé de vérification de la validité d'un code d'identification (PIN) dans une position (10—19) connectée par un réseau de communications à un centre de traitement de données (20—25) dans lequel des codes d'identification valides sont mémorisés, consistant:

a) à recevoir à la position, le code d'identification (PIN) et un numéro d'index (PAN)

b) à dériver du code d'identification (PIN) et du numéro d'index (PAN) un paramètre d'autorisation dérivé (DAF), et caractérisé en ce qu'il consiste à:

c) produire un nombre variable unique à chaque essai particulier de validation,

d) mémoriser le nombre variable dans une mémoire de position et transmettre le nombre variable avec le numéro d'index (PAN) au centre de traitement de données,

e) utiliser, au centre de traitement de données, le numéro d'index (PAN) pour identifier ou dériver un paramètre d'autorisation valide (VAP),

f) crypter le nombre variable en utilisant le paramètre d'autorisation valide (VAP) comme clé de cryptage et utiliser le résultat comme un code d'authentification de message valide (MAC),

g) crypter, à la position, le nombre variable en utilisant le paramètre d'autorisation dérivé (DAP) comme clé de cryptage et utiliser le résultat comme un code d'authentification de message dérivé (DMAC),

h) comparer le code d'authentification de message valide (MAC) avec le code d'authentification de message dérivé (DMAC) et utiliser le résultat de la comparaison comme une détermination de la validité du code d'identification (PIN).

2. Procédé selon la revendication 1, dans lequel le nombre variable est un message contenant des informations pour chaque vérification de validation.

3. Procédé selon la revendication 2, dans lequel le nombre variable contient un nombre aléatoire.

4. Procédé selon l'une quelconque des revendications 1, 2 et 3 dans lequel la phase (h) est exécutée à la position.

5. Procédé selon l'une quelconque des revendications 1, 2, 3 et 4 dans lequel le nombre variable contient les informations de message produites par le centre de traitement de données, combinées logiquement avec des informations de message produites par la position.

6. Procédé selon la revendication 5, dans lequel les messages produits par la position et le centre de traitement de données sont assemblées.

7. Procédé de vérification selon l'une quelconque des revendications précédentes, dans lequel la position est un terminal de transaction de système de transfert électronique de fonds, le code d'identification est un numéro d'identification personnel (PIN) et le nombre d'index est un numéro de compte personnel (PAN).

8. Procédé selon l'une quelconque des revendications précédentes, consistant en outre à effectuer un cryptage sous des messages clés de systèmes de réseau émis entre la position et le centre de traitement de données.

9. Terminal de transaction destiné à être connecté à un réseau de transmission de données dans lequel des numéros d'identification (PIN) introduits dans une position éloignée (10—19) connectée à un centre de traitement de données (20—25) sont vérifiées quant à leur validité, com-

portant un premier dispositif destiné à recevoir et à mémoriser des codes d'identification et des nombres d'index associés, un premier dispositif de traitement de position ayant pour fonction de dériver du code d'identification (PIN) et du numéro d'index (PAN), un paramètre d'autorisation dérivé (DAP) et caractérisé en ce qu'il comporte un second dispositif ayant pour fonction de produire un nombre variable pour chaque essai particulier de validation, un troisième dispositif ayant pour fonction d'émettre le nombre d'index (PAN) et le nombre variable vers le centre de traitement de données et de recevoir du centre de traitement de données un code d'authentification de message (MAC), un second dispositif de traitement comportant un dispositif de cryptage ayant pour fonction de dériver un code d'authentification de message dérivé (DMAC) en utilisant le paramètre d'autorisation dérivé (DAP) comme une clé de cryptage afin de coder le nombre variable et un dispositif de comparaison qui a pour fonction de comparer le code d'authentification de message reçu (MAC) avec le code d'authentification de message dérivé (DMAC) et utilisant le résultat de la comparaison pour déterminer la validité du numéro d'identification (PIN).

10. Réseau de transmission de données comprenant plusieurs terminaux de transaction selon la revendication 9 et comportant, à chaque centre de traitement de données, un dispositif ayant pour fonction de produire un paramètre d'autorisation valide (VAP) en réponse à un numéro d'index reçu (PAN) d'un terminal d'origine, un dispositif ayant pour fonction de produire un code d'identification de message valide (MAC) en cryptant le nombre variable en utilisant le paramètre d'autorisation valide (VAP) comme clé de cryptage et produisant un code d'authentification de message (MAC), et un dispositif qui émet le code d'identification de message vers le terminal d'origine.

45

50

55

60

65

7

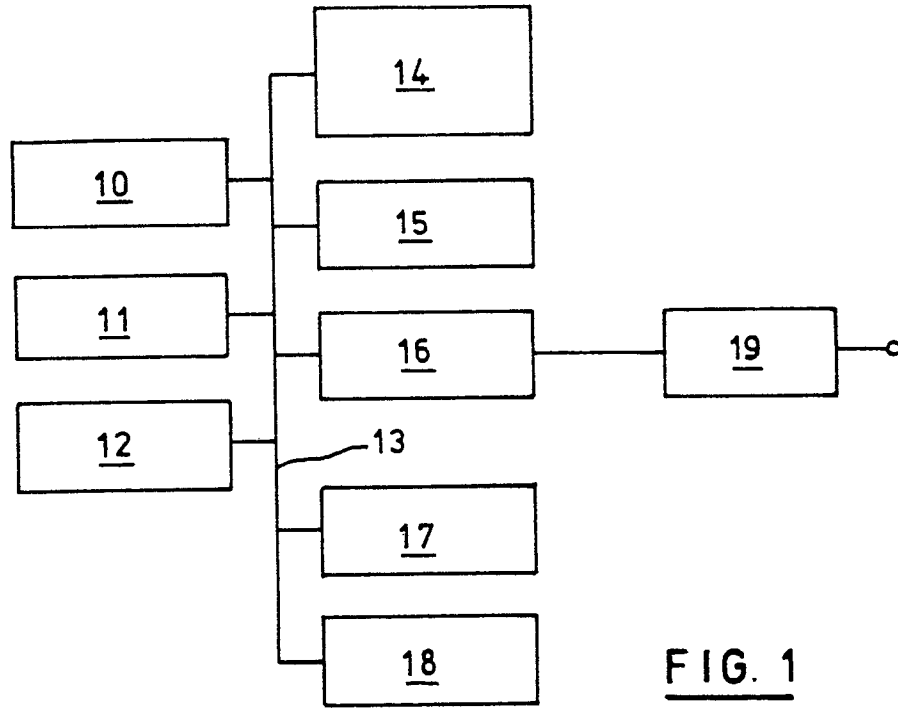


FIG. 1

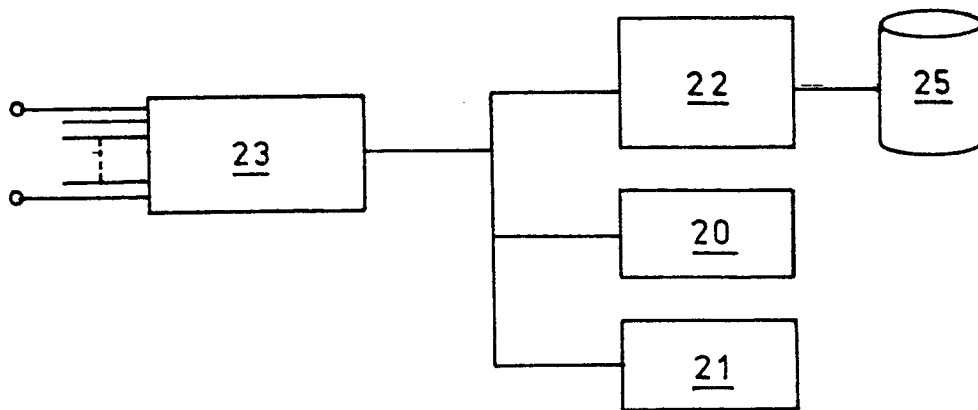


FIG. 2