(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 112 944**
**A1**

(12) # EUROPEAN PATENT APPLICATION

(21) Application number: **82306989.3**

(51) Int. Cl.³: **G 07 F 7/10**

(22) Date of filing: **30.12.82**

(43) Date of publication of application:
**11.07.84 Bulletin 84/28**

(84) Designated Contracting States:
**DE FR GB IT**

(71) Applicant: **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 Patent Operations Hursley Park**
**Winchester, Hants, SO21 2JN(GB)**

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

(57) A method and apparatus for testing the validity of personal identification numbers (PIN) entered at a transaction terminal of an electronic funds transfer network in which the PIN is not transmitted through the network. The PIN and the personal account number (PAN) are used to derive an authorisation parameter (DAP). A unique message is sent with the PAN to the host processor where the PAN is used to identify a valid authorisation parameter (VAP). The VAP is used to encode the unique message and the result (a message authentication code MAC) transmitted back to the transaction terminal. The terminal generates a parallel message authentication code by using the DAP to encode the unique message. The two MAC's are compared and the result of the comparison used to determine the validity of the PIN.

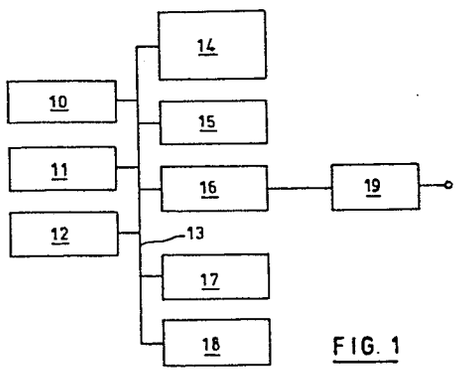


FIG. 1

EP 0 112 944 A1

# TESTING THE VALIDITY OF IDENTIFICATION CODES

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 Kr and users key Kp - which is stored together with the user's identify 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 Technovations) 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 stripe 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 disadvantages 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.

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,

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 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,

f) 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 network with direct lines to local exchanges. In such a system it is 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 cards 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 authentication 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 authentication parameter to derive a valid message authentication code (MAC). The terminal encodes the variable using the locally derived authentication 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 a 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 a card schematically issuing agency's processing system in which a processor 20 is connected to a 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 authentication 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 authentication parameter (VAP) which is the combination of PIN and PAN, and other staic 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 derive a local authentication parameter (DAP). This is done by using the processor 15 to perform an exclusive or (XOR) function on the PIN and PAN. The DAP is then stored in the RAM 14. The control unit and processor 15 now perform 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 LAP 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 generated the LAP 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 microcode 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 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,

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 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,

f) 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.

2. A method as claimed in claim 1 in which the variable number is a message containing information unique to 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 (f) 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 and the index number is a personal account number.

8. A method as claimed in any one of the preceding claims including the further step of encrypting under a network master 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 entered at a remote location connected to a data processing centre are tested for validity, including first means to receive and store related identification codes and index numbers, first location processing means operable to derive from the identification code and index number a derived authorisation parameter, second means operable to generate a variable number unique to each particular validation test, third means operable to transmit the index number and the variable number to the data processing centre, and to receive from the data processing centre a message authentication code,

second processing means including an encryption device operable to derive a derived message authentication code by using the derived authorisation parameter as an encryption key to encode the variable number and comparing means operable to compare the received message authentication code with the derived message authentication code and using the result of the comparison to determine the validity of the identification number.

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 in response to a received index number from an originating terminal, means operable to generate a valid message authentication code by encrypting the variable number using the valid authorisation parameter as an encryption key and producing a message authentication code and means to transmit the message authentication code to the originating terminal.

11. A data communication network as claimed in claim 10 operable to perform a method of testing as claimed in any one of claims 1 to 8.

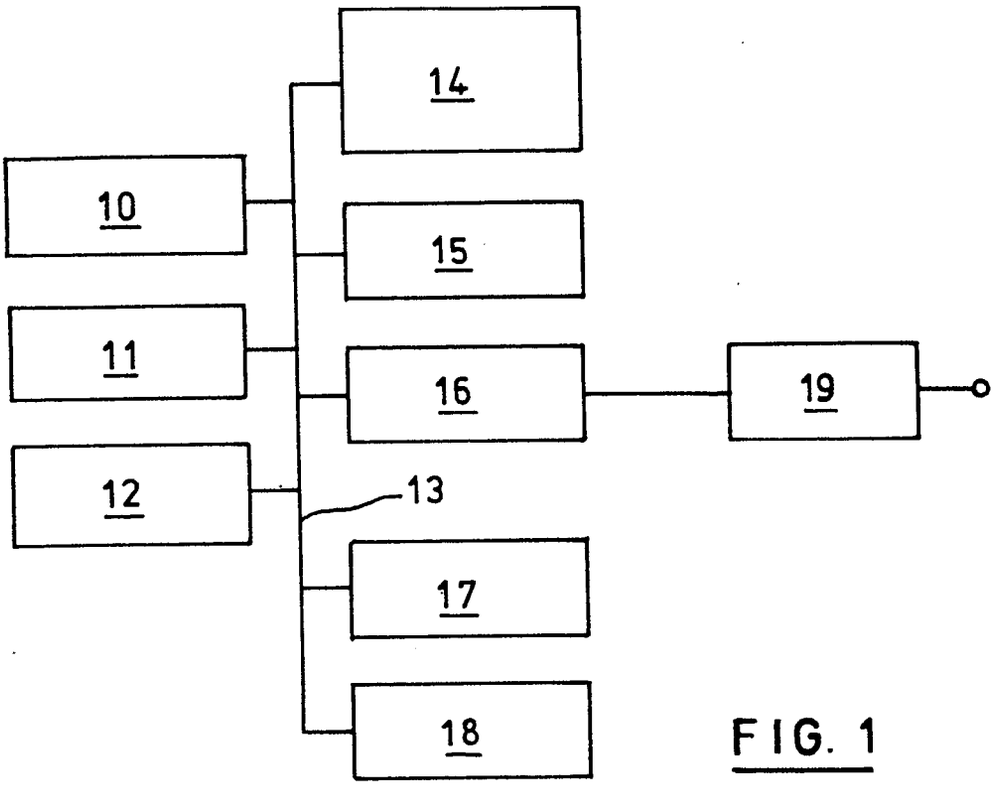


FIG. 1

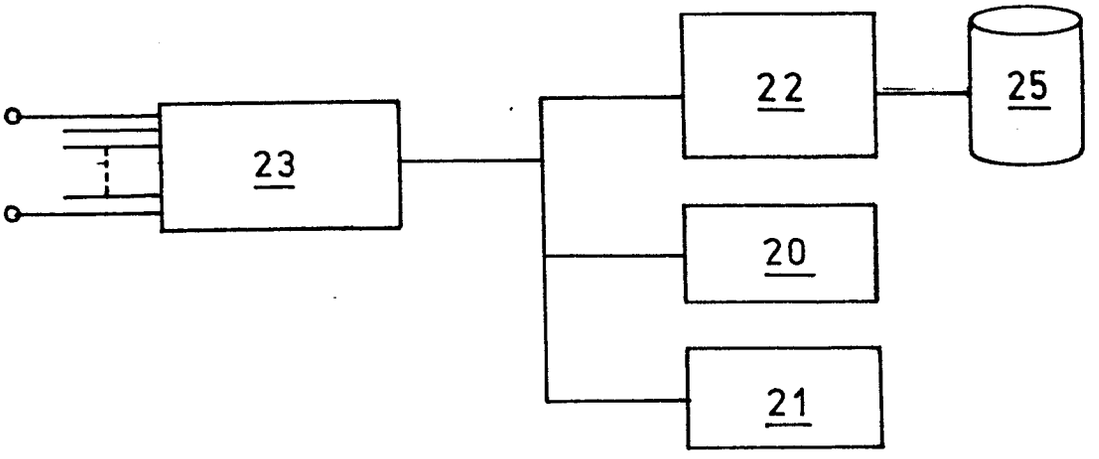


FIG. 2

European Patent Office

0112944

Application number

EP 82 30 6989

# EUROPEAN SEARCH REPORT

## DOCUMENTS CONSIDERED TO BE RELEVANT

| Category | Citation of document with indication, where appropriate, of relevant passages | Relevant to claim | CLASSIFICATION OF THE APPLICATION (Int. Cl. ³) |
|---|---|---|---|
| Y | WO-A-8 202 446 (TRANSAC-ALCATEL) * Abstract; figures 1,2; page 3, line 3 - page 8, line 33; claims * | 1,7-10 | G 07 F 7/10 |
| Y | EP-A-0 007 002 (IBM) * Abstract; figures 4A-4B,5A-5B; claims; page 6, last paragraph - page 9, 1st paragraph * | 1,2,7-10 | |
| A | 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" * Whole article * | 1,2,9 | |
| D,A | GB-A-2 020 513 (ATALLA TECHNOVATIONS) * Abstract; figures, claims * | 1-3 | |
| A | EP-A-0 029 894 (IBM) * Abstract; figures; claims * | 1-7 | |
| A | EP-A-0 028 965 (CII-HB) * Abstract; figure 1; claims * | 1-3 | |

TECHNICAL FIELDS SEARCHED (Int. Cl. ³)

G 07 F 7/00
G 07 F 7/02
G 07 F 7/08
G 07 F 7/10
G 06 F 15/30
H 04 L 9/00
H 04 L 9/02

The present search report has been drawn up for all claims

| Place of search | Date of completion of the search | Examiner |
|---|---|---|
| THE HAGUE | 07-10-1983 | DAVID J.Y.H. |

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO Form 1503. 03 82