The present invention concerns a method of routing secret keys, and in particular keys for operating a new service, to security modules and user cards in a data processing network.

This invention applies in particular to the setting up and operation of a new service in an existing network. It also allows the user of a data storage and processing card, to access a new or existing service, in a network.

A network consists of several data processing or exchange units such as for example one or more central processing units, and one or more terminals connected to each central processing unit and capable of communicating with service user cards. The services may be, for example, offered by a banking establishment, a mail order establishment, etc. It is known that in a network, each processing or exchange unit itself comprises a so-called security module which generally includes a microprocessor connected to a memory, constructed in monolithic form. Each security module allows an authorised body to load into this module at least one secret base key. The security module can calculate from this base key and by a suitable diversification algorithm, at least one diversified key. Each security module can authenticate in particular, by a suitable programme, a diversified key as having been worked out from a predetermined base key.

The user card is itself designed as a security module.

A security module of this type as well as the method of diversifying a base key and authenticating the diversified key obtained are described in European patent application EP-A 0 253 722 published on 20.01.88 in the name of the same applicant.

Any security module belonging to a data processing or communications unit or constituting a user card in a network contains a diversified key, when the network operates for a predetermined service.

It is known that diversified secret keys which allow the different modules of the network to communicate by providing the above-mentioned authentication are recorded in the different security modules of the network, by the

manufacturer of these modules or by an authorised body, in a room under high surveillance, in order to prevent any criminal from finding out the base keys and the diversified secret keys calculated from these base keys.

Thus, each security module has its own secret diversified key different to the diversified secret keys attributed to the other security modules or to the card. These diversified keys allow any security module in the network (the card itself may be considered as a security module) to verify that the diversified key recorded in a predetermined module does in fact correspond to the secret base key which has made it possible to obtain this secret diversified key; this base key is recorded in another security module to which the predetermined module is connected.

This mechanism for authenticating or certifying diversified keys is described in the aforementioned European patent application.

The operation of a new service in a network, if it does in fact require the use of these secret base keys and of these secret diversified keys obtained respectively from these base keys, as well as implementation of the procedures for authenticating the diversified keys described above, further requires the entry, in the security modules of the network, of secret base keys called keys for operating this service; these operating keys are diversified only in the last security module of the network (the user card, for example), thus allowing this last module to access the new service thus set up in the network.

At present, it is not known how to set up a new service in an existing network, without having to return the security modules (including the user cards) of this network to an authorised body under high surveillance, in order for the latter to record in these modules the secret keys (diversified in the user card) for operating this new service.

It follows that the setting up of a new service is complicated, since it requires withdrawal of the security modules of the network in order to return them to the

authorised body, then re-installation of these modules in the network. These operations are long and make the network inoperative while they are being carried out; consequently they are expensive. Further, they comprise risks of loss or destruction of one or more of the security modules temporarily withdrawn from the network, or even diversion of these modules by a criminal with ill intentions.

Thus, for example, the article published in "I.B.M. Technical Disclosure Bulletin," vol. 22, no. 2 of July 1979 (pages 629-631) describes a method of inserting user keys in a multi-user network.

The addition of one or more new stations to the network, that is in fact the setting up of one or more new services in the existing network, requires that a directory stored in each of the old stations should be modified in order to take each new station into account, and that a directory should be stored in each new station, in order for all the stations to be able to communicate with each other in a protected manner. As long as this operation has not been carried out in full, the network cannot operate with the new stations: it is therefore inoperative; similarly, during modification of the directories of the old stations, the network is inoperative.

It is precisely the object of the invention to remedy these disadvantages and in particular to allow the setting up of a new service in an existing network, as well as access to this new service for users, without it being necessary to return the security modules of the different modules of this network as well as the user cards to an authorised body, in order to install in these modules and these cards the secret keys for operating this new service in the network.

The objects are achieved in particular by using a module for loading operating keys, connected to one or more of the security modules of the network. The operating keys pass in coded form, step by step, to the security modules of lower and lower hierarchy (security module of a terminal connected to the central processing unit, then user card,

for example); these operating keys are diversified only in the last security module (the user card in the example chosen). Transmission of the operating keys from the loading module to the other modules of the network, which is carried out in coded form, avoids any fraud during this transmission.

The invention therefore proposes a method of routing at least one predetermined secret key, with the object of protecting the operation of a service, from one security module of a central processing unit (C1) of a network for operating a service to another security module of a terminal of this network, or to user cards connectable to the terminal and themselves constituting security modules, characterised in that it consists of transmitting a predetermined operating key in coded form, from a security module having a predetermined hierarchical level to a security module (terminal or card) having a hierarchical level lower than the predetermined level, this coding consisting of using a coding algorithm contained in the module with the predetermined hierarchical level and involving the predetermined operating key as well as at least one diversified transfer key recorded in the module having a hierarchical level lower than the predetermined level, this diversified key necessary for coding is obtained by a diversification algorithm contained in the module of predetermined hierarchical level and involving a base key of this diversified transfer key, as well as diversification data coming from the module of lower hierarchical level, the coded predetermined operating key being decoded by using, in the module with a hierarchical level lower than the predetermined level, a decoding algorithm which is the reverse of the coding algorithm.

According to another characteristic, any diversified key transmitted from a module of predetermined hierarchical level to a module of lower hierarchical level in order to be recorded therein, is coded, the method consisting of using a coding algorithm contained in the module of predetermined hierarchical level and involving the diversified transfer key to be transmitted as well as another

diversified key calculated by the diversification algorithm contained in the module of predetermined hierarchical level and recorded in the module of hierarchical level lower than the predetermined level, the diversified key thus coded being decoded by an algorithm which is the reverse of the coding algorithm, contained in the module of hierarchical level lower than the predetermined level.

According to another characteristic, the method consists of using a loading module connectable to the module with the highest hierarchical level in the network, this module containing base keys recorded by an authorised body, these base keys corresponding to the predetermined operating keys to be routed, as well as to the diversified keys serving for the coded transmission of each predetermined secret operating key, this loading module containing at least one algorithm for the diversification of base keys and at least one algorithm for the coding of base keys or diversified keys to be transmitted to the modules of the network for routing the operating keys.

According to another characteristic, diversified keys are prerecorded respectively in the modules and in the cards by an authorised body before use of the modules and cards in the network.

According to another characteristic, the method consists of coding, by a coding algorithm contained in the loading module, a first predetermined base key for operation of a service recorded in this loading module, this first coded key being transmitted from the loading module to the security module of the central processing unit where it is decoded by an algorithm which is the reverse of the coding algorithm, this first key being recoded by a coding algorithm contained in the security module of the central processing unit in order to be transmitted to the security module of the terminal where it is decoded by an algorithm which is the reverse of the coding algorithm, this first key being diversified and coded in the security module of the central processing unit, by diversification and coding algorithms contained in the module of the central processing unit, in order to be

transmitted to the user card where it is decoded by an algorithm which is the reverse of the coding algorithm.

According to another characteristic, the coding algorithm of the first operating key transmitted from the loading module to the security module of the central processing unit involves the base key of this first key, as well as a first diversified transfer key obtained by a diversification algorithm contained in the loading module and involving a base key of this first transfer key contained in the loading module, as well as diversification data coming from the security module of the central processing unit.

According to another characteristic, the coding algorithm of the first coded key transmitted from the security module of the central processing unit to the security module of the terminal involves this first key contained in the security module of the central processing unit, as well as a diversified communication key recorded in the security module of the terminal and calculated in the security module of the central processing unit, by a diversification algorithm involving the base key of this diversified communication key recorded in the security module of the central processing unit, as well as diversification data coming from the security module of the terminal.

According to another characteristic, the base communication key recorded in the security module of the central processing unit is transmitted in coded form from the loading module to the security module of the central processing unit, the coding of this communication key using a coding algorithm contained in the loading module and involving the base key contained in the loading module, as well as the first diversified transfer key calculated in the loading module, the diversified communication key to be recorded in the security module of the terminal being transmitted from the loading module to the security module of the terminal, in diversified and coded form, the diversification of this key using a diversification algorithm of the loading module involving the base communication key contained in the loading module as well

as diversification data coming from the security module of the terminal, the coding of this diversified communication key using a coding algorithm involving the diversified communication key, as well as a second diversified transfer key obtained by a diversification algorithm contained in the loading module and involving the base key of this second transfer key contained in the loading module, as well as diversification data coming from the security module of the terminal.

According to another characteristic, the diversification algorithm contained in the security module of the central processing unit for diversifying an operating key to be transmitted to the user card, involves the base key of this operating key contained in this security module, as well as diversification data coming from the user card, the coding of the diversified operating key being obtained by an algorithm contained in the security module of the central processing unit and involving the diversified operating key as well as a diversified opening key recorded in the user card and calculated in the security module of the central processing unit by a diversification algorithm involving a base key of this opening key, recorded in the security module of the central processing unit, as well as diversification data coming from the user card.

According to another characteristic, the base opening key recorded in the security module of the central processing unit is transmitted in coded form by the loading module, the coding of this base key being obtained by a coding algorithm contained in the loading module, and using said first diversified transfer key.

According to another characteristic, the diversified opening key recorded in the user card is transmitted to the user card in coded form by the security module of the central processing unit, the coding of this diversified opening key using a coding algorithm contained in the security module of the central processing unit and involving this diversified opening key as well as a diversified fabrication key prerecorded in the card and calculated by the security module of the central processing

unit from a base fabrication key.

According to another characteristic, the base key of the diversified fabrication keys prerecorded in the user cards is transmitted to the security module of the central processing unit, in coded form, the loading module containing a coding algorithm involving this base key of the prerecorded diversified keys, as well as the first transfer key calculated by the loading module and present in the security module of the central processing unit.

According to another characteristic, the first and second diversified transfer keys are respectively prerecorded in the security module of the central processing unit and in the security module of the terminal.

The characteristics and advantages of the invention will be more apparent from the description below, given with reference to the attached drawings in which:

- Fig. 1 shows schematically and as an example, a network in which the method of the invention is carried out,
- Fig. 2 shows schematically the operations of preloading a diversified transfer key ensuring communication between a loading module MCH and security modules which will subsequently be allocated to the network,
- Fig. 3 shows schematically the operations of preloading, in a module of the network, a communication key CX diversified as CXd, in another module for the transfer of keys for operating a service, from one module to another,
- Fig. 4 shows schematically the operations of loading a key CP for providing a service into the modules of the network,
- Fig. 5 shows schematically the operations of loading and diversifying a key CPd for providing a service, in the module of the network which has the lowest hierarchy (the user card, for example),
- Fig. 6 shows schematically the operations of loading an opening key CO in the security modules which will be allocated to central processing units MSC1 from a loading module MCH,
- Fig. 7 shows schematically the operations of loading the diversified opening key CO in a module with the lowest

hierarchical level (card) with the aid of a fabrication key CF prerecorded in the card in a diversified form and loaded into the module MSC1 by the loading module in order to ensure coding of the opening key to be transmitted in its diversified form.

The network shown as an example in Fig. 1 comprises for example, in a data processing assembly, a central processing unit C1 connected to terminals T1, T2 to which may be connected user cards such as U1 or U2. Of course, the processing assembly may comprise one or more other central processing units such as C2, other terminals such as T3, and other cards such as U3, which in the example of carrying out the method of the invention do not belong to the network in question, but could perhaps belong to it.

In a known manner, the terminal T1 comprises a security module MST1 which will not be described here in detail, and which includes in particular a memory and processing circuits, such as a microprocessor for example, constructed in monolithic form. This security module makes it possible to record secret keys making it possible for example to identify by suitable algorithms the user card; this module also makes it possible to code, by coding algorithms, data which are supplied to the card U1, or to the central processing unit C1. These algorithms are moreover reversible in order to make it possible in the same way to decode data or keys which come from the central processing unit C1 or from a terminal T2 or from a card U1. A type of monolithic microprocessor used may be like the one described in patent application FR-A-2 536 880.

The central processing unit C1 also has a security module MSC1 having a structure and operation comparable to those of the security module MST1 of the terminal T1. The data circulating between the terminal T1 and the card U1 are coded; the same applies to the data circulating between the terminal T1 and the central processing unit C1 which are coded by suitable reversible algorithms. This security module contains in particular algorithms for diversification and coding of keys transmitted to the security module MST1 of the terminal or to the card U1.

The user card (U1 or U2 in Fig. 1) has storage and processing functions, and also constitutes a security module comparable to that of the central processing unit.

It is considered that, in a network, a central processing unit, in this particular case C1, and its associated security module MSC1, have in this network the highest hierarchical level according to the processing power of this unit. The terminals and their associated security modules have hierarchical levels lower than the predetermined hierarchical level of the central processing unit, and these levels are themselves higher than the hierarchical levels of the cards which are the lowest in the network.

When the network is used for a predetermined service, keys for providing a service are recorded in the security modules of the central processing unit, and some, or even others, are recorded in the terminal in question. These keys are diversified in the user card and allow this user to access the predetermined service, by connection of the card to the terminal, after recording in this card at least one diversified service providing key.

As indicated above, according to the state of the art, when the user of a card wants to access a service which was not provided at the time when the card was entrusted to him, it is necessary for this user to return the card to an authorised centre in order for this centre to enter in this card the diversified service providing key or keys corresponding to the desired service. The authorised centre, after entering these diversified keys in the card, returns the card to the user who can then use it for this new service, but after being deprived of his card and incurring the risks mentioned above. The security modules of the central processing unit and of the terminal must also be returned to the authorised centre in order to be loaded with service providing keys corresponding to a new service, offered in the network, if this service was not already set up in this network.

According to the method of the invention, it is no longer necessary, when it is wished to set up a service in

an existing network, to return the security modules of this network as well as the cards of the users wanting to be granted this service, to an authorised centre which records secret service providing keys in these modules and these cards. When the service already exists in the network, it is not necessary to return to an authorised centre the cards for which access to this service is desired.

The method of the invention will now be described in detail, supposing that it is wished to set up a new service in a network and that it is also wished to give access to this new service, to user cards for which this access was not provided.

The method of the invention consists of using a key loading module MCH, connected to the security module MSC1 of the central processing unit C1 of the network in question. This loading module contains the base keys necessary for carrying out the method. These keys are loaded into this module by the authorised body. The module MCH makes it possible to load into the security module of the central processing unit at least one service providing key CP which is recorded in diversified form CPd only in the security module having the lowest hierarchy in the network (the user card, for example).

The service providing key CP which is supplied by the loading module MCH is transmitted from this loading module to the security module MSC1 of the central processing unit C1, then to the security module MST1 of the terminal in coded form by diversified transfer keys (CTd1, CXd). It is transmitted in diversified form and then coded by another transfer key, also diversified (COd), from the security module of the central processing unit to the user card.

The result CPc1 of coding the service providing key CP, for transmission thereof from the loading module MCH, to the security module MSC1 of the central processing unit, uses in particular a diversified transfer key CTd1 which establishes the hierarchy in communication between the two modules MCH and MSC1. The results CPc2 of coding the key CP, for transmission thereof from the security module MSC1 of the central processing unit to the security module MST1

of the terminal, uses in particular a diversified communication key CXd which establishes another hierarchy in communication between the two modules MSC1, MST1. The key CP is diversified and coded as CPdc in order to be transmitted from the security module MSC1 of the central processing unit to the user card U1. This coding uses in particular a diversified key for opening a service COd. The diversification and coding of the different keys use specific algorithms which will be described below in detail.

The diversified transfer keys CTd1 and CTd2 correspond to at least one base key CT contained in the loading module. CTd2 is the diversified transfer key establishing the hierarchy in communication between the loading module MCH and the module of the terminal MST1. In the same way, the diversified keys for communication CXd and opening COd correspond to base keys CX, CO respectively, contained in the loading module and loaded into this module by the authorised body, in the required security environment.

The following figures allow a better understanding of carrying out the method of the invention and in particular the different operations of loading keys performed from the loading module MCH, as well as the operations of transfer, coding and diversification performed during this method.

These operations include, for setting up means of communication in a hierarchy:

An initialisation stage making it possible to set up the means of communication CT between the loading module MCH on the one hand and the security modules MSC, MST of the central processing units C or terminals T;

A stage for installation of the means of communication CX between the security modules MSC of the central processing units and MST of the terminals;

Another stage for installation of the means of communication by an opening key CO between the security modules of the central processing units MSC and of the user cards.

Subsequently, these means will be used to set up a service in the network by protected insertion of at least one service providing base key CP.

Fig. 2 shows schematically the loading of diversified transfer keys CTd1 and CTd2 of the initialisation stage which are loaded by the authorised body, into the security modules, from a base transfer key CT contained in the loading module MCH. These diversified keys are loaded into the security modules before installing these modules in the network. Each arrow entering the loading module MCH represents the entry in plain language of the keys to which they point. The arrows leaving the loading module or the other modules represent the coded transmission of the keys, which may be diversified, situated opposite these arrows.

The diversified transfer keys CTd1 and CTd2 are obtained owing to a diversification algorithm fA contained in the loading module MCH. This algorithm involves in a known manner the base transfer key CT contained in the loading module, as well as diversification data coming from the security modules MS1, MS2 which subsequently may be allocated to a central processing unit or a terminal. These diversification data are of course supplied to the loading module. The diversification algorithm is for example of the type described in the above-mentioned European patent application EP-A 0 253 722.

It follows that we can write:

CTd1 = fA (CT, diversification data of MS1), and

CTd2 = fA (CT, diversification data of MS2).

The diversified transfer keys CTd1 and CTd2, recorded in this way in the security modules MS1, MS2 respectively, will make it possible, as will be seen below in detail, to establish protected transmissions of coded keys between the loading module MCH and the security modules MS1 and MS2.

The next stage which is shown in Fig. 3 consists of managing the different security modules in a hierarchical system according to their destination for the central processing units or terminals by recording in the latter hierarchical communication keys which will allow or prevent communications according to whether they have corresponding keys or not.

Hence a module MS1 allocated to a central processing unit C1 will become a central processing unit security

module MSC1 and similarly a module MS2 allocated to a terminal T1 will become a terminal security module MST1. These objects are achieved owing to entry of the so-called hierarchical communication base key CX in the loading module MCH.

The key CX is recorded undiversified in the security module MSC1. Its transmission between MCH and MSC1 is carried out in coded form (CXc in Fig. 3). Coding of the key CX is obtained from a coding algorithm fA of the loading module, which involves the key CX, as well as the diversified transfer key CTd1, which is calculated beforehand by the loading module.

Thus we can write:

CTd1 = fA (CT, diversification data of MSC1)

and CXc = fA (CTd1, CX).

The key CXc is decoded (CX) by the security module MSC1 owing to an algorithm which is the reverse of the coding algorithm, since this module already contains the diversified transfer key CTd1. Naturally, the algorithm fA for coding the key CX may be different to the algorithm fA for diversifying the key CT.

The key CX is recorded diversified (CXd) in the security module MST1 of the terminal. This key CXd is obtained from the communication key CX of the module MCH. It is transmitted in diversified and coded form (CXdc) from the module MCH to the module MST1.

Diversification (CXd) of the key CX is obtained owing to a diversification algorithm fB of the loading module MCH involving the key CX, as well as diversification data coming from the security module MST1 of the terminal.

Thus we can write:

CXd = fB (CX, diversification data of MST1).

The hierarchy is therefore established between the modules MSC1 and MST1 by the keys CX and CXd, but each key CX, CXd has been supplied by the loading module MCH.

Coding (CXdc) of the key CXd for transmission of this diversified communication key between the loading module MCH and the security module MST1 is obtained owing to a coding algorithm fA contained in the loading module MCH and

involving the diversified transfer key CTd2, as well as the diversified key CXd calculated in the loading module MCH.

The loading module therefore calculates:

CTd2 = fA (CT, diversification data of MST1),

then CXdc = fA (CTd2, CXd).

The diversified coded key CXdc is decoded (CXd), in the security module MST1, by an algorithm which is the reverse of the coding algorithm, this module already containing the diversified transfer key CTd2. In the event that one or more central processing unit security modules MSC1 are enabled to deliver new services to users who hold cards U1 in the network, it is necessary to set up in these modules MSC1 opening keys CO making it possible to establish a hierarchical means of communication between the service provider modules MSC1 and the user cards U1.

For this it is necessary to insert in each central module MSC1 an opening key CO and to have inserted in the cards at least one diversified opening key COd, in a phase prior to putting each card into operation. This prior phase may be executed independently of the network protection phase which corresponds to insertion of the keys CT, CX and CO in the network, and preferably may be carried out outside of the operating network.

Insertion of the key CO is carried out as follows:

The key CO loaded by the authorised body into the loading module MCH is transmitted as shown in Fig. 6 in coded form (COc) to the security module MSC1 of the central processing unit. This coding is obtained owing to a coding algorithm fA contained in the loading module MCH and involving the diversified transfer key CTd1 contained in the security module MSC1, as well as the key CO. For this, the loading module calculates, as indicated above:

CTd1 = fA (CT, diversification data of MSC1),

then COc = fA (CTd1, CO).

The key COc is decoded (CO) by a reverse algorithm in the security module MSC1, since the diversified transfer key CTd1 is already recorded in this module.

Prior insertion of the diversified opening key COd in the cards is carried out as follows:

The diversified opening key COd is recorded in the user card U1 and its transfer from the central processing unit module MSC1 to the card U1 is carried out in coded form COdc as shown in Fig. 7.

The module MSC1 of Fig. 7 is a central processing unit security module which can only be used for prior loading or be used subsequently as a central module of the network.

Coding COdc of the diversified opening key COd is provided owing to a coding algorithm fB contained in the module MSC1 and involving the diversified key COd, as well as a diversified so-called fabrication key CFd already recorded in the card, at fabrication thereof; this key CFd characterises the card.

We may write COdc = fB (COd, CFd).

COd is calculated by the central processing unit security module MSC1 using the opening key CO according to the formula:

COd = fB (CO, diversification data of U1).

This requires calculation beforehand of the key CFd by the module MSC1. For this purpose, the base fabrication key CF entered by the authorised body in the loading module MCH is transferred in coded form CFc to the security module MSC1 of the central processing unit. This coding of the key CF is obtained owing to an algorithm fA of the loading module, which involves the key CF, as well as the diversified transfer key CTd.

The loading module therefore calculates first of all:

CTd1 = fA (CT, diversification data of MSC1)

then CFc = fA (CTd1, CF).

This coded key transmitted to the module MSC1 is decoded by a reverse algorithm, since MSC1 already contains the diversified transfer key CTd1.

The module MSC1 can then calculate by the diversification algorithm fB the diversified fabrication key CFd, this algorithm involving the base key CF contained in the security module MSC1, as well as diversification data coming from the card U1. We may write:

CFd = fB (CF, diversification data of U1).

It is after this last calculation that there can be

calculated, as indicated above, by the module MSC1, the diversified and coded opening key COdc = fB (COd, CFd), which is transferred to the card U1, where it is decoded (COd), for the card already contains the key CFd, since fabrication thereof. Naturally the algorithm fB for diversifying the keys CX and CF may be different to the algorithm fB for coding the keys CF and COd. It is obvious that in the event that it is not chosen to preload the diversified opening keys COd on the cards, but to load them by the installed network, one would start by inserting, by the central processing unit security module of the network MSC1, the key CF and then the key CO and the diversified key COd. In this case, a diversified fabrication key CFd is inserted in the card beforehand.

The next stage shown in Fig. 4 consists of setting up a service in the network thus installed which comprises the security modules MSC1 and MST1 and for which the preceding stages have enabled communications between the loading module MCH and the security modules MSC1 or MST1, and between the security module MSC1 of the central processing unit and the security module MST1 of the terminal.

This insertion of a service consists of using at least one service providing key CP prerecorded in the loading module MCH by an authorised body. This key may, as will be seen, be transmitted to the modules MSC1 and MST1. It will then be recorded in diversified form CPd in the user card U1 which will therefore have access to this service.

The service providing key CP is transmitted in coded form (CPc1) to the security module MSC1.

Coding of the key CP is obtained owing to an algorithm fA of the loading module MCH involving the diversified transfer key CTd1 calculated by MCH on the basis of the diversification data supplied by MSC1, as well as the key CP. For this, the loading module calculates first of all the diversified transfer key CTd1:

CTd1 = fA (CT, diversification data of MSC1),

then calculates:

$$CPc1 = fA\ (CTd1,\ CP).$$

The coded key CPc1 received by the security module

MSC1 is decoded by a reverse algorithm, since this module already contains the diversified key CTd1.

Next, the service providing key CP is transmitted in coded form (CPc2) from the security module MSC1 of the central processing unit, to the security module MST1 of the terminal. This coding is obtained owing to a coding algorithm fB contained in the security module MSC1 and involving the diversified communication key CXd calculated by MSC1 on the basis of the diversification data supplied by MST1 as well as the key CP. The security module MSC1 therefore calculates:

CXd = fB (CX, diversification data of MST1)

then CPc2 = fB (CXd, CP).

Naturally, a reverse algorithm contained in the security module MST1 makes it possible to deduce CP from CPc2, since this module already contains the diversified communication key CXd.

It is obvious that any transmission of a key requires prior authentication of the recipient by the issuer. This authentication is known, for example, from the aforementioned European patent application.

At the end of this operation, it may be considered that the service is now set up in a network comprising a single central processing unit and a single terminal, but the procedure would be identical in the case of a network having one central processing unit and several terminals or several central processing units in a hierarchical system each with several terminals. By contrast at this stage the user card does not yet have access to this service.

The next operation shown in Fig. 5 will consist of supplying to the user card U1 the keys necessary for operation thereof in the network for the service in question, and in particular the diversified key CPd from the key CP.

For this, there is used the means of communication established by the opening key CO and its diversified keys COd dedicated to the user cards U1. Coded transmission (CPdc) of the diversified service providing key CPd from the security module MSC1 of the central processing unit to

the user card U1 does not pass through the security module MST1 of the terminal in order to increase security. In this operation, the security module MST1 of the terminal is transparent, since the card is connected to the terminal and the module MST1 is not involved.

The service providing key CP will be recorded in the user card U1 in a diversified form (CPd), as Fig. 5 shows.

As indicated above, the key CP is recorded in the loading module MCH by the authorised body. It is then transmitted to the security module MSC1 of the central processing unit in coded form (CPc1), where it is decoded (CP) and then recorded in its uncoded form (CP).

The key CP will now be diversified and coded (CPdc) to be transmitted from the security module MSC1 to the user card U1 where it is decoded (CPd) and recorded.

Diversification (CPd) of the key CP is obtained owing to an algorithm fB of the security module MSC1, which involves the key CP, as well as diversification data coming from the user card U1.

We may write:

CPd = fB (CP, diversification data of U1).

This algorithm fB may be different to the above-mentioned algorithm fB.

Coding (CPdc) of the key CPd is obtained owing to an algorithm fB of the security module, which involves the diversified opening key COd, and the diversified service providing key CPd, calculated as indicated above.

The diversified opening key COd is obtained owing to a diversification algorithm fB of the security module MSC1 of the central processing unit.

This algorithm involves the base opening key CO supplied by the loading module as well as diversification data supplied by the user card U1.

We may write:

COd = fB (CO, diversification data of U1)

then CPdc = fB (COd, CPd).

This diversified and coded service providing key CPdc may be decoded in the card by an algorithm which is the reverse of the coding algorithm, since the card now

contains the diversified opening key COd.

Henceforth the card holder can enjoy this new service.

In the description of the invention, it could be considered that the security module MSC1 of the network already contains the key CP relating to provision of the desired service and that the method then consists of giving cards access to this service already set up. The method would then consist only of transmitting the key CPd to the card, naturally using the keys necessary for this transmission.

In the account of the invention a distinction has been established between on the one hand the algorithm fA which is an algorithm specific to the transfer function and which must be found in the modules MSC, MCH, MST and on the other hand the algorithm fB which is peculiar to the application contained in the "user" cards used by the system. However, it is obvious that the use of one and the same algorithm can be envisaged for employing the invention, or the combination with each key and/or each coding and diversification function of a different algorithm which must in this case be available in the modules where it is necessary.

The invention does not apply only to the embodiments described, but it extends obviously to all equivalents within the scope of anyone skilled in the art.

* C L M S *

Claims

1. Method of routing at least one predetermined secret key (CP), with the object of protecting the operation of a service, from one security module (MSC1) of a central processing unit (C1) of a network for operating a service to another security module (MST1) of a terminal (T1) of this network, or one of the user cards (U1) connectable to the terminal (T1) and themselves constituting security modules, characterised in that it consists of transmitting a predetermined operating key (CPd) in coded form, from a security module (MSC1) having a predetermined hierarchical level to a security module (MST1) or card (U1) having a hierarchical level lower than the predetermined level, this coding consisting of using a coding algorithm contained in the module with the predetermined hierarchical level and involving the predetermined operating key as well as at least one diversified transfer key (CTd; CXd; Cod) recorded in the module having a hierarchical level lower than the predetermined level, this diversified transfer key necessary for coding is obtained by a diversification algorithm contained in the module of predetermined hierarchical level and involving a base key (CT) of this diversified transfer key, as well as diversification data coming from the module of lower hierarchical level, the coded predetermined operating key (Cpd) being decoded by using, in the module with a hierarchical level lower than the predetermined level, a decoding algorithm which is the reverse of the coding algorithm.

2. Method according to claim 1, characterised in that any diversified key (Cpd) transmitted from a module of predetermined hierarchical level to a module of lower hierarchical level in order to be recorded therein, is coded, the method consisting of using a coding algorithm contained in the module of predetermined hierarchical level and involving the diversified operating key (Cpd) to be

transmitted, as well as a diversified transfer key (Ctd; Cxd; Cod) calculated by the diversification algorithm contained in the module of predetermined hierarchical level and recorded in the module of hierarchical level lower than the predetermined level, the diversified key (Cpd) thus coded being decoded by an algorithm which is the reverse of the coding algorithm, contained in the module of hierarchical level lower than the predetermined level.

3. Method according to claim 2, characterised in that it consists of using a loading module (MCH) connectable to the module with the highest hierarchical level in the network, this module containing base keys recorded by an authorised body, these base keys corresponding to the predetermined operating keys (Cpd) to be routed, as well as to the diversified keys serving for the coded transmission of each predetermined secret operating key, this loading module containing at least one algorithm for the diversification of base keys and at least one algorithm for the coding of base keys or diversified keys to be transmitted to the modules of the network for routing the operating keys.

4. Method according to claim 3, characterised in that diversified keys are prerecorded respectively in the modules and in the cards by an authorised body before use of the modules and cards in the network.

5. Method according to claim 4, characterised in that it consists of coding (CPc1), by a coding algorithm contained in the loading module (MCH), a first predetermined base key (CP) for operation of a service recorded in this loading module, this first coded key (Cpc1) being transmitted from the loading module (MCH) to the security module (MSC1) of the central processing unit where it is decoded (CP) by an algorithm which is the reverse of the coding algorithm, this first key (CP) being recoded (CPc2) by a coding algorithm contained in the security module (MSC1) of the

central processing unit in order to be transmitted to the security module (MST1) of the terminal where it is decoded by an algorithm which is the reverse of the coding algorithm, this first key being diversified and coded (CPdc) in the security module of the central processing unit, by diversification algorithms (Cpd) and coding algorithms (Cpdc) contained in the module of the central processing unit, in order to be transmitted to the user card where it is decoded by an algorithm which is the reverse of the coding algorithm.

6. Method according to claim 5, characterised in that the coding algorithm of the first operating key (Cpc1) transmitted from the loading module (MCH) to the security module (MSC1) of the central processing unit involves the base key (CP) of this first key, as well as a first diversified transfer key (Ctd) obtained by a diversification algorithm contained in the loading module and involving a base key (CT) of this first transfer key contained in the loading module, as well as diversification data coming from the security module (MSC1) of the central processing unit.

7. Method according to claim 5, characterised in that the coding algorithm of the first coded key (Cpc2) transmitted from the security module (MSC1) of the central processing unit to the security module (MST) of the terminal involves this first key (CP) contained in the security module (MSC1) of the central processing unit, as well as a diversified communication key (Cxd) recorded in the security module (MST1) of the terminal and calculated in the security module of the central processing unit, by a diversification algorithm involving the base key (CX) of this diversified communication key recorded in the security module (MSC1) of the central processing unit, as well as diversification data coming from the security module (MST1) of the terminal.

8. Method according to claim 7, characterised in that the base communication key (CX) recorded in the security module (MSC1) of the central processing unit is transmitted in coded form (CXc) from the loading module (MCH) to the security module of the central processing unit, the coding of this communication key using a coding algorithm contained in the loading module and involving the base key (CX) contained in the loading module, as well as the first diversified transfer key (CTd1) calculated in the loading module, the diversified communication key (Cxd) to be recorded in the security module (MST1) of the terminal being transmitted from the loading module (MCH) to the security module of the terminal, in diversified and coded form (CXdc), the diversification (Cxd) of this key using a diversification algorithm of the loading module involving the base communication key (CX) contained in the loading module as well as diversification data coming from the security module of the terminal (MST1), the coding of this diversified communication key (Cxdc) using a coding algorithm involving the diversified communication key (Cxd), as well as a second diversified transfer key (CTd2) obtained by a diversification algorithm contained in the loading module and involving the base key (CT) of this second transfer key contained in the loading module (MCH), as well as diversification data coming from the security module (MST1) of the terminal.

9. Method according to claim 8, characterised in that the diversification algorithm contained in the security module (MSC1) of the central processing unit for diversifying (Cpd) an operating key to be transmitted to the user card, involves the base key (CP) of this operating key contained in this security module, as well as diversification data coming from the user card, the coding of the diversified operating key (Cpdc) being obtained by an algorithm contained in the security module of the central processing unit and involving the diversified operating key (Cpd), as

well as a diversified opening key (Cod) recorded in the user card and calculated in the security module of the central processing unit by a diversification algorithm involving a base key (CO) of this opening key, recorded in the security module of the central processing unit, as well as diversification data coming from the user card.

10. Method according to claim 9, characterised in that the base opening key (CO) recorded in the security module of the central processing unit is transmitted in coded form (COc) by the loading module, the coding of this base key being obtained by a coding algorithm contained in the loading module, and using said first diversified transfer key (Ctd1).

11. Method according to claim 10, characterised in that the diversified opening key (Cod) recorded in the user card is transmitted to the user card in coded form (COdc) by the security module (MSC1) of the central processing unit, the coding of this diversified opening key using a coding algorithm contained in the security module of the central processing unit and involving this diversified opening key (Cod) as well as a diversified fabrication key (CFd) prerecorded in the card and calculated by the security module (MSC1) from a base fabrication key (CF).

12. Method according to claim 11, characterised in that the base key (CF) of the diversified fabrication keys prerecorded in the user cards is transmitted to the security module of the central processing unit, in coded form (CFc), the loading module containing a coding algorithm involving this base key (CF) of the prerecorded diversified keys, as well as the first transfer key (Ctd1) calculated by the loading module and present in the security module (MSC1) of the central processing unit.

13. Method according to any of claims 6, 8, 10, character-

ised in that the first and second diversified transfer keys are respectively prerecorded in the security module (MSC1) of the central processing unit and in the security module (MST1) of the terminal.

14. Application of the method according to any of claims 1 to 13 to a network consisting of a central processing unit (C1) and at least one terminal (T1) each comprising at least one security module (MSC1, MST1), characterised in that, prior to installation of the security modules of the network, a given diversified transfer key corresponding to a loading module is recorded in each of them.

15. Application according to claim 14, characterised in that the network cooperating with user cards (U1), in each of them is recorded, prior to putting it into operation, at least one diversified opening key (Cod).