OPIC
Office de la propriété intellectuelle du Canada

CIPO
Canadian Intellectual Property Office

(12) (19) (CA) **Demande-Application**

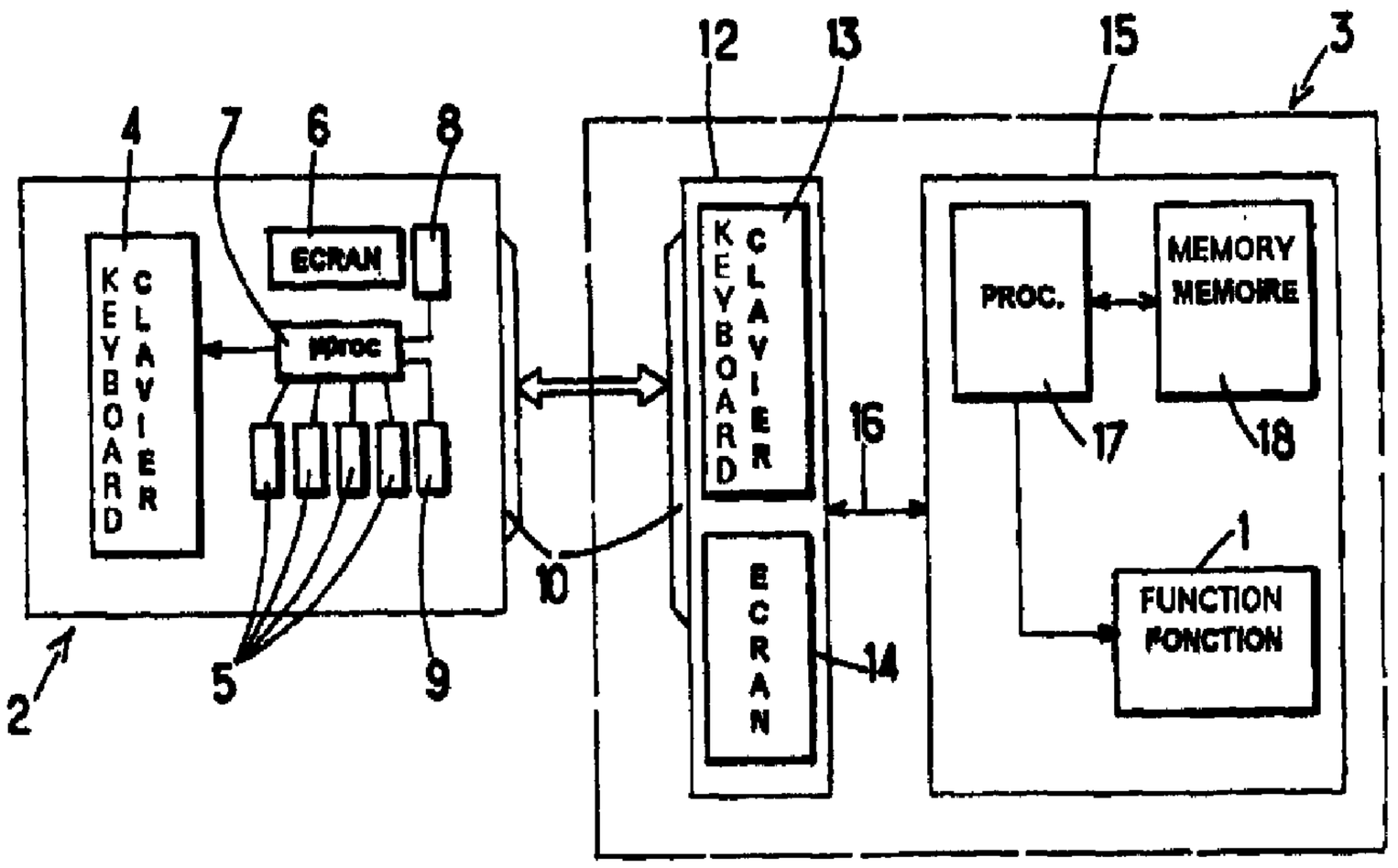
(21) (A1) **2,300,933**
(86) 1998/08/19
(87) 1999/03/04

(72) AUDEBERT, YVES LOUIS GABRIEL, US
(71) ACTIVCARD, FR

(51) Int.Cl.[7] G07F 7/10
(30) 1997/08/21 (97/10548) FR

(54) **DISPOSITIF PORTABLE ELECTRONIQUE POUR SYSTEME DE COMMUNICATION SECURISEE, ET PROCEDE D'INITIALISATION DE SES PARAMETRES**

(54) **PORTABLE ELECTRONIC DEVICE FOR SAFE COMMUNICATION SYSTEM, AND METHOD FOR INITIALISING ITS PARAMETERS**



(57) Ce dispositif portable électronique sécurisé de communication avec au moins une unité électronique comprend des moyens de mémorisation de données (8, 9), des moyens (10) d'interface avec au moins un outil extérieur pour charger des données dans lesdits moyens de mémorisation, et des moyens de traitement de données (7) comprenant des moyens d'initialisation pour permettre, en réponse à l'application d'un code secret d'accès en personnalisation, la modification dudit code d'accès et le chargement de données de personnalisation dans lesdits moyens de mémorisation. Ce dispositif comprend une pluralité de fonctions et de codes secrets

(57) The invention concerns a portable electronic device for safe communication with at least one electronic unit comprising means for data storage (8, 9), means (10) interfacing with at least an external tool for loading data in said storage means, and means for data processing (7) including initialisation means for enabling, in response to the application of a secret personalization access code, to modify said access code and personalization data loading into said storage means. Said device comprises a plurality of functions and particular re-programmable secret access codes different from one another (K_{PERX}, K_{PERY}) and each assigned to personalizing a particular

OPIC
Office de la propriété intellectuelle du Canada

CIPO
Canadian Intellectual Property Office

(21) (A1) **2,300,933**
(86) 1998/08/19
(87) 1999/03/04

d'accès particuliers reprogrammables différents les uns des autres (K_{PERX}, K_{PERY}) et affectés chacun à la personnalisation d'une fonction particulière (X, Y, ...) dudit dispositif, et des moyens d'inhibition (7; 222) adaptés pour n'autoriser l'accès desdits moyens de traitement au chargement et/ou à la lecture de données de personnalisation particulières à une fonction qu'en réponse à l'application du code d'accès particulier affecté à ladite fonction.

function (X, Y...) of said device, and inhibiting means (7; 222) adapted for authorising said processing means access to loading and/or reading personalization data particular to a function only in response to the application of the access code assigned to said function.

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

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

(51) Classification internationale des brevets 6 : G07F 7/10

A1

(11) Numéro de publication internationale: **WO 99/10848**

(43) Date de publication internationale: 4 mars 1999 (04.03.99)

(21) Numéro de la demande internationale: PCT/FR98/01820

(22) Date de dépôt international: 19 août 1998 (19.08.98)

(30) Données relatives à la priorité:
97/10548 21 août 1997 (21.08.97) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: ACTIVCARD [FR/FR]; 24–28, avenue du Général de Gaulle, F–92156 Suresnes Cedex (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(US seulement)*: AUDEBERT, Yves, Louis, Gabriel [FR/FR]; 2, allée Jehan–le–Jeune, F–78290 Croissy–sur–Seine (FR).

(74) Mandataire: CABINET DE BOISSE ET COLAS; 37, avenue Franklin D. Roosevelt, F–75008 Paris (FR).

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

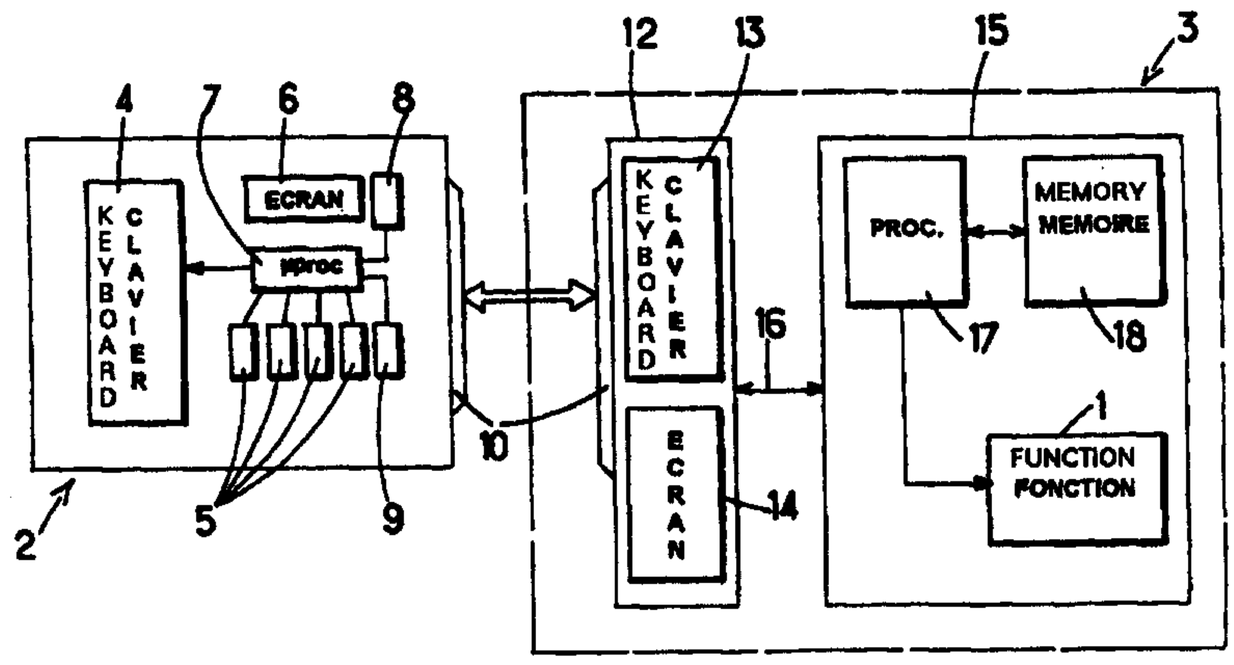
Publiée
Avec rapport de recherche internationale.
Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues.

(54) Title: PORTABLE ELECTRONIC DEVICE FOR SAFE COMMUNICATION SYSTEM, AND METHOD FOR INITIALISING ITS PARAMETERS

(54) Titre: DISPOSITIF PORTABLE ELECTRONIQUE POUR SYSTEME DE COMMUNICATION SECURISEE, ET PROCEDE D'INITIALISATION DE SES PARAMETRES

(57) Abstract

The invention concerns a portable electronic device for safe communication with at least one electronic unit comprising means for data storage (8, 9), means (10) interfacing with at least an external tool for loading data in said storage means, and means for data processing (7) including initialisation means for enabling, in response to the application of a secret personalization access code, to modify said access code and personalization data loading into said storage means. Said device comprises a plurality of functions and particular re–programmable secret access codes different from one another (K_{PERX}, K_{PERY}) and each assigned to personalizing a particular function (X, Y...) of said device, and inhibiting means (7; 222) adapted for authorising said processing means access to loading and/or reading personalization data particular to a function only in response to the application of the access code assigned to said function.



6,14... DISPLAY
7... MICROPROCESSOR
15... PROCESSOR

Portable electronic device for safe communication system, and method for initializing its parameters.

The present invention relates generally to secure electronic communication systems and more particularly to systems of this kind in which portable secure electronic devices are used to set up a call or communication to and/or to access another electronic unit.

Many electronic communication systems require access of users to particular applications to be controlled, such control generally entailing authenticating persons and/or messages. This is the case in particular when it is a question of controlling access to a computer or more generally a data processing network whose use is reserved to duly authorized persons. Such networks can be used, for example, to provide all kinds of services involving a transaction, usually with an economic consideration, such as telepurchasing, pay-per-view television, home banking, interactive video games, etc.

Access control systems of this kind are described in particular in documents US-A-3 806 874, US-A-4 601 011, US-A-4 720 860, US-A-4 800 590 and US-A-5 060 263. The systems described in the above documents use a portable secure electronic device which generates a password by encrypting a variable. A verification unit performs the same calculation or a similar calculation on the same or approximately the same variable and authorizes access to the requested application if the passwords generated in the portable device and the verification unit match. The variable can be a random or pseudo-random number, referred to hereinafter as a die, transmitted from the verification unit to the portable device, or it can be generated independently in the portable device and in the verification unit by means of a clock and/or an event counter, for example.

If the encryption process used in the portable device and the verification unit uses a symmetrical algorithm and a secret key, for example the DES (Data Encryption Standard) algorithm, the security of the system relies on the preservation of the secret character of the key stored both in the portable device and in the verification unit.

In some cases, the key can be static, i.e. it retains the same value throughout the service life of the portable device.

In other cases, the key can be dynamic, i.e. it changes in time as a function of the content of a counter incremented by a clock signal and/or an event counter, for example.

Whether the key is static or dynamic, it must initially, i.e. when the device is personalized, have a particular value which is stored both in the portable electronic device and in a database associated with the verification unit. When a user requests access, he or she must one way or another, for example using a public identification number or a personal identification number (PIN), identify himself or herself to the verification unit which obtains from the database the static key or, in the case of a dynamic key, the information that may be needed to calculate the current key.

Security problems of a similar kind arise in secure electronic communication systems using portable electronic devices and verification units employing encryption and decryption by means of asymmetric algorithms with public and private keys. The mechanisms used by an algorithm of the above kind (authentication, signature, etc) are such that the secret character of one or more of the keys stored in the devices and/or the verification units must be conserved.

During the personalizing process the key(s) and

other secret personalizing data are loaded into memory in the device by the entity which supplies the device to the end user. Protecting the personalizing data by enabling the supplier of a smart card to substitute a new master key controlling access to the personalizing data for the initial key installed by the card manufacturer is well known in the art, in particular from document WO 93/10509.

What is more, the rapid expansion of secure electronic communication systems is leading to the design of products for implementing a number of different applications and having a number of different security levels for the same application. The problem then arises of guaranteeing the independence of the applications and the associated security levels, i.e. the various functions implemented by the device.

One object of the invention is to provide a secure portable electronic device for communication with another electronic unit which is capable of assuring this independence of the functions.

To this end, the invention concerns a device of the above kind including data storage means, interface means with at least one external tool for loading data into said storage means, data processing means including initialization means for enabling, in response to the application of a secret personalizing access code, modification of said access code and loading of personalizing data into said storage means, characterized in that said device is adapted to use a plurality of functions and includes means for loading a plurality of particular secret data respectively representative of different particular access secret codes and each assigned to personalizing a particular function of said device, and inhibitor means adapted to authorize access of said processing means to loading and/or reading of personalizing data particular to a function only in response to

application of the particular access code assigned to said function.

According to one feature of the invention said inhibitor means are adapted to prohibit read mode access to any of said secret data.

According to another feature of the invention said loading means include at least one specific reprogrammable secret datum representative of a specific secret code common to all of said functions and in that said inhibitor means are adapted to prohibit access of said processing means to said particular personalizing data by way of said specific secret code.

According to another feature of the invention said data processing means are adapted to authorize modification of a secret datum representative of an access code particular to a function and loaded into said storage means via said specific access secret code in response to the application of said particular access code.

According to another feature of the invention said loading means are adapted to authorize, by means of said specific reprogrammable secret data, the deletion of particular secret data and of particular personalizing data previously loaded and the loading of new particular secret data.

Said specific secret code is preferably an access code to personalization of personalizing data common to all said functions of the device.

According to other features of the invention, taken in isolation or in combination:

- said storage means include at least one non-volatile memory in which a basic secret key is stored and said initialization means include first means for calculating an initial value of said specific secret data as a function of said basic secret key and an initial secret parameter;

- said inhibitor means are adapted to delete from said storage means one of said secret data representative of an access code in response to the loading, by means of said access code, of a new secret datum representative of a new access code;

- said secret datum is a secret key for calculating a code for verifying the access code of which said datum is representative;

- said processing means include second means for calculating said verification code by encrypting a variable by means of said calculation secret key;

- said personalizing data include at least one plurality of authentication secret keys which are different from each other and each of which is assigned to one of said functions and in that said processing means include third means for calculating an authentication code vis-à-vis a verification unit as a function of one of said authentication secret keys.

The invention also provides a method of initializing a device as defined hereinabove, characterized in that it includes:

- an initialization first step consisting in defining and storing in said storage means a personalizing key specific to said device,

- a personalizing second step consisting in loading into said storage means, by means of a specific access code dependent on said specific personalizing key, personalizing data common to said functions and secret keys for calculating said particular access secret codes each assigned to loading personalizing data relative to one of said functions, and

- a personalizing third step consisting in, for each of said functions, loading the personalizing data relating to said function into said storage means by means of the corresponding particular access secret code.

Said third step preferably includes a step consisting in, when loading personalizing data relative to at least one of said functions, modifying said secret key for calculating said particular access secret code assigned to said function.

According to one feature of the invention the initialization first step includes:

- at least one initialization first phase consisting in defining at least one secret datum common to a set of devices intended for the same entity,
- at least one second initialization phase including the steps of, for each device of said set:

a) reading a specific identification datum carried by said device,

b) calculating a first specific personalizing key as a function of said common secret datum and said identification datum,

c) storing said identification data and said first specific personalizing key in said storage means, and

- at least one initialization third phase including the following steps, for each device of said set:

d) extracting said specific identification datum from said device,

e) calculating in a first external tool said first specific personalizing key as a function of said common secret datum and said specific identification datum,

f) calculating in said external tool a first access code as a function of said specific personalizing key and a challenge transmitted by said device,

g) transmitting from said first tool to said device said first access code with personalizing parameters including a second personalizing key different from said first personalizing key,

h) calculating in said device a code for verifying said first access code as a function of said first specific personalizing key and said challenge,

i) comparing in said device said first access code and said verification code and, in response to a match of said codes:

j) storing said personalizing parameters in said storage means, and

k) substituting said second personalizing key for said first personalizing key in said storage means.

According to an embodiment of the invention said method is characterized in that it includes a fourth phase consisting in initially storing a common base secret key in a permanent memory of said storage means and in that steps a) and b) consist in:

- applying said secret datum and said base key to a second external tool,
- reading said identification datum by means of said second tool,
- calculating said specific personalizing key by means of said second tool,
- encrypting said specific personalizing key by means of said common base key in said second external tool,
- transmitting the result of said encryption from said second tool to said device, and
- decrypting said result in said device by means of said base key to reconstitute said specific personalizing key.

According to another embodiment of the invention said method is characterized in that it includes a fourth phase consisting in initially storing a common base key in a permanent memory of said storage means, in that said first phase equally consists in encrypting said common secret datum by means of said common base key and applying

the result of said encryption to a second external tool, and in that said second phase equally consists in:

a) reading said specific identification datum by means of said second tool and transmitting said identification datum and the result of said encryption to said device,

b) decrypting said result in said device by means of said base key to restore said common secret datum and thereafter calculating said specific personalizing key.

The invention also provides a secure communication system which includes a set of devices as defined hereinabove and at least one tool for initializing personalizing parameters for use of said third phase of the method defined hereinabove.

According to one feature of the invention said system further includes a tool for initializing production parameters for use of said second phase of the method defined hereinabove.

Finally, the invention also provides a secure communication system which includes a set of devices including means as defined hereinabove for implementing authentication mechanisms and at least one verification unit.

Other features and advantages of the invention will emerge from the following description of embodiments of the invention given by way of example and illustrated by the accompanying drawings, in which:

figure 1 is a general block diagram of a secure communication system in accordance with the invention applied to access control;

figure 2 is a diagram showing mechanisms for initializing parameters of the portable electronic device which is part of the system from figure 1 during production;

figure 3 is a diagram showing a variant of the

mechanisms for initializing parameters of the portable electronic device which is part of the system from figure 1 during production;

figure 4 is a diagram showing mechanisms for initializing personalizing parameters of the portable electronic device which is part of the system from figure 1; and

figure 5 is a general block diagram synthesizing the various phases of initializing the portable electronic device which is part of the system from figure 1.

The access control system shown in figure 1 allows conditional access to an application symbolized by the rectangle 1. The term "application" must be understood in a very wide sense. It refers to any application to which access is conditional on authorization involving authentication implying verification of the device (card) by means of which the request is formulated, and preferably also identification of the person requesting access to the application, to determine if the request is legitimate.

The application can be of any kind, for example control of access to premises, to a data processing network or to a computer, execution of a pecuniary or other transaction (telepurchase, home banking, interactive video games, pay-per-view television, etc). Moreover, the authentication of persons and/or messages (electronic signature) is explicitly included within the scope of the present invention.

In the embodiment shown in figure 1, the access control system includes a first portable unit 2 referred to hereinafter as a "card" and at least one second verification unit 3. The access control system in accordance with the invention can include a large number of cards 2 and one or more verification units 3, but in all cases a number that is generally smaller. The numbers of cards 2 and units 3 are in no way limiting on the

invention.

The card 2 is in the form of a pocket calculator or credit card, for example, and includes a keypad 4 for entering information, for example a personal identification number PIN, and various function keys 5. It also includes a display screen 6, for example a liquid crystal display screen, and an integrated electronic circuit including a programmed microcontroller 7, non-volatile read-only memory (ROM) 8 and reprogrammable memory 9 consisting of random access memory (RAM) and possibly electrically erasable programmable read-only memory (EEPROM). The non-volatile memory 8, the reprogrammable memory 9 and the data bus and the address bus of the microcontroller 7 are inaccessible from outside the card to make it impossible to read or modify information contained in the memories 8 and 9 fraudulently from outside the card.

The non-volatile memory (ROM) area 8 includes a program area and a data area.

The program area includes program instructions relating to the implementation of the following mechanisms:

1. Security mechanisms
    - carrier identification
    - authentication of carrier by verification unit
    - authentication of verification unit and personalizing unit
    - authentication of message
    - encryption/decryption
    - possible electronic signature
    - etc.
2. Personalizing mechanisms
    - in production
    - at time of various personalizing operations by client(s)
3. Mechanisms relating to card application(s)
4. Communication mechanism

- communication with user: display, keypad
- communication with verification or personalizing unit
    * infrared
    * DTMF
    * communication with a reader
    - communication with a smart card
    - etc.

The data area includes data common to a fabrication mask:

1. ROM key (K_{ROM})
2. software version number
3. etc.

The reprogrammable memory (RAM and possibly EEPROM) area 9 stores the following information:

1. Data entered during the various phases of initializing production parameters and personalizing parameters:

The data is structured according to the security levels and the applications and modification of a data area is conditional on authentication of the entity requesting personalizing: access code as a function of a challenge generated by the card, signature, etc.

This data can be secret (secret keys) or read-only data, and includes:

* personalizing secret keys
* secret keys relating to security mechanisms: entity authentication, message authentication, challenge generation
* data relating to application: content of messages, types of security mechanism required, etc.
* data relating to use of card in a given application: required length of personal identification number (PIN), challenge length, access code format, etc.
* data common to all applications: PIN value, clock value, counter values, content of standard messages.

2. Working data

The card 2 can include a communication system 10 for communicating with the verification unit 3 or with a production tool or a personalizing tool, as described below, either directly or via a transmission link of greater or lesser length. The communication system 10 can take various forms, for example a bidirectional cable link, a bidirectional DTMF telephone link, a bidirectional infrared link, a bidirectional "connected mode" link in which the card is inserted into an appropriate reader, optical reception means associated, in the unit 3, with means for reading information displayed on the screen 6, as described for example in document EP-A-0 399 897, or any other transmission system well known in the art.

Finally, an electrical power supply (not shown), for example a small electrical storage battery, is provided to power the various circuits of the card 2 and to render it autonomous.

The unit 3 includes interface means enabling it to communicate with the card 2 by means of the communication system 10. The interface means, symbolized by a rectangle 12, can take numerous forms, for example a dedicated reader, a computer terminal, a personal computer connected into a network, etc. The particular feature of the interface means 12 is that they enable communication with the associated card(s) 2 via the communication system 10.

The interface means 12 can also include a keypad 13 and a display screen 14 to enable a user to enter information to be communicated to a part 15 of the unit 3, for example passwords or data to be authenticated relating to the application 1. However, this data can be entered in other ways, in particular automatically, without manual intervention by the user, for example merely by inserting the card 2 into the interface 12 or by the emission of modulated infrared beams commanded by one of the function

keys 5.

The interface 12 communicates with a part 15 of the unit 3 referred to as the "server". This communication, symbolized by the connection 16, can be over a short distance or a long distance and use any appropriate means. The information carried by this connection includes the password to be checked in the server 15 and possibly data to be authenticated and used in the server.

The server 15 includes a processor 17 and a memory 18. The processor 17 is capable of conditionally releasing the applications 1 referred to in access requests formulated by the cards 2.

The microcontroller 7 of the card 2 is programmed to assure the security of the call in the widest sense, in conjunction with the verification unit 3, for example authentication of a user holding the card 2, certification of messages, securing of transactions, etc. These authentication, certification, etc mechanisms are well known to the skilled person and will not be described in detail in this application. These mechanisms use encryption and/or decryption in the card 2 and/or in the unit 3 of one or more items of information by means of a public key and private key algorithm or a secret key algorithm, which keys are stored in the programmable memory 9 associated with the microcontroller 7 and/or in the memory 18 of the "server" 15.

In the following description, the invention uses secret key algorithms, but it must be understood that it is not limited to this type of algorithm.

For example, after the user has identified himself or herself to the verification unit, an authentication procedure using a secret key algorithm entails encrypting a variable in parallel in the card 2 and in the verification unit 3 by means of the algorithm and a shared secret key K_{SEA} and then comparing the two passwords A_{SEA} resulting

from the encryption of that variable, generally in the verification unit 3. In systems referred to as asynchronous systems the variable is a random number (challenge) generated by the verification unit 3 and transmitted to the card 2. In systems referred to as synchronous systems the variable is dynamic, i.e. it is a number which changes in the card 2 and the unit 3 as a function of the content of a clock counter and/or an event counter. Synchronous systems presuppose, subject to a particular tolerance, a match between the contents of the clock counters and/or event counters of the card 2 and the content at the address associated with the card 2 of a database which is part of the verification unit 3 or to which the latter unit has access for implementing the authentication process. Detailed examples of these authentication mechanisms are given in document EP-A-0 338 936 and in French patent application No. 96 04797 filed 17 April 1996, for example, which may be referred to for more information.

As previously indicated, the secret encryption and/or decryption key(s) stored in the card 2 and the server 15 can be static, i.e. they can retain the same value throughout the service life of the product, or dynamic, i.e. their value can change with time. The value of the dynamic keys can itself be a function of the content of the clock and/or event counters, as described for example in French patent application No. 96 04798 filed 17 April 1996.

Whether the key is a static key or a dynamic key, it is necessary during the phase of initializing the production parameters or personalizing parameters of the card 2 to load into the programmable memory 9 thereof an initial value that will constitute the static key, the initial dynamic key or a root enabling the initial dynamic key to be calculated. In a system including a large number of cards, for example several thousand to several tens of

thousands, administering one or more secret keys specific to each card and different from those of all the other cards causes security problems. It is desirable for the end user of the card to be assured that the security offered by the card cannot be compromised by programming operations performed on the upstream side by the entity or entities responsible for initializing the production parameters and/or personalizing parameters of the card.

These security problems are accentuated by the current expansion of secure communication systems which must be able to respond to requirements related to the multiplicity of applications and the multiplicity of security levels for an application. For example, for a security system of given configuration, i.e. a set of cards and associated software installed in the cards 2 and the verification units 3 in order to perform particular functions, the same card can be used for different applications, for example authentication vis-à-vis a data processing or similar network to obtain access to one or more resources of that network (access to each resource may require separate authentication), telepurchasing, etc. Moreover, there may be several security levels for the same application, for example according to different categories of users, with the result that the cards have to be personalized according to their end user.

The multiplicity of applications for the same security system and of security levels for the same application, combined with the various phases of the life of the system between its manufacture and its supply to the end user, means that there can be for the same system, simultaneously or not, a plurality of administrators responsible for administering security problems.

Considering a simple case in which the security system includes only one application, a card can circulate during its life cycle between a number of entities, namely:

- the manufacturer or the supplier who sells the security system to the client;

- a general administrator, who can be the security manager of the client, which can have several geographical sites, each site having its own security system administration organization, independent of that of other sites;

- local administrators each responsible for the organization of the security system of the business at the level of one geographic site; and

- end users each of whom will hold a card 2 and use it on one or more particular geographical sites.

Once a batch of cards has been sold to a client by the supplier or the manufacturer, administering a system of this kind presupposes that only the general administrator can use the batch of cards and that another client cannot use them. Thus:

- on the one hand, the manufacturer or the supplier must during production initialize a number of parameters common to a batch of cards for a given client who alone will be able to initialize his personalizing parameters in the cards; and

- personalization by the client must be irreversible: once the general administrator has personalized the cards, they must no longer be usable by the supplier or the manufacturer.

Once in possession of the batch of cards the general administrator initializes all the personalizing parameters common to all the sites in the cards. The cards are then distributed to various sites on each of which a local administrator initializes the personalizing parameters specific to the site concerned. If cards have to be used and recognized on more than one site, they are handed over to a first local administrator for initializing the personalizing parameters of the first site, then to a

second local administrator for initializing the personalizing parameters of the second site, and so on. In this context, it is necessary to assure the independence of the administration means, in other words:

- a local administrator X must be able to initialize only the personalizing parameters of site X: being able to initialize the personalizing parameters of site X does not make it possible to initialize the personalizing parameters of site Y or to know the personalizing parameters of site Y; and
- to assure that administration at each site is autonomous, being the general administrator must not imply a knowledge of the personalizing parameters of the various sites.

These various functions are implemented by means of mechanisms for initializing production parameters and personalizing parameters described next with reference to figures 2 to 4.

Figure 2 is a diagram showing in-production mechanisms for initializing data or parameters, referred to hereinafter as production parameters, which are common to a batch of cards for a given client. In the figure, the lefthand column shows the operations performed by the supplier of the card, i.e. the entity which is responsible for supplying the security system to the client. The middle column shows the operations performed by a tool 20 for manufacturing the cards 2, the manufacturer being the same entity as the supplier or not. Finally, the righthand column shows the operations implemented in the card 2. The production tool 20 used by the manufacturer includes conventional hardware and software that there is no need to describe here and which are used, among other things, to generate data and to transmit it to the cards 2 to program their programmable memory 9.

The lefthand column in figure 2 shows a number of

secret keys K_{ROM}, K_{PEM}, K_{ALE} and K_{MES} which are common to an entire batch of cards for a given client.

The key K_{ROM} is defined by the supplier and is known only to the supplier. The key K_{ROM} is installed in the permanent read-only memory 8 of the cards when masking the integrated circuits but is not known to the manufacturer of the cards 2 if this is not the same entity as the supplier. To this end, it can be embedded in encrypted form in the software controlling the card production tool, for example.

The supplier also chooses the keys K_{PEM}, K_{ALE} and K_{MES} and enters them in encrypted form in the software controlling the production tool. The values of these three keys are communicated confidentially to the client, preferably separately from the batch of cards. The key K_{PEM} is a master personalizing key which, as described below, is used to generate a personalizing key specific to each card according to its serial number. The key K_{ALE} is a key enabling the cards to generate challenges and the key K_{MES} is a key enabling an alphabet and messages to be loaded into the cards.

As shown in the centre column in figure 2, the production tool 20 reads the serial number NS associated with a given card and an algorithm submits the number NS to an encryption operation E using the master personalizing key K_{PEM} (block 100). The result of this encryption is a specific personalizing key K_{PER} which is specific to the card and is submitted by means of an algorithm and the key K_{ROM} (block 101) to an inverse operation E-1 to produce a datum $E(K_{PER})$. The key K_{PER} is used in blocks 102 and 103 to generate data $E(K_{MES})$ and $E(K_{ALE})$ from the keys K_{MES} and K_{ALE}, respectively, using the inverse operation E-1. In the foregoing description, and in the subsequent description, if $B = E[K_X](A)$ is the result of the encryption E of a datum A by means of a key K_X, E-1 represents the inverse

operation A = E - 1[K_X](B) enabling the datum A to be obtained at the output, by means of the key K_X, by applying to the input the key for encrypting the datum B.

For a given card 2, the production parameters (block 104) include the serial number NS, the output data of blocks 101, 102 and 103 and the status of an internal clock counter of the production tool enabling initialization of a clock counter of the card 2, in particular if the system uses dynamic keys and/or variables.

After the parameters have been reset to zero and the internal parameters of the card 2 concerned have been initialized, the card waits to receive a production frame (block 105). In step 106 the card 2 receives the production frame consisting of the data previously listed (block 104). By means of the software programmed into it, the microcontroller 7 then calculates (block 107) the key K_{PER} from the datum E(K_{PER}) and the key K_{ROM}, using operation E. It also uses operation E to calculate (block 108) the key K_{MES} from the datum E(K_{MES}) and the key K_{PER} and (block 109) the key K_{ALE} from the datum E(K_{ALE}) and the key K_{PER}.

In step 110 the serial number NS and the keys K_{PER}, K_{ALE} and K_{MES} are stored in memory and the card is ready to be sent to a client to be personalized.

In the process described above, it is sufficient to know the format of the production frame (block 104) to load parameters into a card because this operation does not require an access code. However, a pirate in possession of the format of the production frame would nevertheless be unable to personalize and use the card because he or she would not know the key K_{ROM}.

Figure 3 shows a variant of the process for initializing the production parameters which has the advantage of not introducing the keys K_{ROM} and K_{PEM} into the software for initializing the production parameters of

the production tool 20. To this end, by means of its own software, the supplier (lefthand column) calculates the data $E(K_{PER})$, $E(K_{MES})$ and $E(K_{ALE})$ from the data K_{PER}, K_{MES} and K_{ALE} respectively, and the key K_{ROM}. After calculating this data by an operation E-1 (blocks 111, 112 and 113), the supplier introduces the data into the software for initializing the production parameters of the production tool (step 114).

After the tool 20 has read the serial number of the card concerned (step 115) and the parameters have been reset to zero and the internal parameters of the card have been initialized (step 116), the production tool 20 transmits the production parameters to the card (step 117): these parameters are the serial number NS, the data $E\text{-}1(K_{PER})$, $E\text{-}1(K_{MES})$ and $E\text{-}1(K_{ALE})$, and the status of the internal clock counter. After receiving the corresponding frame (step 118), the microcontroller 6 uses operation E to calculate the key K_{PEM} from the datum $E(K_{PEM})$ and the key K_{ROM} (step 119). It then calculates the personalizing key K_{PER} specific to the card using operation E, the data NS and the master personalizing key K_{PEM} (step 120). Finally, the microcontroller 7 uses operation E to calculate the keys K_{ALE} and K_{MES} from the data $E(K_{ALE})$ and $E(K_{MES})$, respectively, and the key K_{ROM} stored in the permanent memory 8 of the card (steps 121 and 122). In step 123 the data NS, K_{PER}, K_{ALE} and K_{MES} is stored in the programmable memory 9 of the card 2. This data is the same as that obtained by the process of initializing the production parameters described with reference to figure 2.

When the production parameters of a batch of cards from a given client have been initialized in this way, they are shipped to the client. The keys common to this batch, namely the master personalizing key K_{PEM}, the key K_{ALE} for generating challenges and the key K_{MES} for loading the alphabet and messages, are communicated confidentially to

the client. Each card holds in memory the keys K_{ALE} and K_{MES} which are common to the batch of cards and the key K_{PER} and the serial number NS specific to it.

Furthermore, each card 2 holds in memory a code or number identifying the version of the software mask-programmed into the integrated circuits of the card. The software version can vary from one batch of cards to another and within the same batch of cards for a given client there may be several groups of cards with different versions of the software on the basis of requirements expressed by the client as to the use of the cards. The code or number identifying each version of the software programmed in the cards shipped to the client is supplied to the client by the supplier. The client also has software for personalizing cards according to the version of the software programmed therein.

Figure 4 shows the process of personalizing the cards 2 by the client. The lefthand column represents the operations performed by a personalizing tool 30 and the righthand column shows the operations performed in the cards 2. The personalizing tool 30 has a structure similar to that of the verification unit 3, i.e. it includes means for communication with the cards 2, a data processor, memories containing in particular the software needed to personalize the cards according to the version of the software programmed therein, and a database containing the values of the keys K_{PEM}, K_{ALE} and K_{MES} and the personalizing parameters to be loaded into the cards 2 according to the version of the software programmed therein.

In figure 4, in step 200, the card is awaiting a call or communication opening frame from the personalizing tool. In step 201 the personalizing tool opens communication with the card to be personalized and sends the communication opening frame INIT-MAT. In step 202 the card receives the

communication opening frame INIT-MAT and sends the personalizing tool an identification frame IDENT-MAT including the code or number of the version of the software it contains. In step 203 the personalizing tool 30 receives the identification frame IDENT-MAT and the software version number is input to the database to read therein, among other things, the personalizing parameters to be loaded into the card. In step 204 the personalizing tool 30 sends a software initialization frame INIT-LOG which the card receives in step 205, and then proceeds to step 206.

In step 206 the card uses the operation E to calculate a challenge by means of the key K_{ALE} (block 207) and then the datum E(NS) by encrypting the serial number NS of the card using a key which is itself the result of encrypting by means of a logic function F the version number NL of the software using the challenge calculated in step 207. After these encryption operations 208 and 209, the card sends an identification frame IDENT-LOG containing the challenge and E(NS) (step 210). The personalizing tool 30 receives this frame in step 211 and, by means of an operation F in step 212 on the number NL using the challenge transmitted from the card and an operation E-1 in step 213 on E(NS) by means of the result of the operation effected in step 212, generates the serial number NS of the card. The serial number NS of the card being personalized is input to the database to enable the client to retain a table of personalizing data for each card. In step 214 the personalizing tool calculates the key K_{PER} specific to the card by an operation E of encrypting the serial number NS by means of the master personalizing key K_{PEM} which is supplied by the database of the tool 30. The tool then calculates (step 215) an authentication password A_{PO} (which constitutes the access code to personalizing the card) by an operation F which encrypts the challenge by means of the key K_{PER} : $A_{PO} = F[K_{PER}](Challenge)$.

In step 216, the personalizing tool constructs the personalizing data common to the card from the password calculated in step 215 and personalizing parameters received from the database. The common personalizing data includes personalizing command codes, the password A_{PO} authenticating the personalizing tool, a new secret personalizing key NK_{PER} specific to the card and to be substituted for the initial personalizing key K_{PER}, and various personalizing parameters, including, for example, one or more secret keys K_{SEA} for calculating the authentication password A_{SEA} vis-à-vis the verification unit 3 ($A_{PEA} = E[K_{SEA}](Challenge)$, and secondary or particular secret personalizing keys K_{PERX}, K_{PERY}, etc specific to each site X, Y, etc for which the card has to be personalized.

In step 217, the personalizing data is transmitted to the card in the form of several frames.

In step 218, the card receives the personalizing frames, verifies the personalizing command codes, stores the received data and sends an acknowledgement to the personalizing tool.

In step 219, the card calculates a code or password A_{PC} for verifying the authentication password A_{PO} by encrypting the challenge using the logic function F and the specific personalizing key K_{PER} stored in its memory in step 110 or 123: $A_{PC} = F[K_{PER}](Challenge)$.

In step 220, the card verifies that the authentication password A_{PO} received from the personalizing tool 30 is consistent with the verification password A_{PC} calculated by the card and, if so, stores the personalizing data in step 221: for example, consistency can consist in the fact that the two passwords are identical, as shown in figure 4, or that the two passwords are linked by another predetermined relationship.

Finally, in step 222 the card substitutes the new

personalizing key NK_{PER} received from the personalizing tool for the old key K_{PER}. The new key NK_{PER} is not known to the supplier, who is thereafter unable to access the personalizing data of the client. Read and/or write mode access to the personalizing data requires the personalizing tool to supply the card with a new authentication password $NAp_O = F[NK_{PER}](Challenge)$ consistent with the verification password NAp_C calculated in the card as explained with reference to step 219, NAp_O and NAp_C being calculated on the basis of a new challenge generated in the card and transmitted to the personalizing tool.

However, a knowledge of the common secret personalizing key NK_{PER} does not make it possible to read secondary personalizing secret keys K_{PERX}, K_{PERY}, etc loaded into the card in step 221, or any other secret key.

This is because the secret keys cannot be read because the program of the microcontroller 7 does not include any command for reading these parameters.

After step 222, the general administrator can transmit the cards to the local administrators of sites X, Y, etc., each of whom will be able, using respective secondary keys K_{PERX}, K_{PERY}, etc, and a process similar to that shown in figure 4, and which does not need to be described again in detail, to load the card with the personalizing parameters specific to the site for which he or she is responsible. To this end, the secondary key specific to personalizing the card for each site is communicated confidentially by the general administrator to the local administrator concerned.

Using the secondary key communicated to him or her, the local administrator loads the card with the personalizing data specific to the site concerned, for example an authentication key for calculating an authentication password vis-à-vis a verification unit of that site. Thus the local administrator of site X can load

an authentication key K_{SEAX}, the local administrator of site Y can load an authentication key K_{SEAY}, and so on. During the process of personalizing the card for a given site X, the local administrator can substitute a new secondary personalizing key NK_{PERX} for the secondary personalizing key K_{PERX} in the card received from the general administrator for the site concerned, as described with reference to figure 4. This will prevent general administrators having access in read and/or modify mode to the personalizing parameters of cards whose secondary personalizing key has been modified. Modifying the secondary keys also provides a seal between the various segments or functions of the card. Modifying the secondary keys K_{PERX}, K_{PERY}, etc (replaced by NK_{PERX}, NK_{PERY}, etc) protects against hacking with the aim of writing other secret data into the segments. The effect of this type of hacking is limited because it is not possible to read the secret data even if the corresponding secondary secret personalizing key is known. However, exclusive access to personalizing each segment is guaranteed, as is exclusive access to the common personalizing data with the key K_{PER}, NK_{PER}.

After the segments have been personalized by means of the secondary keys K_{PERX}, K_{PERY}, NK_{PERX}, NK_{PERY}, it is preferred that the key K_{PER}, NK_{PER} specific to the card enables them to be overwritten in order to perform a new process of initializing all the personalizing parameters of the card, if necessary. This facility can be useful in the event of an anomaly, to prevent the device being rendered permanently unusable.

However, in one variant, this possibility can be prohibited.

Figure 5 is a general flowchart showing the main phases of the program that executes in a card 2 provided with a plurality of segments which, after the common

personalizing parameters have been initialized, must be initialized with personalizing parameters that are specific to them in order to use the functions specific to each segment by means of the card.

The program starts in step 300 and in step 301 a test is performed to determine if this is the first start since a reset.

If so, the memory is reset to zero in step 302, after which a test is performed in step 303 to determine if a flag representative of initialization of the parameters during production (parameters initialized by the manufacturer) is active. If the response to the test in step 301 is negative, the next step is a test step 303.

If the response to test step 303 is negative, the program waits for initialization of the production parameters (step 304). The next step 305 corresponds to initialization of the production parameters in the card 2, as described with reference to figures 2 and 3. When this initialization has been completed, a flag is activated in step 306 and the program goes back to the entry of test step 303.

If the response to test step 303 is positive, i.e. if the production parameters have been initialized, the program runs a test step 307 to determine if a flag representative of initialization by the client of the common personalizing parameters is active. If not, the program waits for initialization of the common personalizing parameters (step 308). The next step 309 corresponds to initialization of the common personalizing parameters in the card 2, as described with reference to figure 4. The common personalizing parameters include the reprogrammable personalizing keys K_{PERX}, K_{PERY} specific to each segment or function. When this initialization has been completed, a flag is activated in step 310 and the program returns to the entry of test step 307.

If the response to test step 307 is positive, the program moves on to a test step 311 to determine if a flag representative of initialization of personalizing parameters specific or particular to the various segments of the card is active. If not, the program waits for initialization of the personalizing parameters particular to the segments (step 312). Step 313 corresponds to initialization in the card 2 of the personalizing parameters particular to the segments. For each segment, this initialization is subordinate to the supply to the card of a correct access code A_{PX}, A_{PY} dependent on the key K_{PERX}, K_{PERY} allocated to that segment and a challenge supplied by the card to the personalizing tool, as described with reference to figure 4. As appropriate, this initialization is performed by the general administrator or by the local administrators at the various geographical sites, as previously described. During this process of initializing the particular personalizing parameters, the responsible administrator can substitute a new particular personalizing key NK_{PERX}, NK_{PERY} for the initial personalizing key K_{PERX}, K_{PERY} for the segment concerned, which was loaded in step 309. Only the holder of the new key NK_{PERX}, NK_{PERY} can generate the new access code NA_{PX}, NA_{PY} and subsequently access (in read mode and/or in write mode, depending on how the processing means are programmed) the personalizing data particular to the corresponding segment and the holder of the specific personalizing key K_{PER} (or NK_{PER} if it has been modified) does not have access thereto if he or she does not know the new particular personalizing key.

When the initialization of the personalizing parameters of all the segments has been completed, a flag is activated in step 314, the response to test step 311 is positive and the program moves on to step 315 which represents access for the end user to the various functions

of the card implemented by the program of the card.

As previously indicated, the invention is not limited to the use of symmetrical algorithms using secret keys and applies equally if the mechanisms for initializing the parameters of the card use asymmetric algorithms employing public and private keys. In this case, the public key is stored in the card or device 2, the challenge is generated in the device 2 and the private key is stored in a personalizing tool or a smart card used by the personalizing tool.

However, using asymmetric algorithms does not allow derivation of keys since the concept of a mother key does not exist in this type of algorithm.

Also, it goes without saying that the embodiments described are merely examples and can be modified, in particular by substitution of equivalent technical means, without departing from the scope of the invention.

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. Portable electronic device for secure communication with at least one electronic unit for use of at least one function, including:

* data storage means,

* interface means with at least one external tool for loading data into said storage means,

* data processing means including initialization means for enabling, in response to the application of a secret personalizing access code specific to said device, modification of said specific access code and loading of personalizing data into said storage means,

characterized in that said device is adapted to use a plurality of functions (X, Y, etc) and includes:

* first means (7, 309) controlled by said specific access code (A_{PO}) for loading into said storage means (9) reprogrammable particular secret data (K_{PERX}, K_{PERY}, etc.) respectively representative of different particular secret personalizing access codes (A_{PX}, A_{PY}, etc) and each assigned to personalizing a particular function (X, Y, etc) of said device,

* second means (7, 313) controlled by said particular access codes (K_{PERX}, K_{PERY}, etc) for loading into said storage means (9) particular personalizing data (K_{SEAX}, K_{SEAY}, etc) assigned to the implementation of said functions (X, Y, etc) by said processing means (7), and

* inhibitor means (7; 313) adapted to authorize modification of any of said particular secret data (K_{PERX}, K_{PERY}, etc) consecutive upon its loading into said storage means and said loading of said personalizing data (K_{SEAX}, (K_{SEAY}, etc) particular to a function (X, Y, etc) only in response to the application of the particular secret personalizing access codes (A_{PX}, A_{PY}, etc) already assigned to said function (X, Y, etc).

2. Device according to claim 1, characterized in that said inhibitor means (7) are adapted to prohibit read mode access to any of said secret data (K_{PER}, K_{PERX}, K_{PERY}, etc).

3. Device according to claim 1 or claim 2, characterized in that said inhibitor means are adapted to prohibit read mode and write mode access by said processing means (7) to said particular personalizing data (K_{SEAX}, K_{SEAY}, etc) by means of said specific secret personalizing access code (A_{PO}, NA_{PO}).

4. Device according to any of claims 1 to 3, characterized in that said inhibitor means are adapted to prohibit read mode access to said particular personalizing data (K_{SEAX}, K_{SEAY}, etc) following the loading of said data by means of said particular secret personalizing access codes (K_{PERX}, K_{PERY}, NK_{PERX}, NK_{PERY}, etc) assigned to said functions (X, Y, etc).

5. Device according to any of claims 1 to 3, characterized in that said inhibitor means are adapted to authorize read mode access to personalizing data (K_{SEAX}, K_{SEAY}, etc) particular to a function (X, Y, etc) by means of the particular secret personalizing access code (A_{PX}, A_{PY}, NA_{PX}, NA_{PY}, etc) assigned to said function.

6. Device according to any of claims 1 to 6 , characterized in that said processing means (7) are adapted to authorize, by means of said specific secret personalizing access code (A_{PO}, NA_{PO}), the deletion of said particular secret data (K_{PERX}, K_{PERY}, etc) and of said particular personalizing data (K_{SEAX}, K_{SEAY}, etc) previously loaded into said storage means and the loading of new particular secret data (NK_{PERX}, NK_{PERY}, etc).

7. Device according to any of claims 1 to 6, characterized in that said specific secret personalizing access code (A_{PO}) is an access code for loading into said

storage means personalizing data (person-param) common to all said functions (X, Y, etc) of the device.

8. Device according to any of claims 1 to 7, characterized in that it includes third means (7, 305) for loading into said storage means a reprogrammable specific secret datum (K_{PER}) representative of said specific secret personalizing access code (A_{PO}), said initialization means (7, 200-222) being adapted to authorize the replacement of said specific secret datum (K_{PER}) by a new specific secret datum (NK_{PER}) representative of a new specific secret personalizing access code (NA_{PO}) only in response to the application to said processing means (7) of the specific access secret code (A_{PO}) imaging said specific secret datum (K_{PER}) to be replaced.

9. Device according to claim 8, characterized in that said storage means include at least one non-volatile memory (8) in which a base secret key (K_{ROM}) is stored and said initialization means (7) include first means (7, 107) for calculating an initial value of said specific secret datum (K_{PER}) as a function of said base secret key (K_{ROM}) and an initial secret parameter ($E(K_{PER})$; $E(K_{PEM})$).

10. Device according to any of claims 1 to 9, characterized in that said secret datum (K_{PER}, NK_{PER}) is a secret key for calculating a code (A_{PC}; NA_{PC}) for verifying the personalizing access code (A_{PO}; NA_{PO}) of which said datum is representative.

11. Device according to claim 10, characterized in that said processing means (7) include second means for calculating said verification code (A_{PC}, A_{PX}, A_{PY}) by encrypting a variable by means of said calculation secret key (K_{PER}, K_{PERX}, K_{PERY}, etc).

12. Device according to any of claims 1 to 11, characterized in that said personalizing data includes at least one plurality of authentication secret keys (K_{SEAX}, K_{SEAY}) which are different from each other and each of

which is assigned to one of said functions and in that said processing means (7) include third means for calculating an authentication code (A_{PEA}) vis-à-vis a verification unit (3) as a function of one of said authentication secret keys (K_{SEAX}, K_{SEAY}).

13. Method of initializing a device according to any of claims 1 to 12, characterized in that it includes:

- an initialization first step (100-110; 111-123) consisting in defining and storing in said storage means (9) a reprogrammable personalizing secret key (K_{PER}) specific to said device,

- a personalizing second step (201-222)consisting in loading into said storage means, by means of a specific access code (A_{PO}) dependent on said specific personalizing key (K_{PER}), personalizing data (person-param) common to said functions and particular reprogrammable secret keys (K_{PERX}, K_{PERY}) for calculating said particular access secret codes (A_{PX}, A_{PY}) each assigned to loading particular personalizing data relative to one of said functions (X, Y) and modifying said specific personalizing key (K_{PER}), and

- a personalizing third step (313) consisting in, for each of said functions (X, Y), loading the personalizing data (K_{SEAX}, K_{SEAY}) relating to said function into said storage means by means of the corresponding particular access secret code (A_{PX}, A_{PY}).

14. Method according to claim 13, characterized in that said third step includes a step consisting in, when loading particular personalizing data relative to at least one of said functions (X, Y), modifying said particular secret key (K_{PERX}, K_{PERY}) for calculating said particular access secret code (A_{PX}, A_{PY}) assigned to said function.

15. Method according to claim 13 or claim 14, characterized in that the initialization first step includes:

- at least one initialization first phase consisting in defining at least one secret datum (K_{PEM}; $E(K_{PEM})$) common to a set of devices intended for the same entity,
- at least one second initialization phase including the steps of, for each device of said set:

a) reading a specific identification datum (NS) carried by said device,

b) calculating a first specific personalizing key (K_{PER}) as a function of said common secret datum (K_{PEM}; $E(K_{PEM})$) and said identification datum (NS),

c) storing said identification data (NS) and said first specific personalizing key (K_{PER}) in said storage means (9).

16. Method according to claim 15, characterized in that said personalizing second step includes the following steps, for each device of said set:

a) extracting (209) said specific identification datum (NS) from said device (2),

b) calculating (214) in a first external tool (30) said first specific personalizing key (K_{PER}) as a function of said common secret datum (K_{PEM}) and said specific identification datum (NS),

c) calculating (215) in said external tool (30) a first specific access code (A_{PO}) as a function of said specific personalizing key (K_{PER}) and a challenge transmitted by said device,

d) transmitting (217) from said first tool to said device (2) said first specific access code (A_{PO}) with personalizing parameters including a second specific personalizing key (NK_{PER}) different from said first specific personalizing key (K_{PER}),

e) calculating (219) in said system a code (A_{PC}) for verifying said first access code (A_{PO}) as a

function of said first specific personalizing key (K_{PER}) and said challenge,

f) comparing (220) in said device said first specific access code (Ap_O) and said verification code (Ap_C) and, in response to a match of said codes:

g) storing (221) said personalizing parameters in said storage means (9), and

h) substituting (222) said second specific personalizing key (NK_{PER}) for said first specific personalizing key (K_{PER}) in said storage means (9).

17. Method according to claim 15 or claim 16, characterized in that said initializing first step includes a third phase consisting in initially storing a common base secret key (K_{ROM}) in a permanent memory (8) of said storage means and in that steps a) and b) of said initialization second phase consist in:

- applying said common secret datum (K_{PEM}) and said base key (K_{ROM}) to a second external tool (20),
- reading said identification datum (NS) by means of said second tool,
- calculating (100) said specific personalizing key (K_{PER}) by means of said second tool (20),
- encrypting (101) said specific personalizing key (K_{PER}) by means of said common base key (K_{ROM}) in said second external tool (20),
- transmitting (104) the result ($E(K_{PER})$) of said encryption from said second tool (20) to said device (2), and
- decrypting (107) said result ($E(K_{PER})$) in said system by means of said base key (K_{ROM}) to reconstitute said specific personalizing key (K_{PER}).

18. Method according to claim 15 or claim 16, characterized in that said initializing first step includes a third phase consisting in initially storing a common base

key (K_{ROM}) in a permanent memory (8) of said storage means, in that said first phase equally consists in encrypting (111) said common secret datum (K_{PEM}) by means of said common base key (K_{ROM}) and applying the result of said encryption ($E(K_{PEM})$) to a second external tool (20), and in that said second phase equally consists in:

a) reading (115) said specific identification datum (NS) by means of said second tool (20) and transmitting said identification datum (NS) and the result of said encryption ($E(K_{PEM})$) to said device,

b) decrypting (119) said result ($E(K_{PEM})$) in said device (2) by means of said base key (K_{ROM}) to restore said common secret datum (K_{PEM}) and thereafter calculating (120) said specific personalizing key (K_{PER}).

19. Secure communication system characterized in that it includes a set of devices according to any of claims 1 to 12 and at least one tool (30) for initializing personalizing parameters for loading into each of said devices:

* personalizing data (person-param) common to the various functions (X, Y) of said device,

* said particular personalizing data (K_{SEAX}, K_{SEAY}, etc), and

* said particular secret data (K_{PERX}, K_{PERY}, etc).

20. Secure communication system according to claim 19, characterized in that it further includes a tool (20) for the initial loading into each of said devices of a reprogrammable secret datum (K_{PER}) specific to each device and representative of said specific secret personalizing access code (Ap_O).

21. Secure communication system characterized in that it includes a set of devices according to claim 12 and at least one verification unit (3).

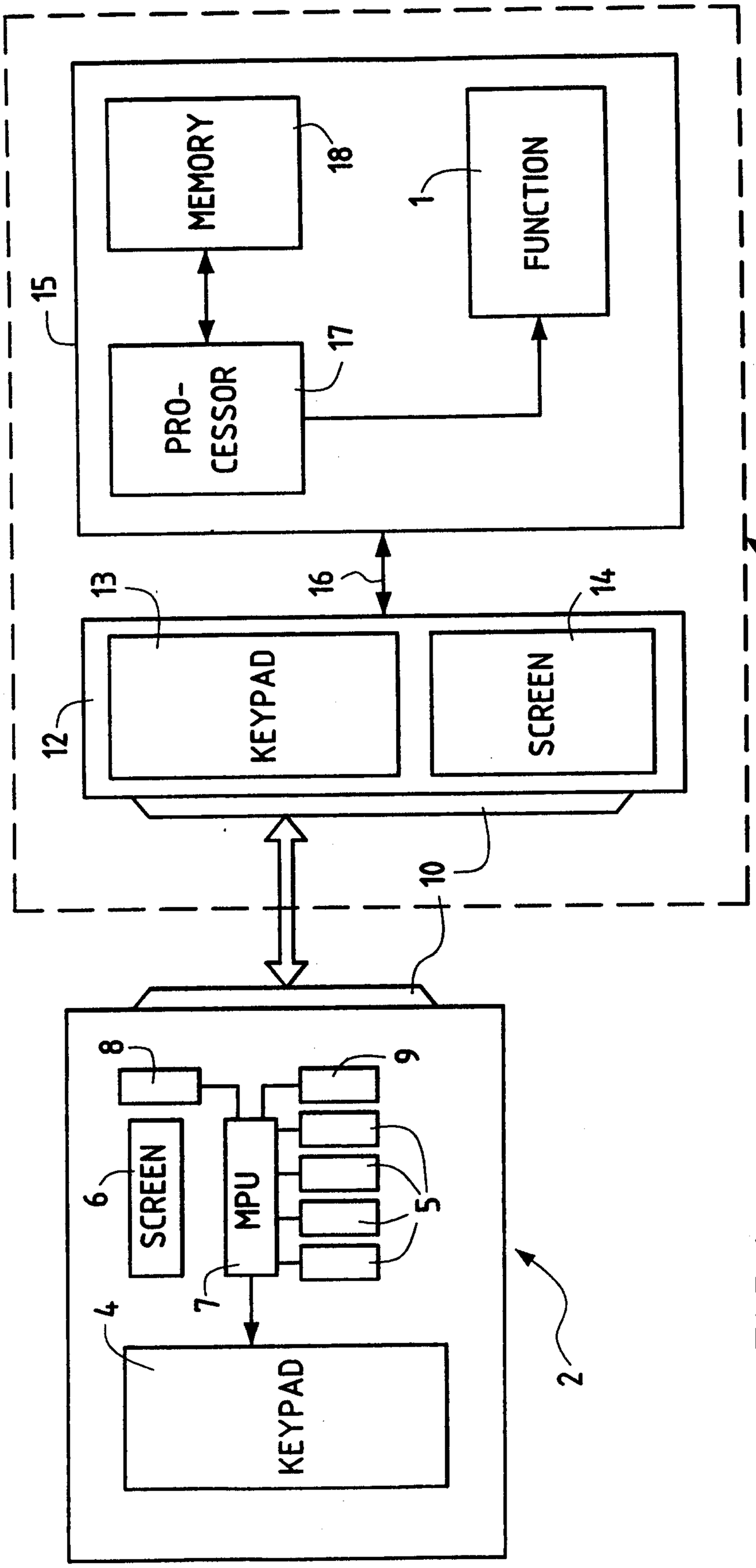


FIG.1

McFadden, Fincham

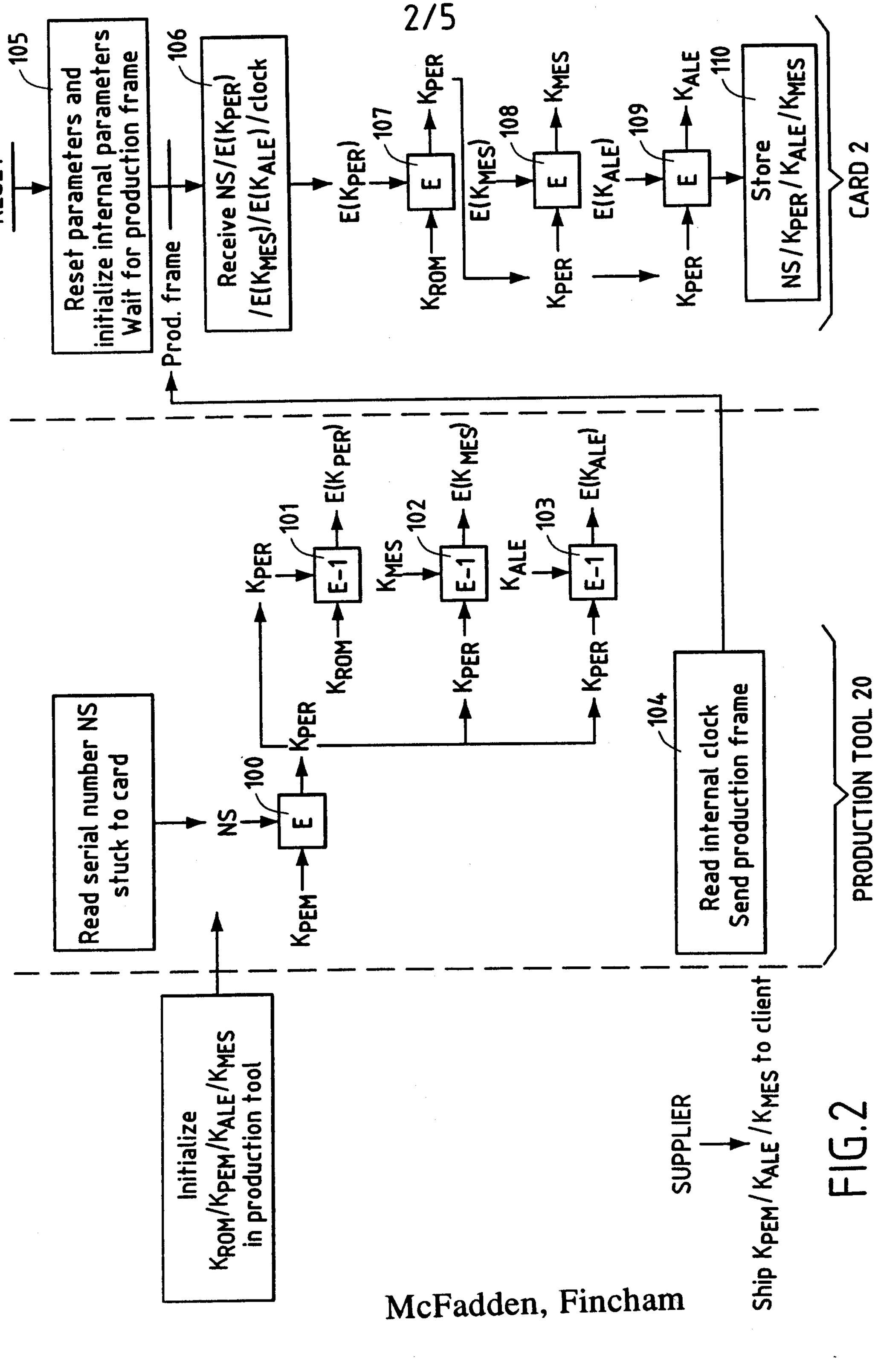

RESET
105
Reset parameters and initialize internal parameters
Wait for production frame
106
Prod. frame
Receive NS/E(KPER)/E(KMES)/E(KALE)/clock
E(KPER)
107
E
KPER
KROM
E(KMES)
108
E
KMES
KPER
E(KALE)
109
E
KALE
KPER
110
Store
NS/KPER/KALE/KMES
CARD 2
KPER
101
E-1
E(KPER)
KROM
KMES
102
E-1
E(KMES)
KPER
KALE
103
E-1
E(KALE)
KPER
KPER
Read serial number NS stuck to card
NS
100
E
KPER
KPEM
104
Read internal clock
Send production frame
PRODUCTION TOOL 20
Initialize KROM/KPEM/KALE/KMES in production tool
SUPPLIER
Ship KPEM/KALE/KMES to client

FIG.2

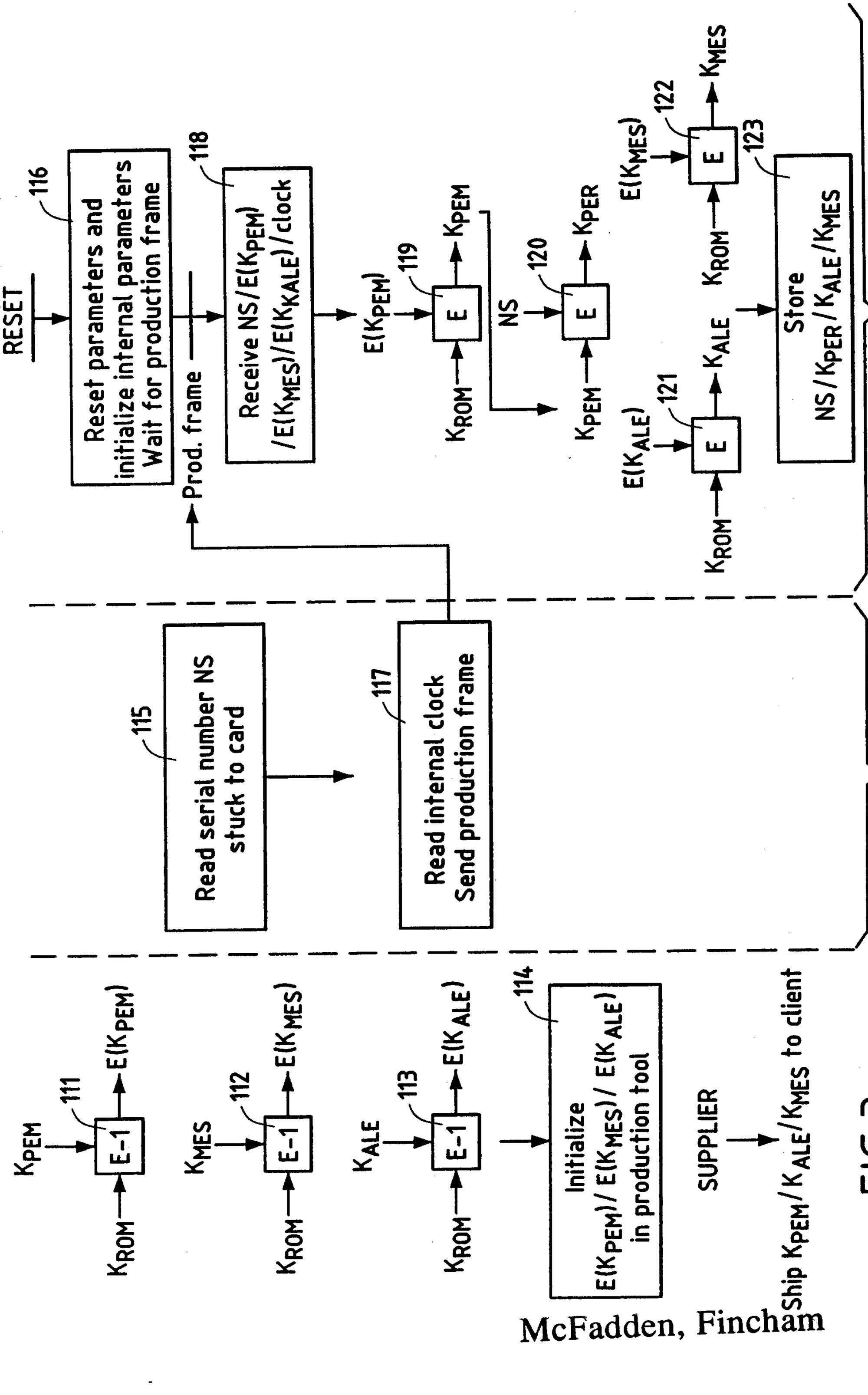
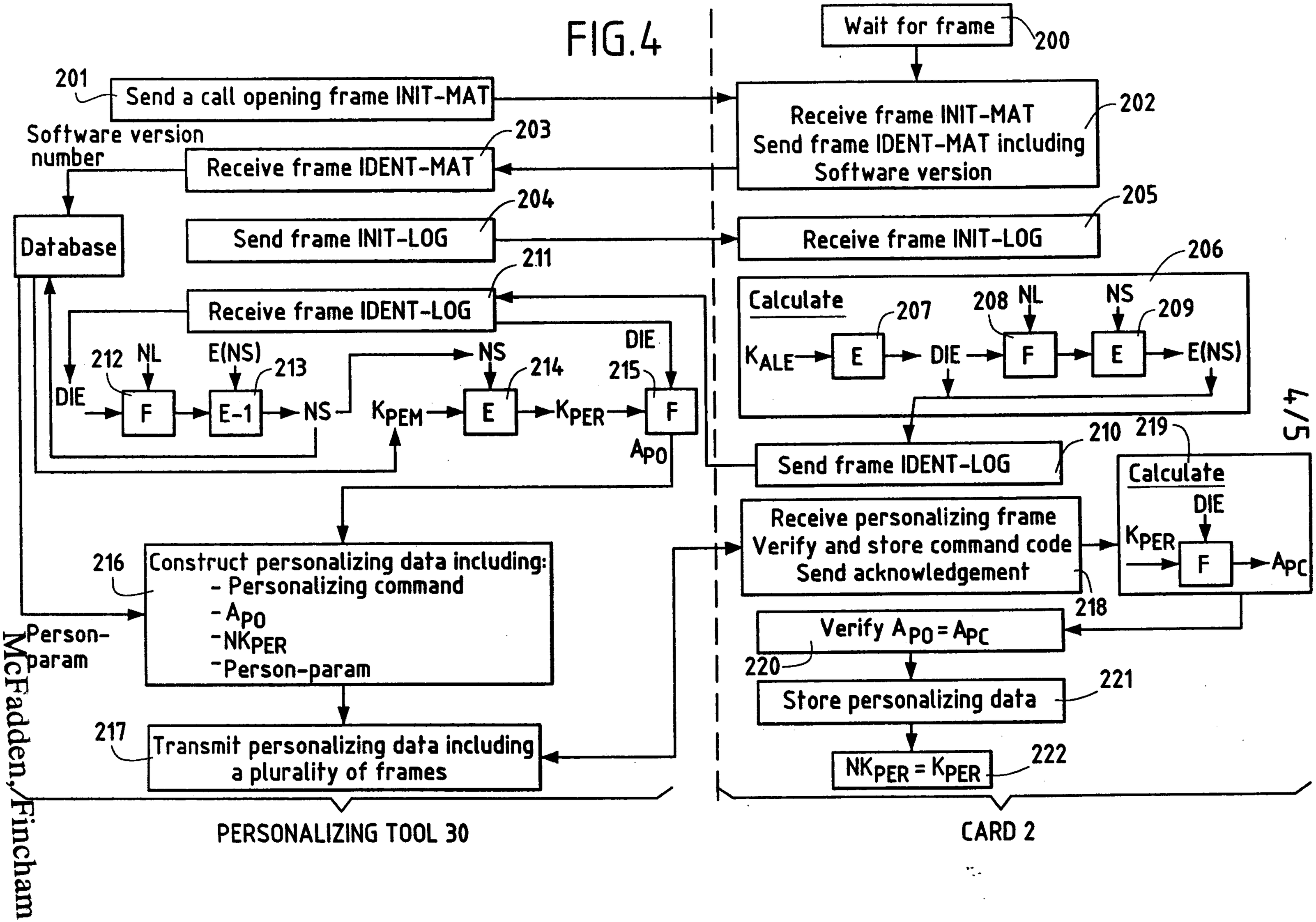

PRODUCTION TOOL 20
CARD 2
RESET
116
Reset parameters and initialize internal parameters
Wait for production frame
Prod. frame
118
Receive NS/E(KPEM)/E(KMES)/E(KKALE)/clock
E(KPEM)
119
E
KROM
KPEM
NS
120
E
KPEM
KPER
E(KMES)
122
E
KROM
KMES
E(KALE)
121
E
KROM
KALE
123
Store
NS/KPER/KALE/KMES
115
Read serial number NS stuck to card
117
Read internal clock
Send production frame
KPEM
111
E-1
KROM
E(KPEM)
KMES
112
E-1
KROM
E(KMES)
KALE
113
E-1
KROM
E(KALE)
114
Initialize
E(KPEM)/E(KMES)/E(KALE)
in production tool
SUPPLIER
Ship KPEM/KALE/KMES to client

FIG.3

FIG.4



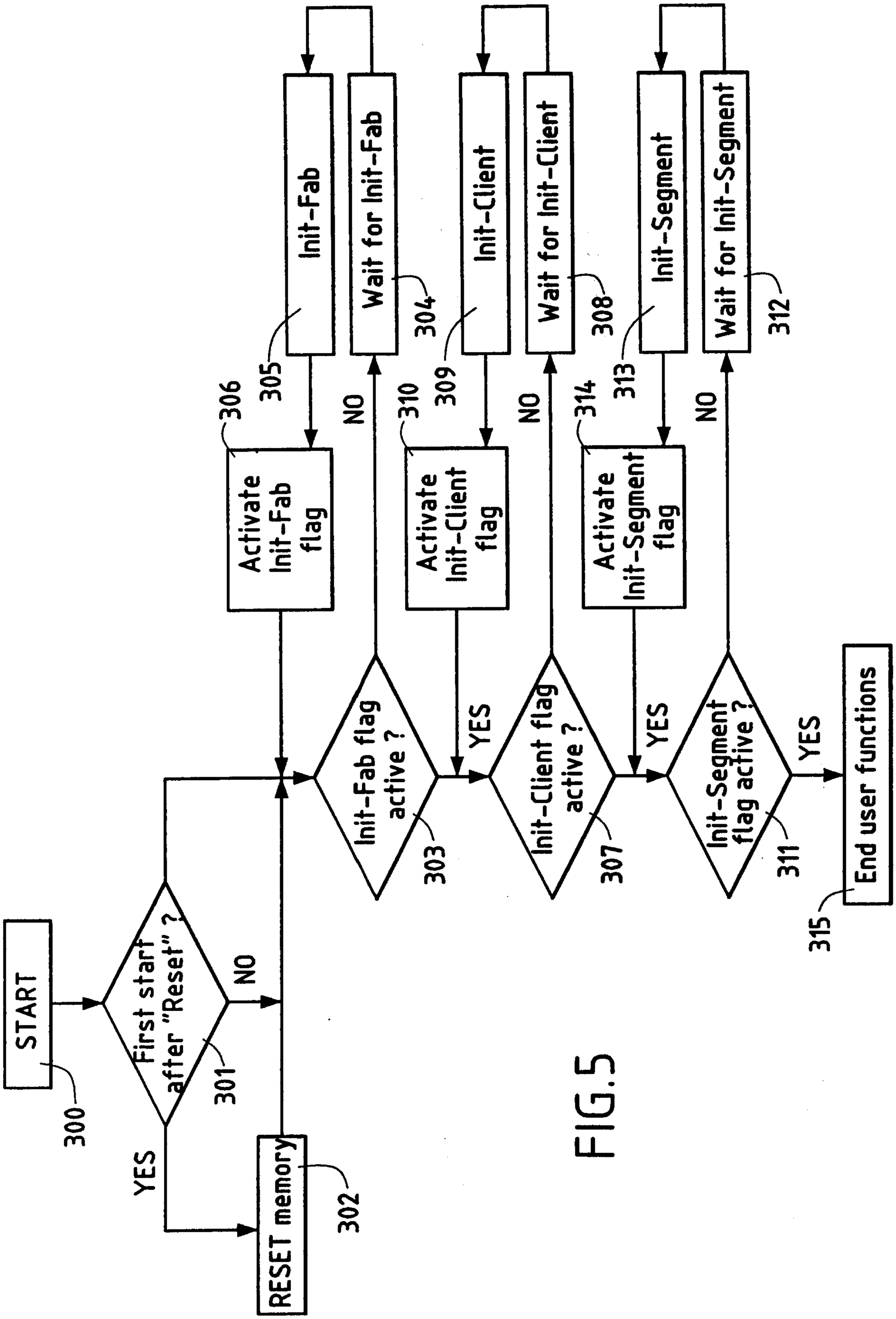

START
300
First start after "Reset" ?
301
YES
NO
RESET memory
302
Init-Fab flag active ?
303
YES
NO
Wait for Init-Fab
304
Init-Fab
305
Activate Init-Fab flag
306
Init-Client flag active ?
307
YES
NO
Wait for Init-Client
308
Init-Client
309
Activate Init-Client flag
310
Init-Segment flag active ?
311
YES
NO
Wait for Init-Segment
312
Init-Segment
313
Activate Init-Segment flag
314
End user functions
315

FIG.5