

Conditional Access Device and Process.

The Field of the Invention

5 This invention relates to the field of conditional access devices created by a pointing device integrating one or several couplers for microcircuit cards.

10 The device is designed to carry out transactions secured by microcircuit cards, to identify the cardholder and/or to check different stages of transactions.

15 The applications mainly concern conditional access to the resources of host equipment, conditional access to available resources on external equipment with which the host equipment is linked or connected, the management of software operating licenses stored in the host equipment or in the external equipment with which the host equipment
20 is linked or connected or electronic payment, etc.

Definitions.

25 The meaning of 'microcircuit card' is a support, generally a card, comprising one or several integrated circuits executing processing functions and/ or storage operations. Smart cards, or microprocessor cards, commonly known as 'chip cards', contactless cards or PCMCIA cards are examples of
30 these.

35 The meaning of "microcircuit card coupler" is any means of operating a signal exchange interface between hardware and a microcircuit card, according to standardized or specific communication protocols. Signal exchange can be carried out by an

electrical connection or a wireless link such as an electromagnetic or light link.

By "host equipment" we mean a computer terminal, a workstation, a personal computer, a multimedia terminal, etc, and particularly but by no means exclusively, all the above-mentioned equipment comprising means of bidirectional connection, all be it temporary or permanent, to a local or public communications network.

The term "pointing device" means any manually operated device with which the user acts upon visual objects. It is intended to be used with interactive host equipment having a screen and a user's graphical interface for visual objects. Examples include an optomechanical mouse pointer, an optical mouse needing a special mat, a ball or track ball, a digitizing stylus or a cursor, a touch pointer, a stick or joystick, or a remote control lever system for CD- I.

The State of the Art.

These peripheral devices work conjointly with the equipment they command and with which they are connected by the intermediary of a RS232, USB communication port or an equivalent system, or in other cases are linked by wireless transmission, for example by infrared or microwave links. In certain instances, especially when the host equipment is a portable computer, these devices are integrated into the equipment, even though the device represents a selfcontained unit.

Generally, they are easily interchangeable devices because most host equipment manufacturers have adopted common standards. They are also relatively cheap in relation to the host

equipment and can be replaced by a similar device independantly to the host equipment without difficulty.

5 It has been suggested in the state of the art to integrate a microcircuit card connector into certain peripheral pointing devices. Such was the case in the EP485275 European patent or the German patent DE4326735 The peripheral device described in the EP485275 European patent application represents
10 the closest state of the art device. It comprises a microcircuit card connector directly linked to the common leads between the computer and the peripheral devices, allowing both signal exchange relative to the pointing functions and signal exchange for the
15 operation of safety functions as sociated with the microcircuit card. The peripheral devices act in a transparent way between the microcircuit card and the computer with which it is connected. No processing occurs in the peripheral device, which only ensures
20 the electrical link between the microcircuit card and the computer. Thus the whole of the personal identification code keyin process is done in the host equipment, which is inconvenient and constitutes a major disadvantage to the commercial development of
25 public networks such as INTERNET.

The Objective Problem of the State of the Art.

30 Indeed, today's host equipment is almost always linked to at least one network, either inside an organization or to a public network like INTERNET. It is therefore possible, and even easy, for a third party to connect himself to the host equipment and examine the data processed by it. There are technical
35 solutions to filter accessible data from third parties, but these solutions are in contradiction to

most users' spirit of openness and their wish to raise the level of communication. They also require complex arbitration to gain optimal performance which is generally beyond the scope of the average user.

5

Summary to the Invention

10 The object of the invention is to counter these drawbacks by proposing a conditional access device which considerably increases the safety level against abusive intrusions coming from third parties seeking to procure the code or access key associated to the microcircuit card through links between the host equipment and a public or internal network. An
15 intrusion into the computer's memory would never be allowed access to the user's certification data.

For this purpose the invention resides in the fact that the microcircuit card is operated locally, meaning in the peripheral pointing device,
20 and not in the host equipment. This feature is essential. It ensures a separation between the user's identification, on one hand, and on the other hand, the computer and the communications network with which it is or could be connected.

25 The means of user identification are found in the peripheral pointing device to which only the user has access. It captures the personal data which is usually secret; for example his confidential code. This data is checked by a local microcalculator using the data recorded on the card. The
30 microcalculator is generally integrated into the microcircuit card, but may also be integrated into the peripheral device. This verification does not involve any transmission of secret data to the computer from
35 either the device or according to the invention's process. The comparison is expressed by approval or

non- approval data of the user, which is the only data transmitted to the computer. This is essential to avoid the accessibility to confidential data, such as a code, by a third party linked to the computer by the intermediary of a local or a telephone network

The invention's additional features

The invention is advantageously enhanced by the different features as follows :

- it comprises a sensor for the capture of a biometrical identification signal, such as a fingerprint image sensor and /or an eye image sensor and/or a vocal recognition sensor ;
- it comprises vocal control means for transactions ;
- the keyboard and/or the screen is/are on the mouse's upper surface in such a way that a cover is joined on to the mouse's casing so in a closed position, it protects the keyboard and/or screen when the chip card.coupler is not in use ;
- a chip card insertion slot is provided at the level of a groove on the mouse's periphery, in the space between the function keys and the main part of the casing of the aforementioned mouse on which the aforementioned keys are installed ;
- in the case in which the peripheral device has a fingerprint image sensor, the device's casing has a guide in which the operator's finger may be placed ; his thumb, for example ;
- the device comprises a clock under permanent power supply which ensures the dating of operations, especially financial operations ;
- the device has at least two chip card inputs;

- it has management and execution means for at least one security application associated with the host equipment applicative software ;

5 - it comprises the means of allowing security operation transfer between storage facilities, management and execution of a security application and a microcircuit card comprising a distribution application of these security applications ;

10 - it comes with a clip-board and a stylus and a double chip card coupler and has means to capture, compress, and record written data and later unload it onto the host equipment :

15 - it comprises a personal multimedia aid and/or incorporates facilities to operate one or several desktop applications, such as a calculator, diary, or a clock etc. :

20 - the device comprises a permanent clock and means of transmission to the peripheral equipment of dated numerical data having a data sequence relative to the authorization calculated for the microcircuit card's stored data and the data keyed-in by the user in addition to a data sequence given by the clock

25 The invention also concerns a security application management and execution process in the host equipment consisting in a comparison in the peripheral device linked to the host equipment, of personal data and data recorded in the microcircuit
30 card without the personal data being transmitted to the host equipment, the peripheral device integrates personal data acquisition means and at least one microcircuit card connector.

35 In accordance with a favourable implementation mode, the process includes an extended communication protocol coming from the communication

protocol specific to the pointing means of the peripheral device. This protocol enables the use of only one serial port between the applicative software and the pointing and security facilities amalgamated in the device according to the invention.

Thus in accordance with this favourable protocol form, the data and the commands are transmitted in the form of frames comprising a whole made up of fields each of which contain a coded sequence comprising a predetermined number of bits, each frame includes an identification field and at least one of the following fields :

- a pointing information field,
- an information field relative to secured means.

The information field relative to secured facilities must contain a control field which specifies the type of information followed by the optional fields giving the length of the security application message and a control field of the aforementioned message's integrity.

Advantageously, the process supplies pointing information to applicative software and at the same time ensures message transmission towards the same or another simultaneously active applicative software and its security application.

In preference, the device transmits messages emitted by secured means in frame form whose first field is the specific pointing frame modified according to the aforesaid complete message or the message divided into several frames of the same type. Thus the pointing frames and the extended frames can be alternated.

According to an embodiment the secured storage and execution means of the said security applications are amalgamated into a releasable miniature microcircuit. Therefore, the management and the availability of the said security applications storage and execution means are made independent in relation to the device's maintenance.

Presentation of the figures in appendix.

The invention will be better understood by reading the following detailed summary, giving as a non-restrictive example and illustrated by the figures in appendix

- figure 1 represents a bottom view, (on the ball side) of the conditional access device according to a possible implementation of the invention in its mouse version.;

- figures 2a and 2b, in perspective view represent two embodiments of possible implementations for figure 1's mouse.

- figure 2c represents the view of a screen to operate an embodiment of the implementation.

- figure 3 is a schematic representation illustrating an advantageous configuration inside the mouse casing of figure 1.

- figure 4 is a top view of the ball mouse model of the conditional access device according to another possible embodiment of the implementation.

- figure 5 is a perspective view illustrating a possible implementation mode of figure 4 's embodiment.



- figure 7 is a block diagram illustrating the conditional access device with biometrical control.

5 - figure 8 is a top view of the conditional access device with biometrical control.

- figure 9 is a schematic representation, in perspective, without the microcomputer keyboard but with a touch pointing device according to the invention.

10 - figure 10 is a flowchart illustrating a possible interrogation sequence by applicative software of a security application borne by a collector card inserted in the conditional access device according to a possible implementation mode of the invention.

15 - figures 11 and 12 are flowcharts illustrating the installation and the uninstallation of a security application on a collector card inserted in the conditional access device according to a possible implementation mode of the invention.

20 - figures 13 to 18 illustrate the structure of communication frames used with the conditional access device according to a possible implementation mode according to the invention.

25 Detailed Summary of Different Examples of the Non-Restrictive Implementations of the Invention.

30 The device according to the invention will be described in the ball mouse model, the same approach applies to the other pointing devices. Figure 1 shows a device according to the invention derived from a optomechanical mouse whose ball (3) is maintained in its casing by a cover. (2). A keyboard (6) is placed in a specified opening on the bottom of

35

the main part of the mouse's casing. The depth of this opening is chosen in relation to the thickness of the keyboard as well as the thickness of the sliding spots (4). Thus the whole device does not touch the supporting surface leading the ball (3).

The device represented in figure 1 comprises a microcircuit card coupler. In figure 1 a microcircuit card (5) for example in accordance with the ISO 7816 norm or even a contactless card is inserted into the device by the lateral slot so- designed. The device may comprise the means of inserting two types of microcircuit cards, to identify the type of card and verify its correct insertion.

Thus the keyboard (6) may be placed on the mouse's upper cover, protected or not by a jointed mask. The device may carry a liquid crystal display (7) to control transactions and operations and it is connected to the host equipment by a link cord with a plug on the ad- hoc port of the host equipment. The device's power supply may be implemented by a self-contained method or by the host equipment. The electrical power supply may be set up using either an independant peripheral based power supply or, as in most cases, by the voltage available from port (RS232, USB, GEOPORT) . which is linked to the peripheral device or a second port (keyboard,).

The device may also incorporate a permanently powersupplied clock which is necessary for the dating of financial transactions. It may also comprise secured means authorized to set up an electronic wallet application. Thus it can receive and keep money or an electronic value. The aforesaid means may be implemented either with a secured

version of a microcontroller and incorporating an electronic wallet application or in using a second microcircuit card coupler having an electronic wallet application. This second electronic wallet card is in preference a miniature contact card (5a) and is placed inside the device, (for example GSM format 15 x 25mm). This facilitates its replacement in the case of validity expiration or failure. This built-in financial function corresponds to an electronic wallet.

An embodiment represented in figure 2c consists in replacing the personal data key- in keyboard by an equivalent computing solution. This equivalent solution is constituted by a program giving a host equipment screen (50) display of a graphical representation of the virtual keyboard (54), made up of virtual keys (51, 52). The virtual keys (51) on this keyboard are positioned in a random way, different in each new activation of this program. The personal data key- in is carried out with the aid of the conditional access device's pointing functions according to the invention. Signal processing operation and index position validation (53) on the virtual keyboard is done exclusively on the peripheral device so as to prevent the data transmission of the validated position to the host equipment.

Several ergonomic configurations are possible on the mouse's casing (1).

As illustrated in figures 2a and 2b, two different configurations may be envisaged.

In the two cases, the slot (1b) is placed on the side of the casing (1) at the opposite end to the mouse's function keys, these keys are referenced 8 on the figures 2a and 2a. The configuration illustrated in figure 2b presents an advantage

because it simplifies the manufacturing tools. The slot (1b) is situated in a groove (1c) usually found on the mouse's peripheral in the extension of the space between the function keys (8) and the main part of the mouse's casing (1).

Figure 3 illustrates an advantageous configuration inside the casing (1). Traditionally in a ball mouse's casing, there are two encoder axes (41, 42) and a thrust roller (43) in permanent contact with the ball (3). These encoder axes (41, 42) track the ball's movements. The thrust roller's holding spring (43) in contact with the ball (3) is a spiral spring which reduces the space required for the pressure mechanism inside and so liberates a volume of space for the chip card's insertion zone.

In another embodiment of the ball mouse model according to the invention, illustrated by figures 4 to 6, the keyboard (6) is placed on the mouse's top surface, meaning on the surface opposite to the bottom (1b). A jointed cover (9) protects the keyboard (6) when the chip card's coupler function is not used. The cover (9) is not represented in figure 4. It is shaped in a way that its top surface is extended exactly in the same shape as the casing in its closed position. Thus the peripheral device is like a traditional mouse.

This cover is hinged to the casing (1) by an arm (10) which pivots on the casing (1). As the aforementioned arm (10) itself pivots in relation to the casing around an axis which is parallel to the pivoting axis of the cover (9) attached to the aforementioned arm (10).

A stop (10a) is provided on the casing (1) to limit the clearance of the cover (9). Therefore there is a joint which enables the operator to completely clear the cover from the keyboard

zone(6), so as to liberate its access. Yet the peripheral device still maintains its compact aspect.

In the case of a financial transaction application on an on- line network or a local network, the device's operator can key- in the following different operations as follows.

- Validation
- Correction, erase last keyed- in number.

- Journal, reading of the list of the last transactions,

- Balance of the account, reading of the remaing sum or balance value in the electronic wallet card,

- Select, currency selection for an intersector electronic

- wallet,
- Cancel, abort current transaction,
- Local, stop communication with host equipment,

- Lock, chip card,
- EW/Card, electronic wallet selection (EW) or inserted card if applicable,

- Transfer, initiate transfer operation,

The device attached to the host equipment comprises suitable software means and if connected to an information network enables secured payments on line of goods and services by credit cards and electronic wallet cards but also secured money transfer between two distant financial bodies.

For example, two people situated in different places, each having a personal computer with a modem according to the invention may execute the following secured transactions :

- transfer an amount of money from the first person's credit card to the electronic wallet card of the other person ;

- select the currency which is the object of the transfer;

- transfer money from an electronic wallet card to another;

- thus, both persons may use on-line financial services for electronic wallets offered by their banks.

- transfer money from a current account to an electronic wallet card and vice versa;

- change money into a different currency and vice versa ;

Each time the cardholder's identity is demanded, his personal code and his identifying signature are keyed- in, the device thus creates a protective shield against computer fraud.

Furthermore the device comprising electronic wallet means allows the following operations :

- checking the remaining value or balance;

- reading the transaction journal;

- locking its electronic wallet.

A chip card (5) may comprise several financial applications, for example a credit card and at least one electronic wallet. Each basic device according to the invention has means of carrying transactions between the resident financial applications on the same chip card, because the security conditions are implicitly ensured by the card itself.

35

The device incorporating, either an internal electronic wallet (EW) or two identical couplers, one of which comprises an electronic wallet card having an intermediary role, may be used in the local working mode in card to card transactions, the cards being successively inserted in the available connector :

- debit a credit card and load an electronic wallet;
- transfer money from one electronic wallet to another ;
- keep the money in the electronic wallet;
- cancel the last transaction.

It should be noted that the means setting in operation the cardholder's identification, (personal code keyin or signature), plus the chip card coupler means and the pointing means (selection, validation, modification), define the basic configuration for each type of device described herein, in combining different means of serial communication with host equipment, keyboards, displays, power-supply, electronic wallets, we obtain device families according to the invention.

A peripheral device of the type just described adds chip card terminal functions used in financial access control, identification, and toll applications to a personal computer or an interactive television.

It allows the payment of goods and services on line networks with credit cards or electronic wallets as well as home banking functions. In the electronic wallet (EW) version, the device may be used as a monetary reserve for payment on line networks or local networks.

The device enables the use of personal payments means (credit cards, electronic wallet), or

anonymous means (electronic wallet, EW).In this way, the device handles electronic money as a direct replacement to physical and brings down the physical barriers between operators.

5 The device may also be used for business network administration; securing access and protecting software.

10 The device replaces the traditional mouse or any other serial pointing device and it comes with a software pilot, suited to each type of host equipment. Generally it is a remote control unit designed for multimedia terminals and is recognized as a pointing device (personal computers, interactive multimedia televisions. It can also incorporate
15 additional applications such as a financial calculator, clip board, diary, etc.

20 Designed in the form of a clip board with a stylus and a double chip card interface which may as an option, record written files compressed into the memory, the device can be favourably used by medical professions

25 Figure 7 represents a configuration setting in operation a biometrical control; a control using, for example, a fingerprint scanner or an eye image scanner comprising an image sensor (15) which is, for instance, a fingerprint scanner or an eye image scanner connected to a peripheral microcontroller (13) seen in figure 7 . The
30 microcontroller (13) is also linked to specific pointing means(11), a display screen (7) as well as a keyboard (6). Thus it communicates with an external chip card (5) through the interface (14), and with the internal chip card through interface (14) and on
35 the other hand by a microcomputer (19), with which the aforementioned peripheral device is associated.

In another embodiment, the microcontroller(12) is conveniently linked to a synthesis and vocal recognition processor (16), which is ,for example,linked to a microphone MIC and a loudspeaker HP ,placed in the casing.(1). An operating embodiment consists in verifying the user's vocal signature during the reading of the data displayed on the peripheral screen or on the host equipment.This implementation mode enables vocal recognition and a comparison with the digital vocal signature recorded on the microcircuit card. (5), coming from an extremely reduced number of words and using algorithms and simplified integrated circuits.It is a low cost method which only slightly reduces the safety of the comparison.

The processing means which constitute the unit (12) take the shape of the biometrical object read by the sensor (15) and / or the vocal recognition unit(16) enabling processing by a card(5). This receives and compares the biometrical object with the reference presented in the memory. In this embodiment the comparison between the reference and the biometrical object read by the sensor (15) or the unit (16) can be implemented by the microcontroller (12).

It should be noted that the microcontroller's processing means (12), may be an optimized mathematical coprocessor for signal processing and/ or crythographical calculations Thus all or part of the unit (16) can be conveniently integrated into the same chip or module.

The biometrical object, such as an image read by a sensor (15) or the vocal recognition implemented by the unit (16) replaces the user's

identification code which does not need to be keyed-in on the keyboard (6).

Figure 8 represents a configuration whose sensor (15) is situated on the lateral edge of the casing (1). The edge takes the form of a guide (17) intended to receive the user 's finger ; his thumb for example. The EN1546 European norm project presents the working and the use of electronic wallet cards in detail. Also the EMV European norm describes in a detailed way the standard procedures of payment by microcircuit cards as well as the features of such cards.

The peripheral device may comprise a wireless communications medium to increase mobility in relation to the host equipment . Radio or infrared solutions can be used to counter environmental constraints and those of target host systems.

The peripheral device can be integrated into the microcomputer itself. An embodiment of this type is illustrated in figure 9. In this embodiment a microcomputer incorporates a tactile pointing device (20). A keyboard (6) which is independant in relation to the computer' s C keyboard, is integrated into the S support on which the C keyboard and the tactile pointing device (20) are installed.

Advantageously ,the device's tactile surface (20) is used to implement the personal data key- in keyboard (6) because a representation of the aforementioned keyboard is superposed on the aforesaid tactile surface. This representation may be constantly visible In another embodiment, it may be visible only during the cardholder's identification operation by retro- lighting implemented by an electroluminescent film, for instance.

Another of the device's embodiment's according to the invention, operates vocal synthesis

means and a suitable dictionary. This dictionary may be downloaded and/ or modified by a secured procedure using an authorized server. This server may be the conditional access device's manufacturer 's model, for instance. The device can with vocal recognition means, learn the minimum number of commands required to carry out transactions; such as accept, cancel, continue. For example to check the price displayed on the computer screen ,for instance \$198. 25, the procedure consists in transmitting the data relative to the price to the peripheral device, which transforms this information by synthesis and vocal reproduction means to emit the sounds , "one", "nine", "eight", "point", "two", "five", "dollars".

Then the device validates the price for the transaction, for example the command "accept" pronounced orally by the holder of the inserted microcircuit card. The vocal commands may be recorded.

We will now turn to figure 10 and following for other aspects of the invention .

The peripheral device comprises a security application, indicated by the initials 'SAM' in the following of the text. By the term 'security application' or SAM we mean object software comprising an executable code and all the specific resources necessary for its working, residing and executing in the secured microcircuit which is also supplied with a secured operating system. A typical example of SAM is the electronic wallet available on the microcircuit card. A security application incorporated in the peripheral device is provided for at least one piece of applicative software in the host electronic equipment with which the aforesaid peripheral device communicates.

Both the applicative and its security application recognize the same secret information in the form of one or several of the keys; it sets into operation the same cryptographical algorithm, enabling the verification this key.

A security distribution application is thus provided to replace the applicative software's ordinary key against fraud. This security application is conveniently but not restrictively, carried by a chip card ; subsequently indicated by the term 'SAMC collector card'. This card is for example, loaded from a second card named distribution card or SAMD, which is for instance, supplied with applicative software needing protection against fraud . In this context, figure 10 is a flowchart of a basic inquiry sequence of a SAM security application residing in the peripheral device's collector card by an applicative executing locally or accessing to host equipment communicating with the peripheral device. SAM's role is a protection key for this applicative. The first stage of the SAM test (stage 101) consists in generating a random code(RNDC) which is subsequently memorized. In a second stage (102), code (RNDC) is crypted according to the balanced key procedure which is well known in the art. This encrypted code is recognized by the applicative and its SAM. The result of stage (102) is another code representing test (CLG) which is transmitted to SAM. In stage (103) the applicative checks if it can transmit test (CLG) to the device's pilot. In stage (104) the test message (CLG) is transferred to the pilot which transmits it, according to an extended protocol in relation to the communication protocol specific to the pointing means of the aforementioned peripheral device to its destination SAM.

In stage (105) the applicative waits for a predefined lapse of time, for SAM's response. SAM uses an algorithm to decrypt test (CLG).

5 If SAM is authentic the decrypting key is the same and refinds a clear initial random code. Its response (RPL) is transmitted to the device's pilot for reading in stage (106) by the applicative. The following stage (107) consists in comparing the initial code (RNDC) with the response (RPL). If they
10 are identical there is not a fraud. Such a SAM sequence test is incorporated in the protected applicative. If figure 10 sequence has only one response message in the case of success (108), the error messages (109) are more numerous in practice
15 and reflect the possible failure situations in all their stages.

The simplified sequence of a security application installation or SAM in the procedure according to the invention is presented in figure 11
20 .

A SAMD security application distribution card can be used for several installations of the same security application. The aforementioned card
25 comprises, for each security application a license counter (LCNT) initialised to the number of installations allowed by the said application. The applicative's installation program requires in stage 110 a SAMD distribution card in the peripheral device's coupler. The procedure is
30 interrupted :

- If test(111) does not recognize the SAMD distribution card or the counter (LCNT) of the number of licences to be installed, is null.

- If test (112) does not read enough memory in the SAM collector card or if the card cannot take the SAM which is to be installed.

5 - If test (114) does not validate the copy.

- If the conditions of (111) and (112) are met, the 113 stage transfers SAM from the SAMD distribution card to the collector card SAMC.

10 The peripheral device's coupler's microcontroller triggers the transfer which subsequently is carried out between the two cards in a standard secured data transfer process.

15 During this transfer, the microcontroller acts only as a link channel between both the SAMC and SAMD cards. The SAMC collector card's operating system brings the SAM to its executable form Then the SAMC card carries out the (114) test which includes the so- called transfer validation and afterwards the correct working verification of the SAM. This
20 verification consists in simulating the interrogation of the SAM and checking its behaviour The SAMC collector card erases an invalid SAM from its memory . The installation of a SAM is equivalent to a value transfer according to a similar transactional
25 mechanism to the one used in the electronic wallet system This transactional mechanism ensures the (115) stage and the license counter LCNT is diminished by a sole unit.if the SAM is validated by the secured means of SAMC storage management and execution.

30 The simplified flowchart of the uninstallement of the SAM application in the process according to the invention is presented by the figure 12.

35 In stage (116) the applicative's uninstallement program protected by the SAM requires

the insertion of a SAMD distribution card or the equivalent, in the peripheral device's coupler.

5 Test (117) checks if the SAM about to be
uninstalled will accept the inserted card in the
aforementioned coupler. If the SAMD card is the
source card ,the SAM code is still present and stage
(119) increases the license counter by a unit (LCNT).

10 If the SAMD card is not the source card,
the SAM code is transferred to the SAMC collector
card in stage (121) on condition (120) that there is
sufficient memory, in similar conditions to stage
15 above. Still in stage (121) the SAMD card's operating
system creates a license counter (LCNT) initialized
to zero. In the case of a SAM code transfer, in stage
(122), the SAMD card checks the copy's validity, as
in stage (114) of the SAM installation flowchart . By
20 the same transactional mechanism as the one found in
the SAM installation, the disassembly operation
ensures that the SAMD card comprises a valid SAM and
a license counter (LCNT) increased by a unit only in
the " success" mode. It also ensures that the SAMC
25 erases the SAM in question from its memory in stage
(123) . The process thus allows all SAMD cards having
received a security application by an uninstallement
process, to be the equivalent to a source
distribution card A security application is
30 transferred between two remote cards communicating
with each other by interposed means ensuring the
transport and integrity of their messages, via
communications networks . Thus a SAM transfer
procedure seen as a floating software license of one
35 piece of host equipment to another, -using

communications networks is similar to the SAM uninstallement process discribed herein - above .

In this case, the distribution card is replaced by the destination collector card .

5 In preference, the communication protocol used for the security applications' management and execution, employs the same serial communication channel to transport pointing information and security messages Thus the pointing and microcircuit
10 card terminal functions are available quasi - simultaneously and independantly to one another . In the framework of the said communications protocol, the information and commands are transmitted in a frame form incorporating a whole made up of fields
15 each constituted by a coded sequence carrying a predetermined number of bits, as illustrated in figure 13 Therefore, a frame necessarily comprises an identification field (FID) and at least one of the following fields :

- 20 - a pointing information field ;
- an information field relative to security operations;

The identification field (FID) initializes the reception means for the analysis of
25 its contents. For peripheral pointing device's and a given functioning mode their frames have a fixed length. In such a frame, the most significant bit is reserved for the identification by its start of frame. The protocol set into operation according to
30 the inventon, uses the same method to remain compatible with traditional pointing devi ces and always places the point ing information at the start of the extended frame . Therefore it is not restrictive to consider the pointing frame as a part
35 of the extended frame's identification field (FID) as illustrated in figure 6 . For example, the presence

of an information field relative to a security application can be indicated according to the same principle by a particular value of a group of bits from the frame's first byte. Thus the information field relative to a security operation comprises all or one part of the following fields in the quotation order, from a position determined by the aforesaid particular value of an identification field's (FID) group of bits :

- control field (OPC)
- field giving the security application's message length (DLEN) ,
- field comprising all or a part of the security application message proper (CLG) or (RPL) ,
- control field of the aforementioned message 's integrity (CRC) .

The extended frames have a variable length according to the control field (OPC). If the frame comprises a (CLG) message, intended for a security application or a (RPL) message meant for an applicative, the (OPC) field is followed by a (DLEN) field giving the length of the said (CLG) or (RPL) message . The length of the (DLEN) field is a function of the maximal length admitted for the (CLG) and (RPL) messages . The device's control and processing means according to the invention ignore the aforesaid (CLG) and (RPL) messages' significance . The optional field (CRC) enables a possible control of (CLG) and (RPL) messages' integrity

An extended frame is completely defined by its control field (OPC) which comprises at least the following information (figure 14) :

- the (OPC. C) code of the operation concerning one or several security application,
- the address of the security application concerned by (OPC .A) frame

- the information field's number of bytes relative to a security application transmitted by extended frame, this number (OPC .S) being at least equal to the field length (OPC) .

5 The (OPC.A) address also takes into account the coupler with which we access to the security application . Long messages are transmitted by segments of a constant length (OPC.S) with the exception of the last segment, divided into several
10 shorter extended frames. This method ensures the uniformity of the pointing information' s acquisition frequency .

15 Figures 15 and 18 illustrate a particular implementation of the extended frame's structure described herein - above with the aid of figures 13 and 14 .

20 Figure 15 presents the frame emitted by a conventional mouse . This frame comprises 3 bytes whose most significant bits are not used .These bits are used to indicate the extended frames

25 From this frame, figure 16 illustrates the structure of an extended frame whose identification field (FID) retakes the pointing frame and positions the most significant bit of its first byte at 1 . Thus the device's pilot detects the extended frame and analyses the fourth byte which corresponds to the control field (OPC) of th security information. The fifth byte (DLEN = m) indicates the
30 length in bytes of a SAM application response alone or in association with an other binary field available in the precedent bytes, for example, the most significant bits of the two and three bytes. The control field (CRC) comprises (n) bytes .

35 Figures 17 and 18 illustrate the structure of, respectively, the first and the fifth

frame of the extended frames which transmits the security application's response in several consecutive segments for the OPC.S =8 parameter, an, (RPL) 32 bytes response and a (CRC) on 16 bits. The
5 (OPC .8)field indicates to the device's driver the information field's number of bytes relative to a security application added to the pointing frame, with the exception of the last frame . Therefore, the pointing frames and the extended frames can be
10 alternated

The invention is described in the preceeding text as a non- restrictive example . It should be understood that a man of the profession could implement several embodiments within the
15 framework of the invention .

CLAIMS

1 - The conditional access device is intended to be used in liaison with host electronic equipment, is made up of a peripheral pointing device incorporating at least one microcircuit card coupler, characterized in that it incorporates as well as personal information acquisition means particular to each user and in that the aforementioned personal information is locally compared with information stored in the microcircuit card, without this aforementioned personal information being transitted to the host equipment.

2 - The conditional access device according to claim 1, is characterized in that the personal information acquisition means particular to each user are constituted by a keyboard to key- in an alphanumerical identification code on a tablet with a sensitive zone for the capture of written personal information. .

3 - The conditional access device according to claim 1 or 2, is characterized in that the personal information capture means are constituted by a sensor for the capture of a biometrical identification signal, such as a fingerprint sensor and/or an eye image sensor and/or a sound sensor associated with vocal recognition means.

4 - The conditional access device according to any one of the precedent claims herein, is characterized in that it comprises a keyboard to key- in

the personal information and/or display means to control the transaction.

5 - The conditional access device according to any one of the precedent- claims herein,



is characterized in that the personal information capture means are constituted by a particular means of invoking a display on the host equipment's screen, of a virtual keyboard comprising graphical representations whose layout varies in a random way with each activation of the aforesaid means, the personal information acquisition is carried out by graphical representation pointing and validation when the position of the pointer is on the sought- after graphical representation, the processing of the pointing information and the validation on the virtual screen being implemented exclusively in the conditional access device.

6 - The conditional access device according to any one of the precedent claims herein, is characterized in that the personal information acquisition means are constituted by an acquisition module and the digitization of the user 's voice.

7 - The conditional access device according to any one of the precedent claims herein, is characterized in that it comprises vocal synthesis means and sound reproduction for the control of the transaction.

8 - The conditional access device according to any one of the precedent claims herein, is characterized in that the personal information acquisition means are constituted by a tactile pointing zone (11) comprising a representation of the keyboard superposed onto the tactile surface.

9 - The conditional access device according to any one of the precedent claims herein, is characterized in that it comprises a permanently working clock and the means of transmitting to the peripheral equipment, dated numerical data comprising a data sequence relative to the authorization calculated from stored data in the microcircuit card



and the data keyed in by the user and a sequence given by the clock.

10 10 - The conditional access device according to any one of the precedent claims herein,
5 is characterized in that it comprises the means of allowing it to execute in co- operation with the host equipment on on- line networks, all or a part of the following secured transactions involving an electronic wallet card or a credit card.

10 a) payment, b) refunding, c) cancelling an operation, d) currency selection and/or all or a part of the following secured transactions involving
15 on inserted electronic wallet card, e) loading on electronic wallet card from a bank account, f)
15 transfer of a value from an electronic wallet card to a bank account, g) the transfer of a value from an electronic wallet card to another electronic wallet card and crediting a credit card.

20 11 - The conditional access device according to any one of the precedent claims herein,
20 is characterized in that it comprises the means of allowing it to execute independantly and/or in co- operation with host equipment, all or a part of the following operations involving an inserted electronic
25 wallet card : a) a verification of the present value or the balance of the account, b) a reading of a list of recent transactions or collector journal. c)
25 Locking an electronic wallet card, d) a change of the identification code.

30 12 - The conditional access device according to any one of the precedent claims herein,
30 is characterized in that it comprises means of carrying out transactions between the resident financial applications on the same microcircuit card.

35 13 - The conditional access device according to any one of the precedent claims herein,



is characterized in that it comprises means including an electronic wallet application and- means allowing it to carry out all or part of the following operations between two cards successively inserted into a same connector. a) transfer of a value from the electronic wallet card to another electronic wallet card, b) transfer of a value from an electronic wallet card to the device itself, c) debit or credit an electronic wallet card and credit or debit the same value on a credit card, d) cancel the operation.

14 - The conditional access device according to any one of the precedent claims herein, is characterized in that aforesaid means including the electronic wallet application are incorporated in a releasable microcircuit card (5).

15 - The conditional access device according to any one of the precedent claims herein, is characterized in that it comprises in addition to an active digitization surface with a stylus and/or tactile, and a readout, the active surface and readout being superposed.

16 - The securisation process of the access to host equipment, sets into operation a conditional access device in accordance with at least one of the precedent claims herein, characterized in that certain functions at least of the said host equipment are only accessible after capture, by the user, of personal information which is conform to information recorded on the microcircuit card and the verification of the conformity between the personal information and the information recorded on the microcircuit card is realized by a peripheral device linked to the host equipment, without the personal information being transitted to the host equipment.



17 - The process of secured data processing transactions comprises a comparison stage between the user's personal information and the data contained in the microcircuit card, setting in
5 operation a conditional access device which is in accordance with at least one of the precedent claims herein, characterized in that the control stage is carried out by the said conditional access device and forms a protective barrier against computer fraud.

10 18 - Process for the management and execution of security applications within interactive electronic equipment equipped with peripheral equipment, the said electronic equipment comprises a screen and the means of allowing local and remote
15 execution of applicative software and having a graphical user interface comprising visual objects which the user can act upon manually by means of the said peripheral device characterized in that the said process comprises a communication protocol between a
20 part at least of the applicative software and secured means of storage, management and execution of a security application, co-operating with at least one coupler intended to receive, especially, a micro-circuit card(5) incorporating a distribution
25 application of the security applications, this protocol being an extension of the communication protocol specific to the pointing means of the said peripheral device.

30 19 - A process according to one of any of the claims from 16 to 18, characterized in that all the information and commands are transmitted in the framework of the said communication protocol in waveform comprising a whole, made up of fields each constituted by a coded sequence comprising a
35 predetermined number of bits, each frame



incorporating an identification field (FID) and at least one of the following fields

- A pointing information field
- A field of information relative to secured means.

20 - A process according to claim 19, is characterized in that the information field relative to the secured means comprises all or a part of the following fields in quotation order.

- control field (OPC)
- field giving the length of the security application message (DLEN),
- a field which includes all or a part of the security application message proper (CLG) or (RPL),
- a control field of the integrity of the said message. (CRC).

21 - A process according to claim 20, is characterized in that the control field (OPC) includes at least the following information :

- the operation code (OPC. C) concerning one or several security applications
- the address of the security application concerned by frame (OPC. A)
- the number (OPC. S) of bytes of the information field relative to a security application transmitted by extended frame this number (OPC. S) being at least equal to the field length (OPC).

22 - A process according to the claims from 16 to 21 is characterized in that the distribution application of the security applications (30) comprises a license counter (LCNT) for the control of multiple transfers of the same security application in the limit of a predefined number of installations or licenses.



23 - A process according to the claims 18 and 22 is characterized in that the transfer operation of the security operation between local and remote secured means comprises all or a part of the following stages :

- identification of the initiator of the transfer
- reciprocal authentication of secured means of the participants
- secured copy of the application code on the destination means
- validation of the copy
- invalidation of the security application in the source means.

24 - A process according to claim 23 is characterized in that the identification stage of the transfer initiator consists in a security application having been installed in the said secured means of storage, management and execution of the security applications (27), or the distribution application of the security applications (30) identifies the transfer initiator by a personal code captured exclusively using the means of the said peripheral device and without the code being transitted through the said interactive electronic equipment.

25 - A process according to claim 24 characterized in that the invalidation stage of the security application in the source means consists in the erasing of its code and the liberation of its resources with the exception of a distribution application of the security applications (30) of which only the license counter (LCNT) is decremented by a unit.

26 - A process according to any one of the precedent claims from 16 to 25, characterized in that the peripheral device's driver, supplies the



pointing information to the applicative software and at the same time ensures the transmission of messages towards the same or another simultaneously active applicative software and its security application.

5 27 - A process of securisation of the
acces to host equipment according to any one of the
claims from 16 to 26, is characterized in that the
host equipment transmits to the conditional access
device information relative to the current
10 transaction, that this information is translated by
vocal synthesis, and that the validation of the
transaction is implemented by the oral pronunciation
of a word or a predetermined phrase by the holder of
microcircuit card inserted in the device.



INVENTION PATENT

CONDITIONAL ACCESS DEVICE AND PROCESS.

5

Invention of : MR Cornel SIRBU

Applicant : MR Cornel SIRBU

ABRIDGED DESCRIPTION

10

This invention concerns a conditional access device intended to be used in liaison with host electronic equipment, constituted by a pointing peripheral device incorporating at least one microcircuit card coupler, characterized in that it incorporates in addition, personal acquisition means particular to a user and that the said personal information is locally compared with memorized information on the microcircuit card (5) without the said personal information being transitted through the host equipment.

15

20

FIGURE OF THE ABRIDGED DESCRIPTION

25

Figure 1

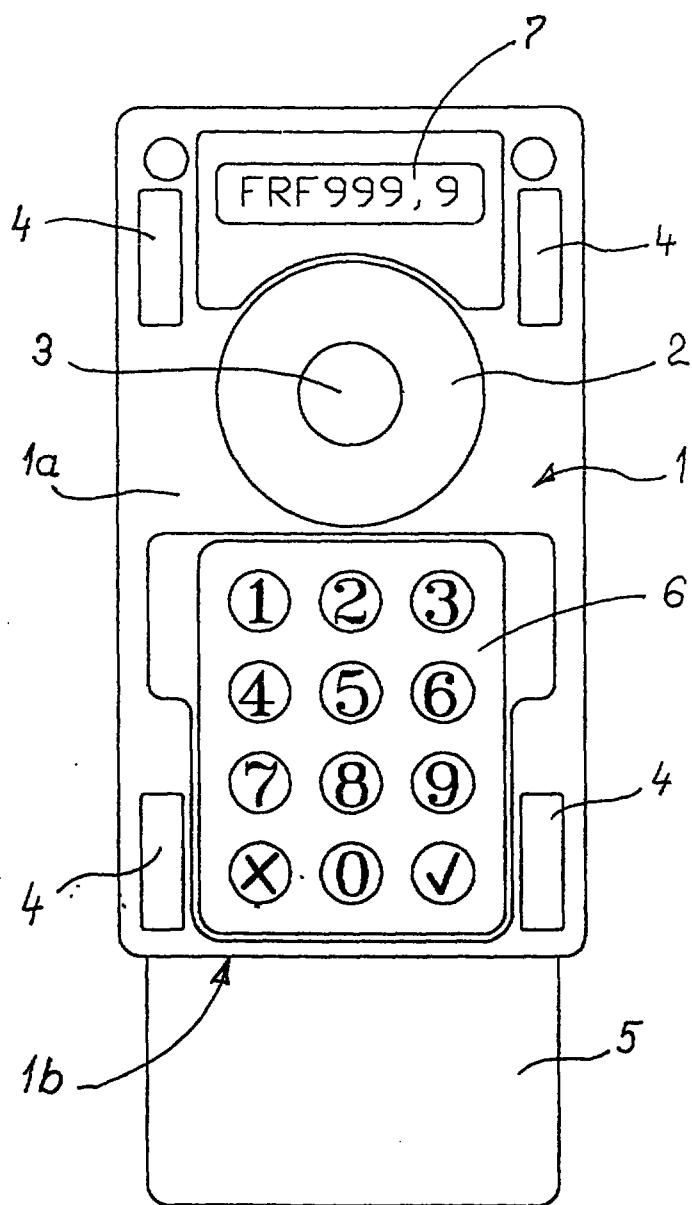


FIG. 1

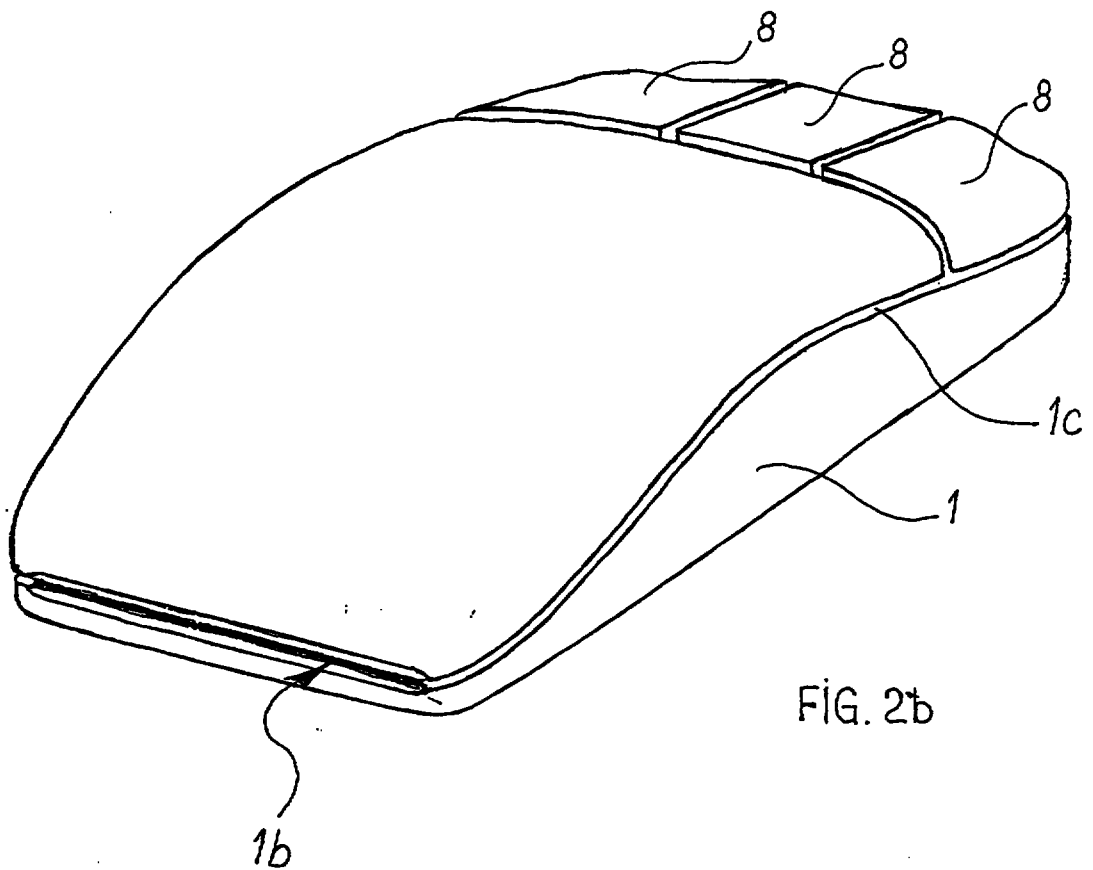
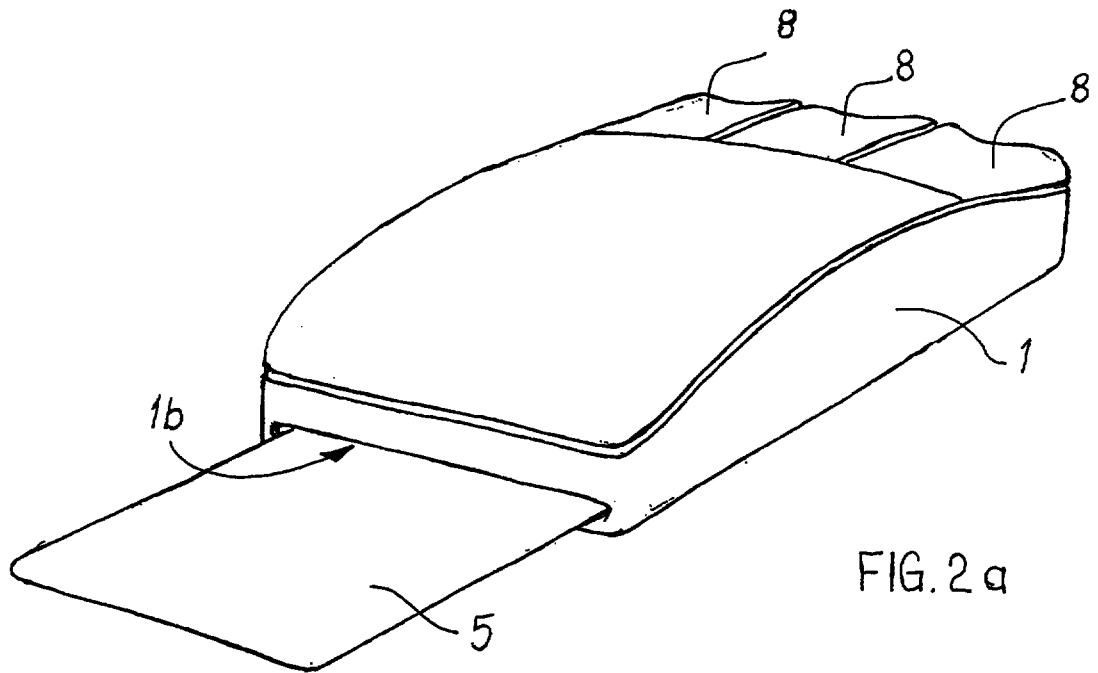
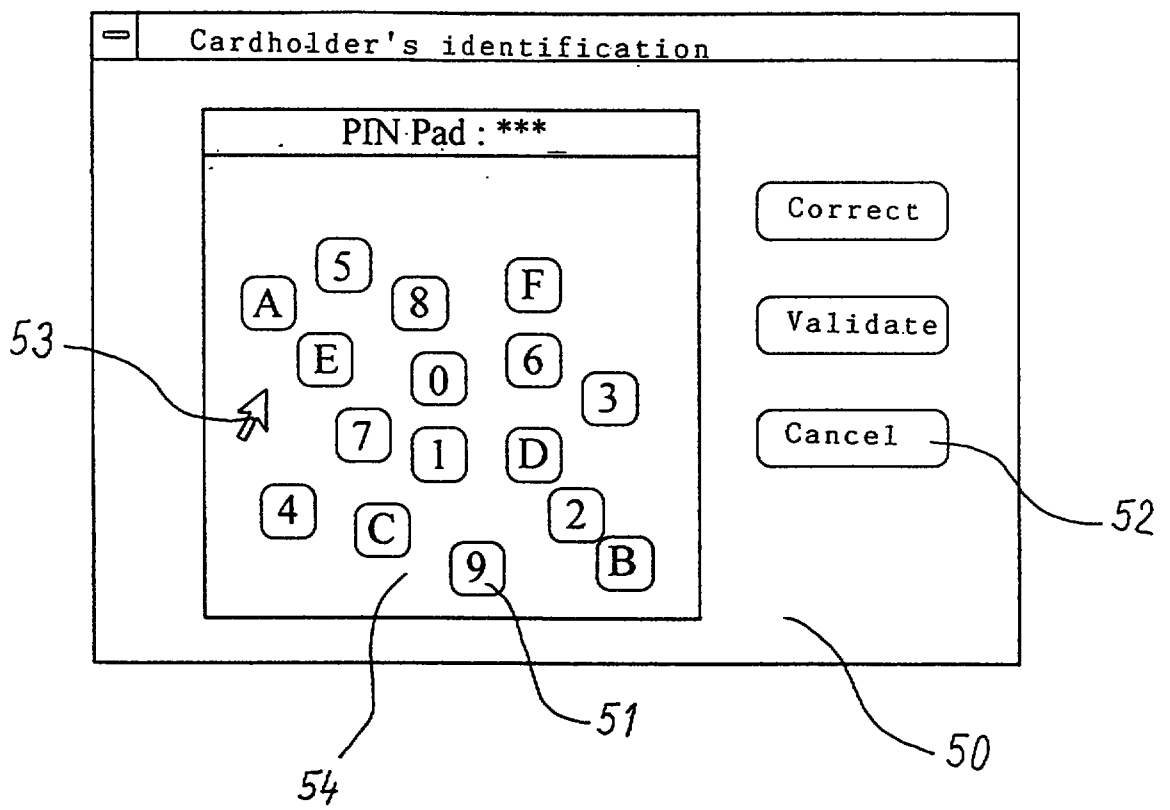


FIG. 2c



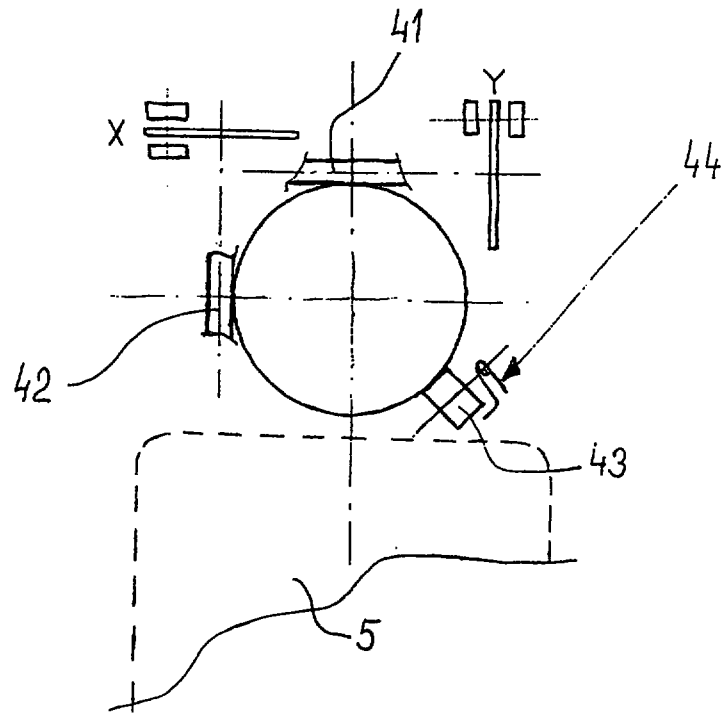


FIG. 3

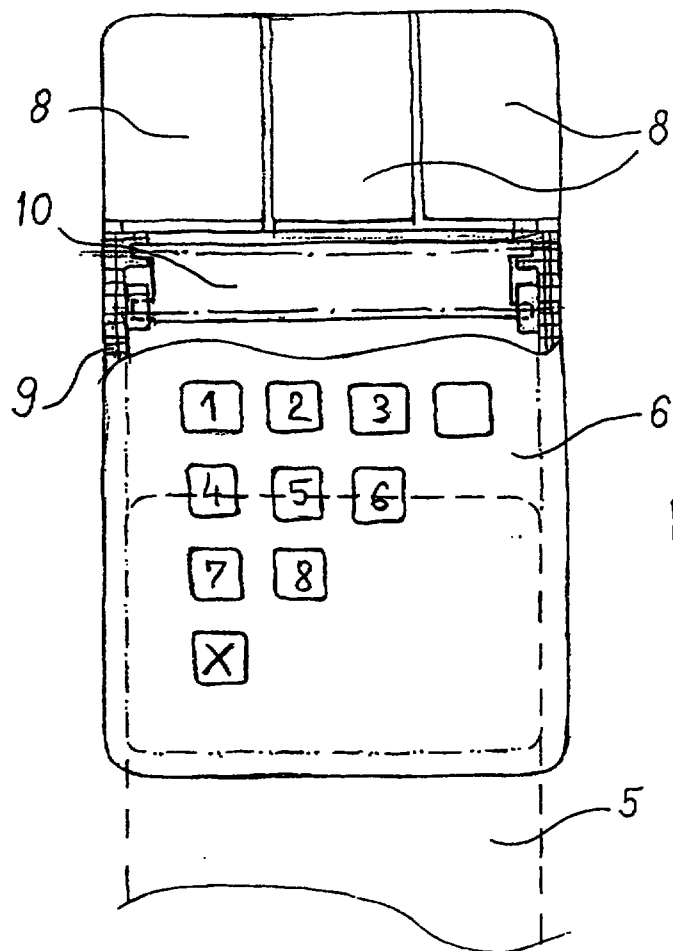
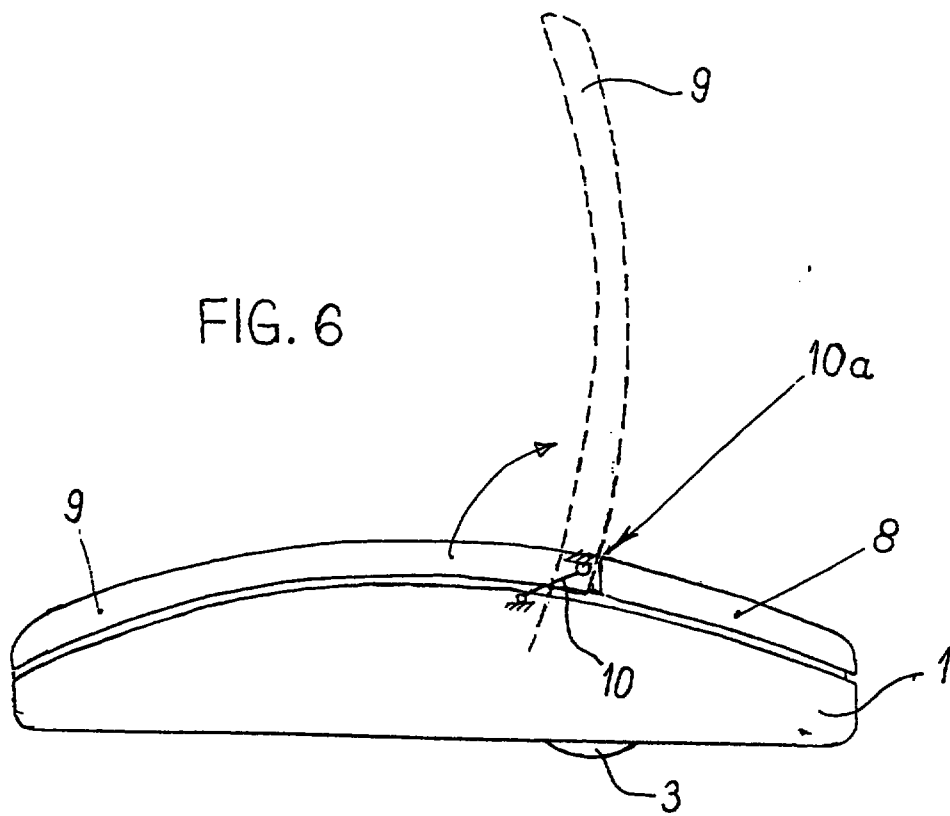
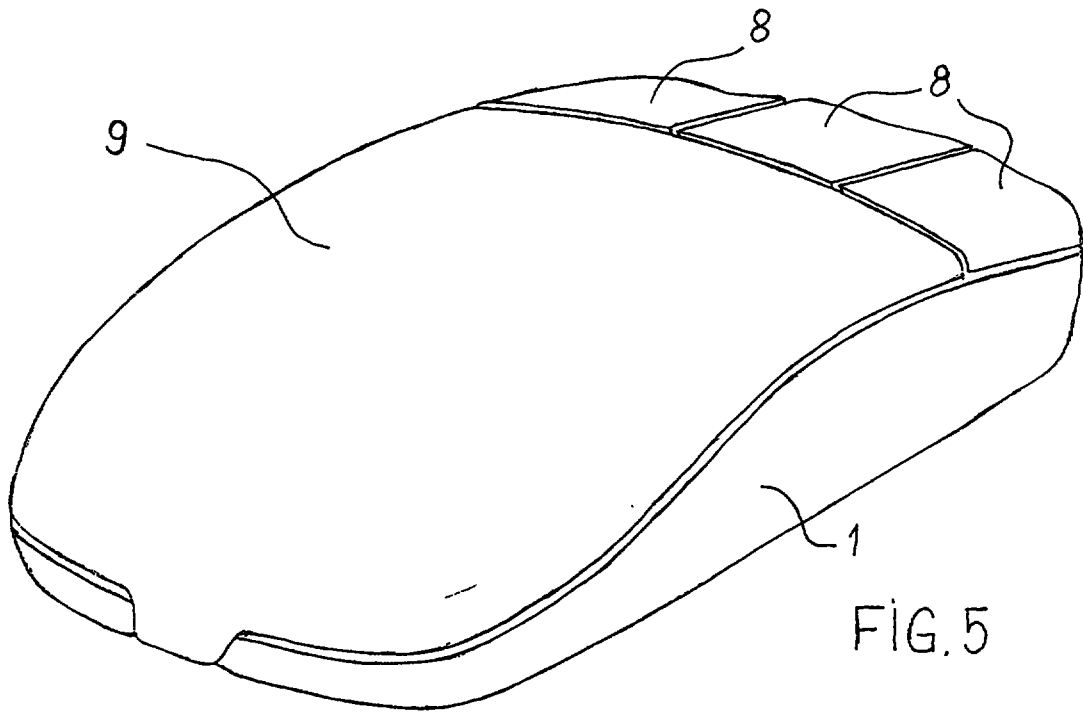


FIG. 4



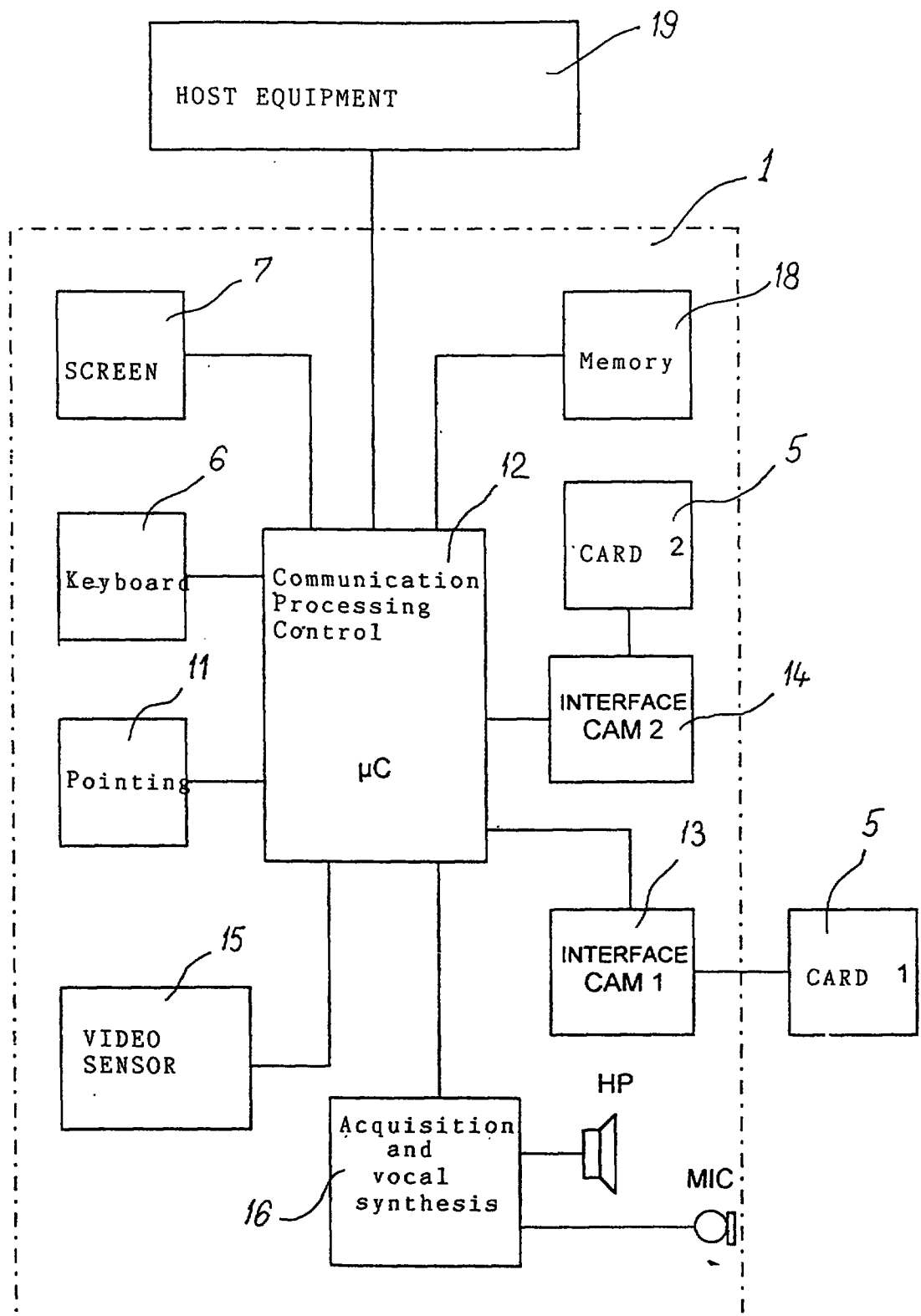
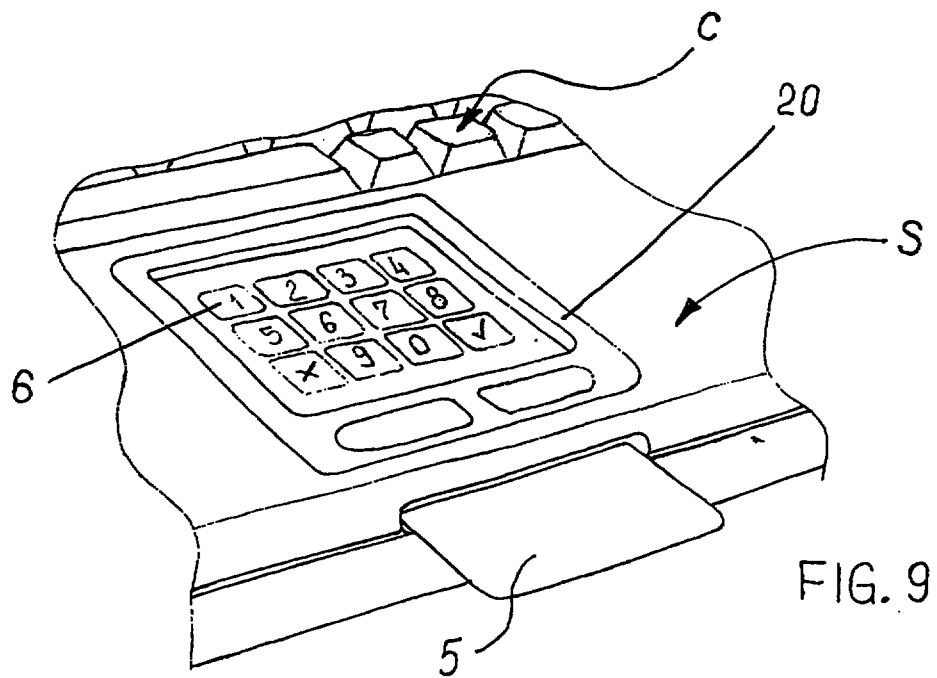
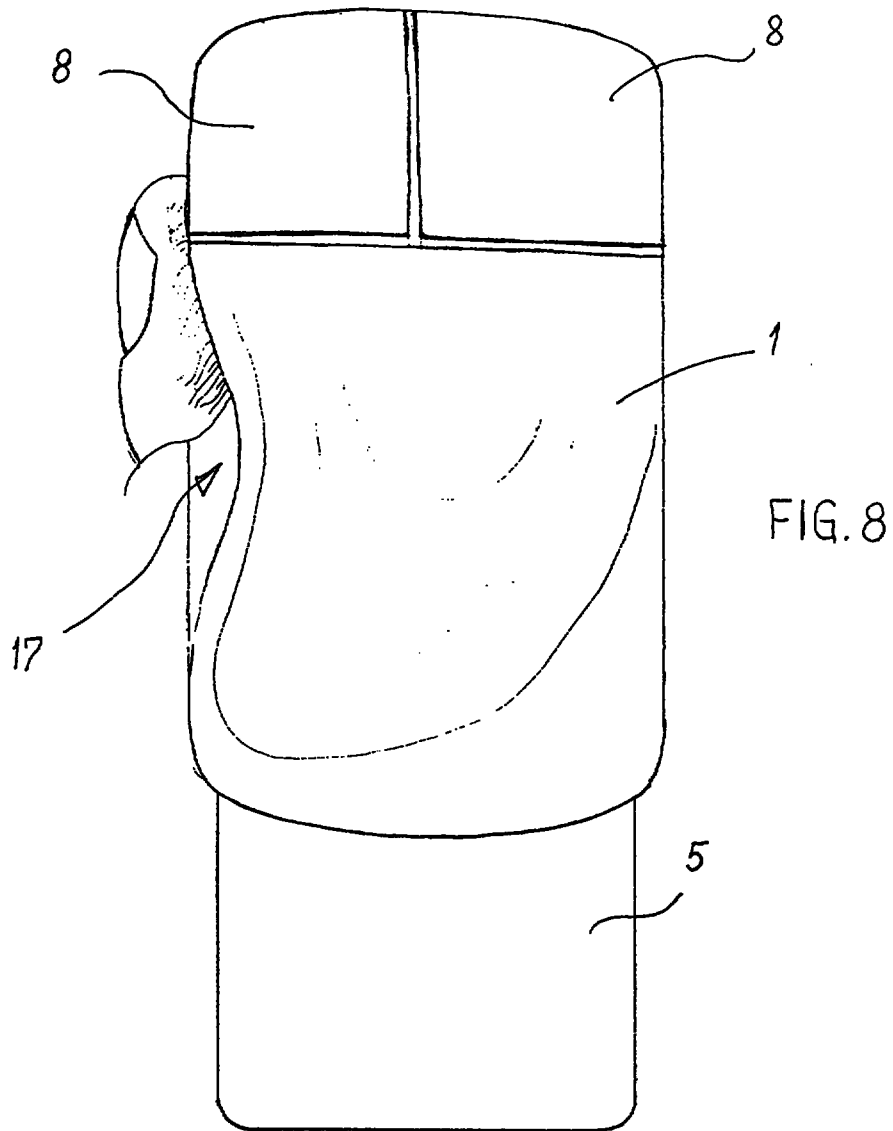


FIG. 7



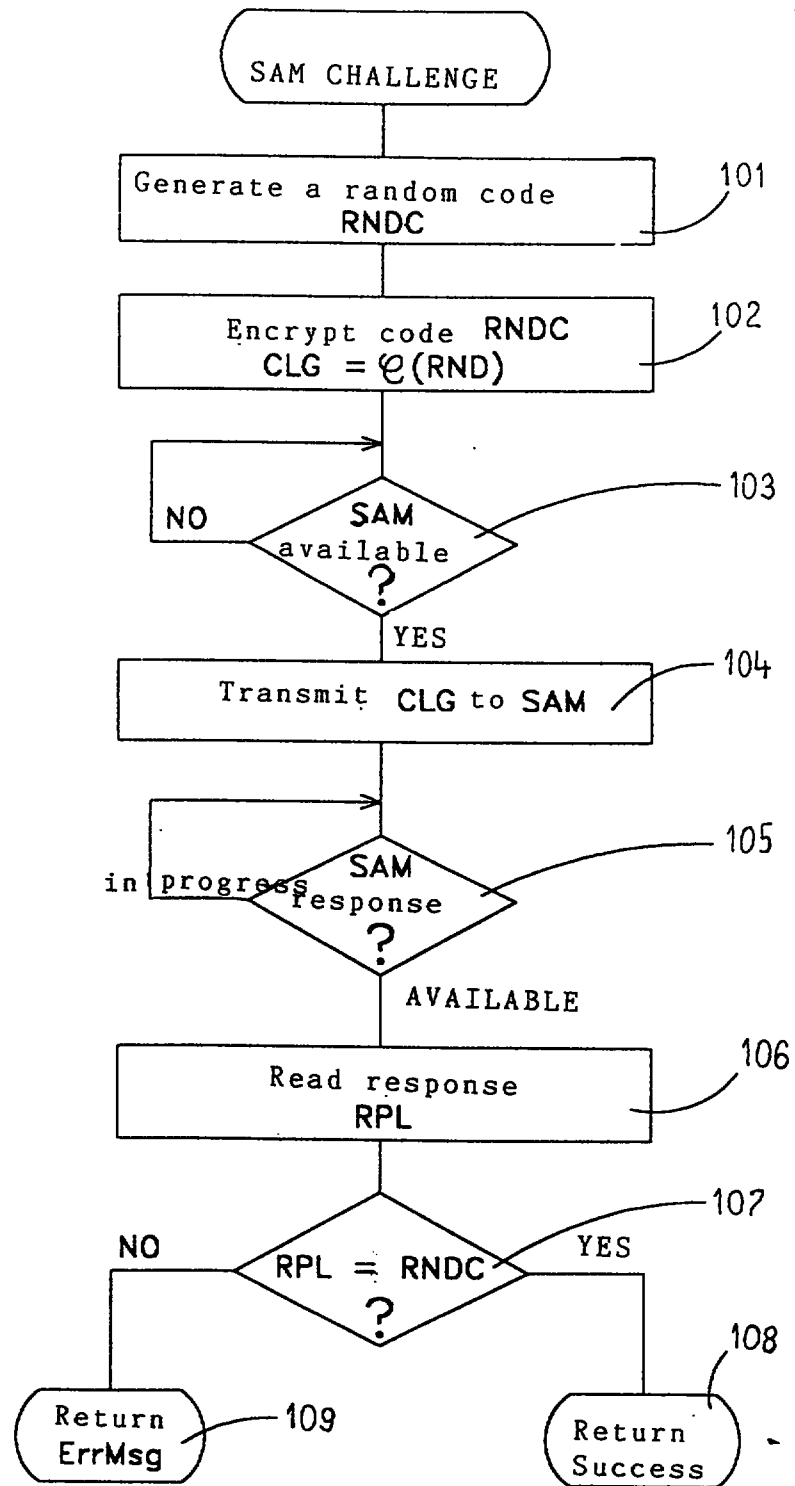


FIG. 10

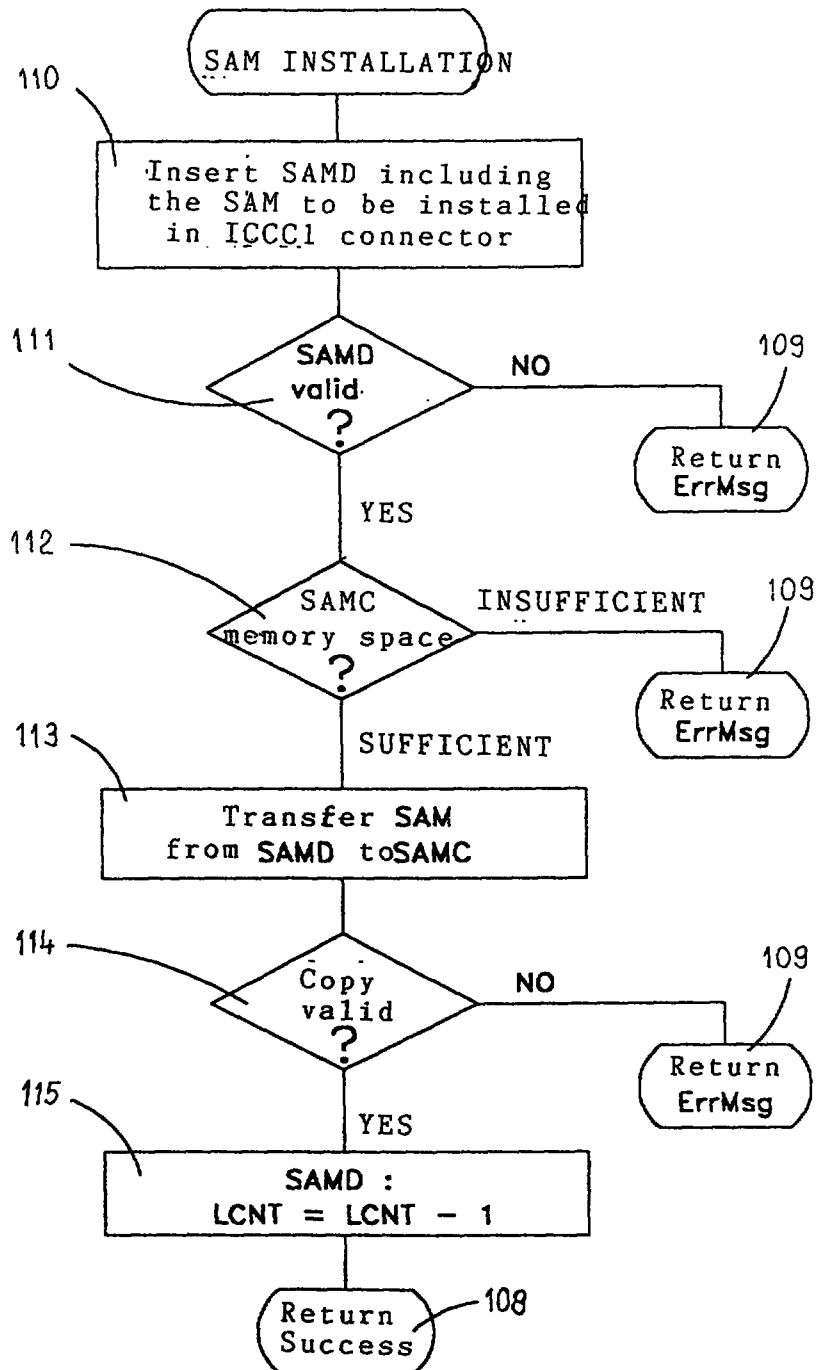


FIG. 11

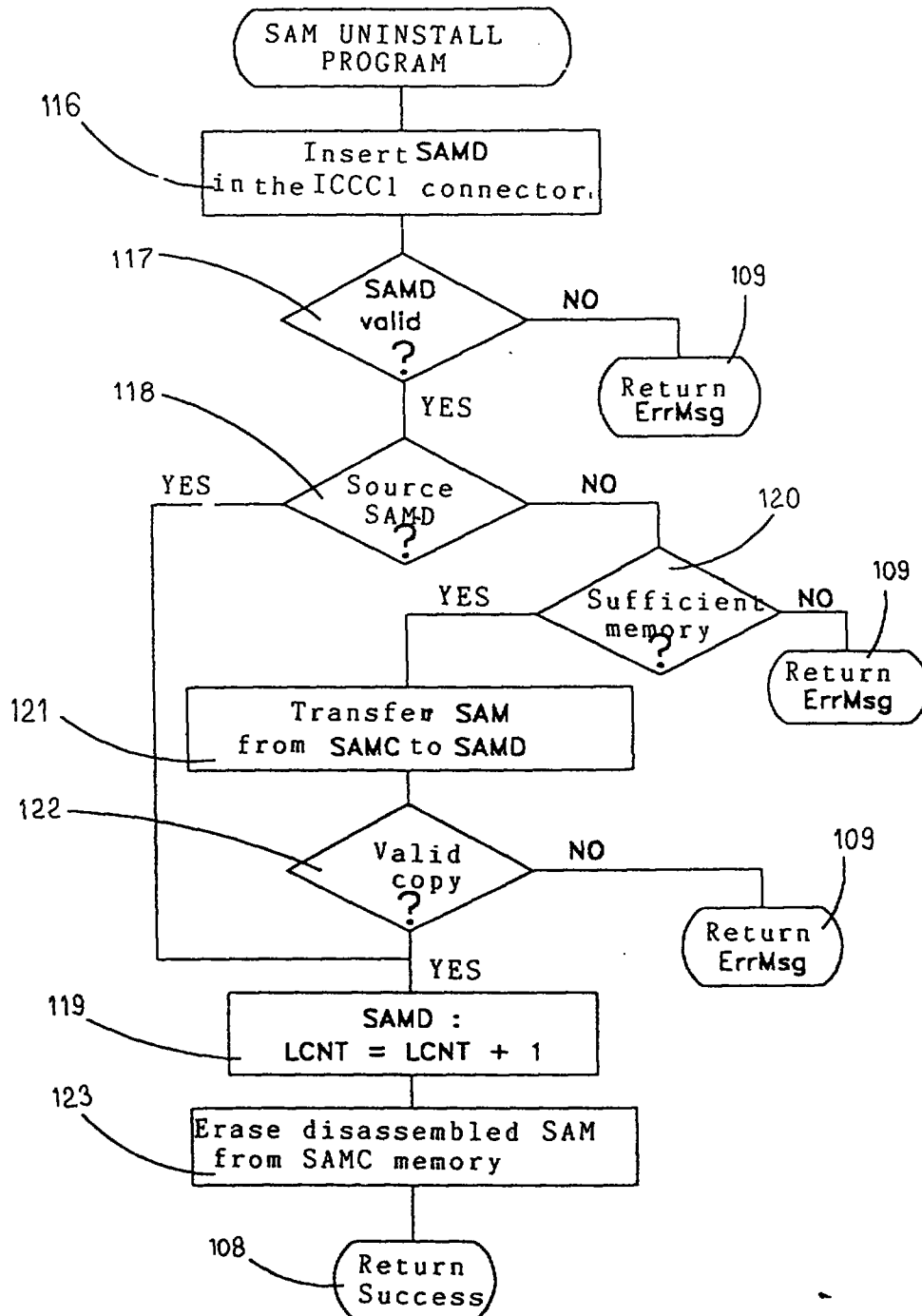


FIG.12

FID	OPC	DLEN	CLG / RPL	CRC
-----	-----	------	-----------	-----

FIG. 13

OPC		
OPC.C	OPC.A	OPC.S

FIG. 14

Séquence	7 MSB	6	5	4	3	2	1	0 LSB
Byte 1	X	1	L	R	X7	X6	Y7	Y6
Byte 2	X	0	X5	X4	X3	X2	X1	X0
Byte 3	X	0	Y5	Y4	Y3	Y2	Y1	Y0

FIG. 15

Séquence	7 MSB	6	5	4	3	2	1	0 LSB
Byte 1	1	1	L	R	X7	X6	Y7	Y6
Byte 2	X	0	X5	X4	X3	X2	X1	X0
Byte 3	X	0	Y5	Y4	Y3	Y2	Y1	Y0
Byte 4	OPC							
Byte 5	DLEN = m							
Byte 6	RPL _{m-1}							
...	...							
Byte m+6	RPL ₀							
Byte m+7	CRC _{n-1}							
...	...							
Byte m+n+6	CRC ₀							

FIG. 16

$m = 32 ; n = 2 ; k = 8 ; FS_{00} ;$

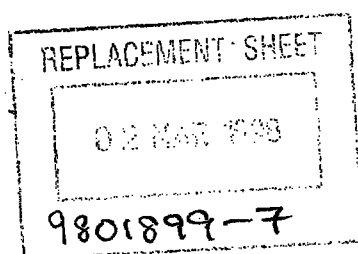
Séquence	7 MSB	6	5	4	3	2	1	0 LSB
Byte 1	1	1	L	R	X7	X6	Y7	Y6
Byte 2	X	0	X5	X4	X3	X2	X1	X0
Byte 3	X	0	Y5	Y4	Y3	Y2	Y1	Y0
Byte 4	OPC							
Byte 5	DLEN = 32							
Byte 6	RPL ₃₁							
Byte 7	RPL ₃₀							
Byte 8	RPL ₂₉							
Byte 9	RPL ₂₈							
Byte 10	RPL ₂₇							
Byte 11	RPL ₂₆							

FIG. 17

$m = 32 ; n = 2 ; k = 8 ; FS_{04} ;$

Byte 1	1	1	L	R	X7	X6	Y7	Y6
Byte 2	X	0	X5	X4	X3	X2	X1	X0
Byte 3	X	0	Y5	Y4	Y3	Y2	Y1	Y0
Byte 4	RPL ₀₁							
Byte 5	RPL ₀₀							
Byte 6	CRC01							
Byte 7	CRC00							

FIG. 18



According to an embodiment the secured storage and execution means of the said security applications are amalgamated into a releasable miniature microcircuit. Therefore, the management and the availability of the said security applications storage and execution means are made independent in relation to the device's maintenance.

Presentation of the figures in appendix.

The invention will be better understood by reading the following detailed summary, giving as a non-restrictive example and illustrated by the figures in appendix

- figure 1 represents a bottom view, (on the ball side) of the conditional access device according to a possible implementation of the invention in its mouse version.;

- figures 2a and 2b, in perspective view represent two embodiments of possible implementations for figure 1's mouse.

- figure 2c represents the view of a screen to operate an embodiment of the implementation.

- figure 3 is a schematic representation illustrating an advantageous configuration inside the mouse casing of figure 1.

- figure 4 is a top view of the ball mouse model of the conditional access device according to another possible embodiment of the implementation.

- figure 5 is a perspective view illustrating a possible implementation mode of figure 4 's embodiment.

- Figure 6 is a schematic representation in a side view, illustrating a possible implementation mode of figure 4.