

The present invention concerns an optional system for the protection of access to a data processing system by means of an intelligent identification card, the method for the protection of access and use of the protection system in a method for access to said data processing system.

In distributed data processing and office automation, it may be advantageous to be able to protect access to microcomputers, stations, terminals or computers.

There are devices for the security of transmission of signals between two data processing stations, but these devices do not take into account the protection of the terminal or computer itself. Moreover, there are also means for locking computers with the aid of keys, for example, which, when the key is not introduced into the lock, inhibit the transmission of data coming from the keyboard. This kind of device, while it has the merit of existing, has the drawback of being readily open to fraud and offering illusory security. It is also known from patent application PCT W081/01063 that access to a terminal can be protected by means of a transmitting card. However, this protection is installed from the start, but the device does not make it possible to initiate protection in an optional manner. Furthermore the device does not provide for checking the authorisation of the bearer of the transmitting card to work with the terminal, which allows easy fraud.

Also known from French patent 2,546,646 is a system for allowing users of intelligent cards to perform transactions if two comparisons are successful, a first one performed in the card, and a second one performed in the terminal. However, such a device or system likewise corresponds to protection installed from the start, but does not make it possible to initiate protection in an optional manner.

European patent EP-A-0,089,876 instructs a method and a device making it possible to monitor distribution of a programme. With this object, the programmes as supplied are non-runnable, and can be run only in the event that they are

used with an intelligent card. This document therefore also instructs possible use of a software resource only in the presence of a card and the possibility of choosing different software resources provided that an enabling key is present in the card. This document therefore instructs use in an optional manner of a software resource, but does not instruct initiation of protection in an optional manner. The programmes are rendered non-runnable by design.

It is a first object of the invention to propose a system for the protection of access to a computer which is both more reliable and not readily open to fraud and which allows implementation of protection in an optional manner.

This first object is achieved by the fact that the optional system for the protection of access to a data processing system by means of an intelligent identification card is characterised in that it comprises a first device offering the user in an optional manner the possibility of initiating the protection of access to the data processing system and, in the case of selection of this option, actuating a second device permitting operation with at least one main resource of the data processing system only in the presence of said card, in that operation with at least one main resource is possible without a card as long as said possibility of initiating the option of protection offered by the first device has not been selected, and in that, as soon as the option of protection has been initiated once, no return to the unselected condition is possible without reconditioning of the system.

According to another characteristic, the main resource is the keyboard and the entry of data coming from the keyboard is inhibited in the absence of the card.

According to another characteristic, the main resource is a magnetic disc and reading of the manager sector of the disc is rendered impossible without a decryption key supplied by the card.

According to another characteristic, the processor of the computer is associated:

with first storage means containing two basic input/output system (BIOS) programmes,
a first so-called programme (BIOS 1) comprising a method for the initialisation and implementation of protection subsequent to choice of the option of protection, and a second so-called programme (BIOS 2) comprising at least one method of access to the protected main resources and calling for the use of an intelligent identification card (CB);
with a second storage means (M), associated with a protective back-up power supply and containing a matrix of pairs of values filed according to an index table, which pairs of values are used in the machine access method of the second programme (BIOS 2); and
with means for selecting use of the second programme (BIOS 2) only, after choosing the option of protection.

A second object of the invention is an optional method for the protection of access to a machine which is economical, reliable and independent of the characteristics peculiar to the machine and to the associated resources.

This object is achieved by the fact that the method for the protection of access to the data processing system by means of an intelligent identification card (CB), said system comprising a processor (1) associated with first (22, 23) and second (M) storage means containing at least first (BIOS 1) and second (BIOS 2) programmes making it possible to implement a method for the initialisation of protection and respectively access to the protected main resources by use of said card (CB) is characterised in that it consists, in the case of selection of the option of protection, of:

- initiating the first programme (BIOS 1) for carrying out initialisation of protection; and
- permitting access to the main resources only by starting of the second programme (BIOS 2), when initialisation has been selected in the course of running the first programme (BIOS 1); and
- preventing any return to the unselected condition without reconditioning of the system.

According to another characteristic, the access method comprises the following steps:

- a) monitoring of the presence of the card (CB);
- b) random drawing of two numbers (dl, dm) from among four possible ones by the second programme (BIOS 2);
- c) determination from the two numbers (dl, dm) and from the associated indices, of the addresses of a pair of values (Ei, Ki) filed in the second storage means;
- d) transmission of a first value (Ei) of the pair (Ei, Ki) to the card (CB);
- e) calculation by the card (CB) of a value $K'i = f(Ei, Nj, S)$;
- f) transmission of the value (K'i) calculated by the card (CB) to the computer for comparison with the second value (Ki) of the pair;
- g) stopping of the programme of the machine access method and locking of the machine in case of non-matching of the values compared (Ki, K'i).

According to another characteristic, the method for access to the disc contained by the second programme (BIOS 2) is carried out only in the event that the values compared (Ki, K'i) match.

According to another characteristic, the method for access to the disc comprises in particular decryption of the encrypted manager sector (s) of the disc, which decryption can be carried out only after supply by the card (CB) of a decryption key (Ci).

It is a third object of the invention to propose a method for the initialisation of protection.

This third object is achieved by the fact that the method for the initialisation of protection comprises the following steps:

- verification of the presence of the material resources formed by the identification card (CB), a printed circuit board (EL) and the connector thereof (CO) and the interface board (I);
- entry by the operator on the keyboard (10) of the

identification number (N_j);

- random drawing carried out by the first programme (BIOS 1) of a first value (E_i) and transmission of this value (E_i) to the identification card (CB);
- storage of the first value (E_i) in the second storage means (M);
- calculation by the identification card (CB) of a second value (K_i) such that $K_i = f(E_i, N_j, S)$;
- transmission of the second value (K_i) to the second storage means (M) and filing in this second storage means;
- implementation of the method for encryption of the disc (PED);
- confirmation of choice of the option of protection;
- locking of the means for selecting exclusive use of the second programme (BIOS 2).

According to another characteristic, the method for encryption of the disc comprises the following steps:

- calculation by the identification card (CB) of a coefficient (C_i) such that $C_i = f(C, N_j, S)$, (C) being a number contained in the card (CB);
- transmission of the coefficient (C_i) to the first programme (BIOS 1);
- calculation by the first programme (BIOS 1) containing the encryption function g , of the encrypted values (s) of the manager sector of the disc from the unencrypted values (s) of this manager sector by the formula $s = g(C_i, s)$.

According to another characteristic, the access method includes between steps a and b a step of input on the keyboard (10) by the bearer of the identification card (CB) of a number N_j for identification and comparison with the number N_j of the card (CB).

Other characteristics and advantages of the present invention will be clearer on reading the description below, given with reference to the attached drawings in which:

Fig. 1 shows a schematic general view of the protection system according to the invention;

Fig. 2 shows a detailed view of the modifications made

to the processor board of the protection system;

Fig. 3 shows the flow chart of the method of initialising the implementation of protection;

Fig. 4 shows the flow chart of the machine access method and disc access method.

The processor board P of a computer or microcomputer or terminal or station for office automation is, as shown in Fig. 1, connected by suitable connectors, not shown, to an interface board (I). This interface board (I) is in turn connected by suitable connectors, not shown, to a printed circuit board (EL) comprising electronics for levelling the signals delivered by an intelligent identity card (CB) to a connector (CO) carried by the printed circuit board (EL). This printed circuit board (EL) also comprises a device for detecting the presence of an identity card, which device consists of a light emitting diode (D) supplied by a voltage source (+V). A phototransistor (T) which is connected by its emitter to earth and the collector of which is connected to a voltage source (+V) via a resistor (R), delivers at its collector the signal indicating the presence or absence of the card. The diode (D) and the phototransistor (T) are arranged relative to the connector (CO) in such a way that the light path of the beam coming from the diode (D) in the direction of the phototransistor (T) is interrupted by the card when the latter is introduced into the connector (CO). The connector (CO) and the electronics of the board (EL) deliver via the series connection (6) and the series connection (4) the information in series supplied by the card (CB) to the series input connection 70 of a series-parallel interface circuit 7 connected by its parallel inputs and outputs (73) to the 8 least significant data bits (D0, D7) of the data bus of the processor board. The series-parallel interface circuit 7 is also connected in a manner known in the art by the lines (71) to the lines of the control bus of the processor (1) necessary for operation thereof and by the lines (72) to the address lines of the address bus (PA) of the processor (1), necessary for

selection of the internal registers of the circuit (7) and for programming this circuit (7). The keyboard (10) is connected by a two-way series connection (100) to a keyboard locking circuit (9). This circuit (9) consists of an AND gate (91) with two inputs of which a first input receives the two-way series connection (100) coming from the keyboard and the second input is connected by means of a connector, not shown, to the line (3) of the board (EL) supplying the signal which indicates the presence of the identity card (CB). Consequently, when the card (CB) is present in the connector (CO), the signal delivered by the line 3 is active (at logic level 1) and the output of the AND gate (91) delivers a signal reproducing the signal transmitted by the series connection (100). This signal is transmitted to the series input (80) of a series-parallel input port (8) of which the parallel outputs (81) are connected to the eight least significant lines (D0 to D7) of the data bus of the processor board (P). A second AND gate (90) with two inputs, of the keyboard lock circuit (9), receives at its first input the signal provided by the two-way series connection (100) and at its second input the signal delivered by the output of a NOT circuit (21) the input of which is connected to the line 20 which transmits the output signal of a logic circuit for selecting the different basic input/output system programmes (BIOS 1), (BIOS 2). This line 20 is at logic level "1" when it is wished to select a second basic input/output system programme (BIOS 2). In this case the output of the NOT circuit (21) is at logic level "0" and the output of the AND gate (90) which is connected to the series input of the port (8) does not transmit the signals coming from the keyboard (10). In the event that the signal transmitted by the line 20 is level "0", this signal indicating that the second programme (BIOS 2) has not been selected, the output of the NOT circuit (21) is at level "1" and the output of the AND gate (90) will reproduce the signal transmitted by the connection (100) coming from the keyboard (10). The processor (1) of the

processor board (P), in the embodiment shown, consists of a processor marketed by the firm INTEL under reference 80 286 and the associated package 82 288. It is quite obvious that this processor could be replaced by any other equivalent processor. The processor board does not show the components necessary for the formation of a microcomputer such as the interface for connection to a magnetic disc or floppy disc reading unit, the connections to the read-write memories for storage of application programmes, etc. Only the components indispensable for understanding the invention and involving modifications in comparison with a conventional processor board have been shown and will be described. First storage means consisting of a memory consisting of two packages (22, 23) of sufficient capacity to contain two basic input/output system programmes are connected on the one hand to the address bus (PA) of the processor (1), and on the other hand to the data bus (BD0 to BD15) of the processor board. The first programme (BIOS 1) comprises a standard basic input/output system programme to which have been added the instructions making it possible to carry out the method for implementing and initialising protection, the flow chart of which is shown in Fig. 3. The second programme (BIOS 2) comprises in addition to the standard input/output programme the instructions making it possible to carry out the machine access method (P.A.M.) and the disc access method (P.A.D.). These programmes are run as for a standard programme (BIOS) by the processor 1. The selection between the first programme (BIOS 1) and the second programme (BIOS 2) compulsorily requiring use of the intelligent card (CB) is made with the aid of the line 20 which is connected to the input (A13) of the ROM packages (22, 23). The selection signal arriving at the input (A13) of the ROM packages (22, 23) authorises half of the capacity of the first storage means, in which half resides the programme (BIOS 2). The protection system also comprises a second confidential storage means (M) which is connected to the address bus (PA) on the one hand, and on the other hand to the 8 least

significant bits (D0 to D7) of the data bus (BD0 to BD15). This read-write memory (M) has its own power supply (29) so as to avoid the loss of data following a power failure, and also avoid reading of the data contained in this memory. In fact, in case of an attempt at reading, it will be necessary to disconnect the memory from the board and hence break the connections (290) with its power supply (29). This will automatically cause loss of the information contained in this read-write memory (M). This memory (M) contains a set of pairs of values (Ki, Ei) used by the second programme (BIOS 2). These pairs of values are filed in this memory at addresses defined by an index table also contained in this memory (M). The power supply of this memory (29) may consist of a battery or a capacitor with a very high capacitance. As an order of magnitude, the capacity of this memory may be 128 octets.

Fig. 2 shows in detail selection between the different programmes residing in first storage means consisting of the read-only memory packages (22, 23) and the circuits which make it possible to access the memory (M) only by an instruction from the programmes (BIOS). The read-only memory packages (22, 23) are addressed at their inputs (A0 to A12) by the address lines (PA1 to PA13) of the address bus of the processor. The selection between the package (22) and the package (23) is made by the address line (PA0) which is connected to a second select input (CS2) of the package (22). This same address line (PA0) is also connected by means of the NOT circuit (230) to the second input (CS2) of the package (23). The first select input (CS1) of the package (23) receives the output of a decoding circuit (34) which receives at its inputs the address lines (PA14 to PA19) of the address bus of the processor. This package (24) by decoding its address lines (PA14 to PA19) activates its output signal when decoding indicates addressing of the programmes (BIOS). The output of the package (24) is also connected to the first select input (CS1) of the read-only memory (22). The package (23) serves

to deliver the least significant data bits (D0 to D7), while the package (22) serves to deliver the most significant data bits (D8 to D15) to the data bus of the processor board. Consequently the logical value of the signal (PA0) will make it possible to determine the least significant octet or most significant octet. The most significant address input (A13) of the read-only memory packages (22, 23) is connected to the line (20) which delivers the signal for selection between the first programme (BIOS 1) and the second programme (BIOS 2). Consequently according to the logic level of this line (20), there is selected one of the two pages of the memory consisting of the two packages (22, 23), selection of which is controlled by (A13) and in which the two programmes are filed. When (A13) is at level "1", the page containing the programme (BIOS 2) is selected, this page of the memory zone corresponding to the occupation of a portion of the package (22) and a portion of the package (23), by the programme (BIOS 2). This line (20) is connected by a resistor (R2) to a voltage source of +5 volts and by a fuse (F) to earth. A resistor (R1) connects the common point to the resistor (R2) and to the fuse (F) at the emitter of a transistor (T2) of which the collector is connected to a voltage source of +5 volts. The base of the transistor is connected on the one hand to earth by a capacitor (C), and on the other hand by a resistor (R3) to the output (Q) of a trigger (28) of type (D). This trigger (28) receives at its clock input the signal (ALE) coming from the processor (1) and at its input (D) a signal coming from the output of a decoder circuit (25). The zero reset input of this trigger (28) is connected to the (RESET/) signal of the processor (A). The decoder (25) receives at its inputs the address lines (PA0 to PA15) of the address bus and the signal (IOW) coming from the processor (1). Consequently when the programme for initialising locking contained, as will be seen later, in the first programme (BIOS 1) transmits an input/output write instruction to the processor (1) with a certain combination of address lines

(PA0 to PA15), the output of the decoder (25) becomes active. Hence the output (Q) of the trigger (28) will be activated as soon as the address authorising signal (ALE) appears. Activation of the output (Q) will cause the transistor (T2) to become conductive and the fuse (F) to burn out. This fuse (F) being burnt, the line (20) will be positioned at logic level "1" and the programme (BIOS 2) will be selected in the memory packages (22, 23). As long as the output (Q) is not enabled, the transistor (T2) does not conduct and the fuse (F) positions the line (20) at logic level "0". This selects the first programme (BIOS 1) in the read-only memory packages (22, 23). On reinitialisation of the system, the signal (RESET) maintains the trigger at "0", which avoids inadvertently causing the output (Q) of the trigger (28) to be set to "1" and the fuse (F) to melt accidentally. The resistors (R3) and the capacitor (C) act as a low-pass filter which prevents the transmission of transition signals, which could arise during reinitialisation of the system. It is therefore only when the signal (Q) is correctly established that the fuse (F) will burn out.

Selection of the memory (M) for loading thereof by the first programme (BIOS 1) or for utilisation of its data by the second programme (BIOS 2) is carried out in the manner described below. The first select input (S1) of the memory (M) receives the address line (PA0) of the address bus of the processor (1). The inputs (MA0 to MA8) of the memory (M) receive 8 of the address lines (PA0 to PA12) of the address bus of the processor (1). This selection on address lines (PA0 to PA12) thus makes it possible to carry out coding of the addresses of the memory (M). The input (W) of the memory (M) receives the output signal (W) of the processor (1), and this signal (W) indicates writing in the memory. The second select input (CS2) of the memory (M) receives the output (Q) of a trigger (26) of type (D) of which the zero set input receives the signal (RESET/) from the processor (1). This trigger (26) receives at its input

(D) the output of the decoding circuit (24) indicating addressing of an instruction of the BIOS. This trigger (26) receives at its clock input the output of an AND gate (27) with five inputs, of which the inputs are connected respectively to the outputs (S1, S0/, COD-INTA/, M/IO/ and ALE). All these outputs being at level "1" indicates that the processor is carrying out reading of an instruction code. It is obvious that in the case of another processor, these signals can easily be replaced by the equivalent signals, which indicate reading of an instruction code by the processor. Hence every time an instruction resides in the read-only memory (BIOS), the input (D) of the trigger (26) is at logic level "1" and when the processor (1) carries out reading of the instruction code, the output of the AND gate also changes from logic level "0" to logic level "1". Hence the output (Q) of the trigger (26) changes to logic level "1", and selects the memory (M). The memory (M) can therefore be accessed only when an instruction filed in the read-only memory containing the programmes (BIOS) is read and when the address of the instruction corresponds to the addresses of the memory (M). So as to lock access to the memory (M), the programmes filed in the read-only memories (22, 23) will have no subprogramme structure, that is, will not comprise the presence of a "RETURN" instruction and will not use the read-write memory (not shown) of the processor as a data storage element. This memory (M) contains a set of pairs of values (Ei, Kj) filed at addresses determined by an index table. This index table is itself filed in the memory (M) at addresses determined by the pairs (dl, dm) of line numbers.

The method for carrying out and initialisation of locking will now be described in connection with Fig. 3.

In the self-test section of the standard programme (BIOS) is found a step (31) in which the operator is asked if he wants to initiate the option of locking or not. In the event that the operator does not wish to initiate the option, the programme goes on to step (32) which is the end

of the normal self-test of a standard programme (BIOS). If the operator selects the option of locking, the programme goes on to step (33) consisting of a test for checking the presence of the material resources necessary for locking, that is, the presence of the interface board, the printed circuit board, the connector (CO) and the presence of an intelligent card (CB) provided with a processor and a memory. If the test is negative, the programme continues with a message and the locking procedure is abandoned as shown by step (34) of the flow chart of Fig. 3. In the case of presence of the material resources, the programme continues with the following conversational steps. Step (34) asks the operator for a code (N_j) specific to the machine or to the user, then the first programme (BIOS 1) undertakes random drawing, making it possible to determine a number (E_i) of 16 bits. This random drawing is shown by step (36). In step (37) the number (E_i) is stored in a register of the processor (1) and transmitted to the card (CB) for carrying out step (38). Step (38) consists of a calculation performed by the card (CB), this calculation making it possible to determine a coefficient (K_i) such that $(K_i) = f(E_i, N_j, S)$. The number (S) is a secret number contained in the card and inaccessible from the outside, (f) is the secret function performed by the wiring of the board, and (N_j) is the code specific to the machine already stored in the card. Step (39) consists of transmitting the calculated (K_i) to the processor (1). In step (40), the key (E_i) determined by the (BIOS) and the key (K_i) calculated by the card are filed in the confidential memory (M) at an address determined by the index table as a function of the random drawing of two values (d_i, d_j) out of four, as will be seen below. After filing, it continues with a step (41) which consists of a test on the value (i) to find out whether the calculated number of pairs is less than a certain value (N). In the embodiment chosen, the value is taken as ($N = 10$). As long as (i) is between 1 and 10, steps (35 to 41) are repeated, and as soon as (i) exceeds a

value of 10, it continues with the method of encryption of the disc (PED). This method begins with a calculation performed by the card (CB) to determine a key (C_i) such that $(C_i) = f(C, N_j, S)$, (C) being a coding value contained in the card (CB). The next step (43) consists of transmitting the calculated value (C_i) to the (BIOS 1). Then the (BIOS 1) goes on to step (44) which consists of encrypting the data (s) of the manager sector of the disc. These data are encrypted by a function (g) present in the first programme (BIOS 1), such that $\hat{s} = g(C_i, s)$, (s) denoting the unencrypted data of the manager sector of the disc, ($\hat{s}$) the encrypted data of the manager sector of the disc, and (g) the encryption function performed by the programme (BIOS 1). The method of implementation and locking continues with a step (45) requesting confirmation of the locking option before carrying out step (46) which carries out burning of the fuse (F) by an input/output write instruction defined by the addresses belonging to the decoder (25). This step (46) causes (BIOS 1) to disappear in favour of (BIOS 2), and subsequently the end of the self-test which had started in (BIOS 1) continues with step (47) in (BIOS 2). Then, every time the system is started up, the programme (BIOS 2) is run. No return to BIOS 1 is possible without reconditioning of the machine.

The process of filing the pairs (K_i, E_i) in the memory (M) as well as the index table contained in this memory will now be described.

In so far as the passage of data becomes invariant between the processor, the memory (M) and the connector (CO), it is still possible to detect the value of the keys with a measuring apparatus connected to the bus or the serial board. There is then provision for performing an algorithm, the principle of which is as follows: providing calculations of different keys from a random draw restricted to a range of values. For a given machine (identified by the serial number N_j), it is possible to precalculate several keys from a random series, say ten pairs K_{ij} and E_{ij}

($i = 1$ to 10). The arrangements are then as follows:

1. The K_{ij} values are filed in the memory M , with the E_{ij} values. An encryption table is thus formed with ten pairs.
2. The method of filing carried out by the first programme (BIOS 1) corresponds to a singular matrix called a parity identification matrix (PIM), the property of which is to retrieve any pair of elements from the line numbers containing these elements.

An example of a known PIM model with mnemonic marking is as follows:

	0	32	64	96	128	160
d1	M	U	T	U	S	
d2	N	O	M	E	N	
d3	D	E	D	I	T	
d4	C	O	C	I	S	

The description is one-to-one between the pairs ($d1$, d_m) $1 \leq m \leq 4$; $1 \leq m \leq 4$ of the line numbers and the elements. From this matrix is deduced the following table of indices combined in a pair of values ($d1$, d_m) of line numbers. The table can be reduced to 10 elements.

LINE NO. --- PIM	INDEX OF ELEMENTS
d1d1 ---- UU	d1 + 32, d1 + 96
d1d2 ---- MM	d1 + 0, d2 + 64
d1d3 ---- TT	d1 + 64, d3 + 128
d1d4 ---- SS	d1 + 128, d4 + 128
d2d2 ---- NN	d2 + 0, d2 + 128
d2d1 ---- MM	d2 + 64, d1 + 0
d2d3 ---- EE	d2 + 96, d3 + 32
d2d4 ---- OO	d2 + 32, d4 + 32
d3d1 ---- TT	d3 + 128, d1 + 64
d3d2 ---- EE	d3 + 32, d2 + 96
d3d3 ---- DD	d3 + 0, d3 + 64
d3d4 ---- II	d3 + 96, d4 + 96
d4d1 ---- SS	d4 + 128, d1 + 128
d4d2 ---- OO	d4 + 32, d2 + 32
d4d3 ---- II	d4 + 96, d3 + 96
d4d4 ---- CC	d4 + 0, d4 + 64

This property makes it possible to provide by the first programme (BIOS 1) for filing of the keys K_{ij} and E_{ij} combined in the memory (M) (inaccessible by the RAM) such that the second programme (BIOS 2) can retrieve the pairs just by the matrix line numbers, drawn at random without knowing the arrangement of elements in the matrix.

As an example, here is a matrix containing the K_i and E_i values filed by the above method.

d1	K1	K2	K3	E2	K4
d2	K5	K6	E1	K7	E5
d3	K8	E7	E8	K9	E3
d4	K10	E6	E10	E9	E4

Initialisation is then carried out in the following manner by the BIOS:

- the lines numbers are drawn randomly by BIOS (e.g. d2d3) in order to file in the registers the corresponding pair K_{ij} and E_{ij} (e.g. K7, E7) from the unknown keys and indices (d2 + 96, d3 + 32) of BIOS.
- subsequent filing will be carried out by another draw of a pair of line numbers, etc.

In conclusion, filing is created:

- without explicit identification of the addresses of elements (the shift values are in the PIM table of M),
- with the possibility of modifying the PIM table either in its structure (the BIOS does not modify its system of access to the table, and only the PIM indices are reviewed), or in its contents (initialisation ensures complete refreshing of the table contents from a smart banker's card). The flow chart of Fig. 4 makes it possible to clarify the machine access method (PAM) and the disc access method (PAD) in the case of a locked machine. In this case this machine uses only the programme (BIOS 2) and consequently while the self-test section of the programme (BIOS 2) proceeds there will be carried out step (61) which consists of a test for the presence of a banker's card containing the value (C), a value (N_j) and the secret value (S). In the event that the presence is

not detected, the keyboard locking step 62 is carried out. These two steps 61 and 62 are in fact carried out by the diode device (D), the transistor (T) and the AND gate (91) of Fig. 1. (In the case of presence of the card, the operator enters in an optional manner on the keyboard an identification number (N_j), and this number is compared with the one (N_j) contained in the card, and in case of non-coincidence, the self-test is stopped. In this case the machine becomes unusable.) In case of detection of presence of the card or coincidence in the event that the above comparison option is chosen, one proceeds to the next step (64) which consists of a random draw of two numbers out of four. These two numbers (d_1, d_m) drawn from among the values (d_1 to d_4) form a pair of line numbers which will make it possible to determine by the memory (M) the index values to be added respectively to each of these two numbers in order to determine the addresses at which are filed the two values of the pair (K_i, E_j) corresponding to these two numbers (d_1, d_m). Following this determination of address, the programme (BIOS 2) carries out reading of the pair (E_i, K_i) contained in this memory (M) and transmits the first value (E_i) to the banker's card (CB). This is accomplished in the course of steps (65 and 66). In step (67) of the process, the card (CB) performs calculation of a value (K'_i) such that $K'_i = f(E_i, N_j, S)$. This value (K'_i) is compared, in the course of a step (68), with the second value of the pair read from the memory (M), this second value being the value K_i . If they do not coincide, a new test is performed, and at the end of a certain number of tests the self-test is stopped; this is shown by step (69) of the flow chart. In the event that they do coincide, it continues either with the end of the self-test (BIOS 2) and the application programmes which follow, or in the event that reading/writing of the disc or diskette is requested, with the disc access method (PAD). A disc read/write step (50) is always followed by a step (51) for

calculation of the value $C_i = f(C, N_j, S)$ by the card (CB) and transmission of this value (C_i) to the (BIOS 2). This step is followed by reading the encrypted manager sector of the disc represented by step (52). The values (s) of the encrypted sector are then decrypted in the course of a step 53 performed by the (BIOS 2) from the function g^{-1} contained in this (BIOS 2) according to the formula $s = g^{-1}(C_i, s)$. Subsequently, the end of the self-test or the application programmes are run normally as if the machine were not protected. Consequently, by encryption of the manager sector of the disc it is impossible to transfer either a hard disc or a diskette to another unlocked machine and to read the data if one does not have the encryption key of the manager sector of the disc, part of which is supplied by the smart card (CB). Moreover, in the event that one does not have a card of the above type either, the keyboard is locked and no command can be input into the machine. Finally, the use of two different programmes, one of which cannot be accessed until after irreversible selection (except by a maintenance service), makes it possible to ensure very efficient protection for access to computers.

Claims

1. Optional system for the protection of access to a data processing system by means of an intelligent identification card (CB), characterised in that it comprises a first device offering the user in an optional manner the possibility of initiating the protection of access to the data processing system and, in the case of selection of this option, actuating a second device permitting operation with at least one main resource of the data processing system only in the presence of said card (CB), in that operation with at least one main resource of the data processing system (10) is possible without a card as long as said possibility of initiating the option of protection offered by the first device has not been selected, and in that, as soon as the option of protection has been initiated once, no return to the unselected condition is possible without reconditioning of the system.

2. System according to claim 1, characterised in that the main resource is the keyboard (10) and the entry of data coming from the keyboard (10) is inhibited in the absence of the card (CB).

3. System according to claim 1, characterised in that the main resource is a magnetic disc reader and reading of the manager sector of the disc (s) is rendered impossible without a decryption key (Ci) supplied by the card (CB).

4. Protection system according to any of the preceding claims, characterised in that the processor (1) of the computer is associated:

with first storage means (22, 23) containing two basic input/output system (BIOS) programmes,

a first so-called programme (BIOS 1) comprising a method for the initialisation and implementation of protection subsequent to choice of the option of protection, and a second so-called programme (BIOS 2) comprising at least one



method of access to the protected main resources and calling for the use of an intelligent identification card (CB); with a second storage means (M), associated with a protective back-up power supply (29) and containing a matrix of pairs of values (E_i , K_i) filed according to an index table, which pairs of values are used in the machine access method of the second programme (BIOS 2); and with means (2, 20, 9) for selecting use of the second programme (BIOS 2) only, after choosing the option of protection.

5. System according to claim 4, characterised in that the interface circuit between the bus of the computer processor (1) and the keyboard (10) comprises means (91) making it possible, in the case of choice of the option of protection, to inhibit the transmission of data coming from the keyboard (10) when a signal indicating presence of the card (CB) is not active.

6. Optional method for the protection of access to a data processing system by means of an intelligent identification card (CB), said system comprising a processor (1) associated with first (22, 23) and second (M) storage means containing at least first (BIOS 1) and second (BIOS 2) programmes making it possible to implement a method for the initialisation of protection and respectively access to the protected main resources by use of said card (CB), characterised in that it consists, in the case of selection of the option of protection, of:

- initiating the first programme (BIOS 1) for carrying out initialisation of protection; and
- permitting access to the main resources only by starting of the second programme (BIOS 2), when initialisation has been selected in the course of running the first programme (BIOS 1); and
- preventing any return to the unselected condition without reconditioning of the system.



7. Method according to claim 6, characterised in that the access method comprises the following steps:

- a) monitoring of the presence of the card (CB);
- b) random drawing of two numbers (dl, dm) from among four possible ones by the second programme (BIOS 2);
- c) determination from the two numbers (dl, dm) and from the associated indices, of the addresses of a pair of values (Ei, Ki) filed in the second storage means;
- d) transmission of a first value (Ei) of the pair (Ei, Ki) to the card (CB);
- e) calculation by the card (CB) of a value $K'i = f(Ei, Nj, S)$;
- f) transmission of the value (K'i) calculated by the card (CB) to the computer for comparison with the second value (Ki) of the pair;
- g) stopping of the programme of the machine access method and locking of the machine in case of non-matching of the values compared (Ki, K'i).

8. Method according to claim 7, characterised in that it consists of carrying out a method for access to the disc contained by the second programme (BIOS 2) only in the event that the values compared (Ki, K'i) match.

9. Method according to claim 8, characterised in that the method for access to the disc comprises in particular decryption of the encrypted manager sector (s) of the disc, which decryption can be carried out only after supply by the card (CB) of a decryption key (Ci).

10. Method according to claim 6, characterised in that the method for the initialisation of protection comprises the following steps:

- verification of the presence of the material resources formed by the identification card (CB), a printed circuit board (EL) and the connector thereof (CO) and the interface board (I);



- entry by the operator on the keyboard (10) of the identification number (N_j);
- random drawing carried out by the first programme (BIOS 1) of a first value (E_i) and transmission of this value (E_i) to the identification card (CB);
- storage of the first value (E_i) in the second storage means (M);
- calculation by the identification card (CB) of a second value (K_i) such that $K_i = f(E_i, N_j, S)$;
- transmission of the second value (K_i) to the second storage means (M) and filing in this second storage means;
- implementation of the method for encryption of the disc (PED);
- confirmation of choice of the option of protection;
- locking of the means for selecting exclusive use of the second programme (BIOS 2).

11. Method according to claim 10, characterised in that the method for encryption of the disc (PED) comprises the following steps:

- calculation by the identification card (CB) of a coefficient (C_i) such that $C_i = f(C, N_j, S)$, (C) being a number contained in the card (CB);
- transmission of the coefficient (C_i) to the first programme (BIOS 1);
- calculation by the first programme (BIOS 1) containing the encryption function g , of the encrypted values (s) of the manager sector of the disc from the unencrypted values (s) of this manager sector by the formula $s = g(C_i, s)$.

12. Method according to claim 7, characterised in that the access method includes between steps a and b a step of input on the keyboard (10) by the bearer of the identification card (CB) of a number N_j for identification and comparison with the number N_j of the card (CB).

